ILGSPD Publication Series
No 10/25: Working Paper

The Legal Status of Ukraine's Mobile App Users in the Russia-Ukraine Armed Conflict

Tamar Chkhitunidze
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

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

THE LEGAL STATUS OF UKRAINE'S MOBILE APP USERS IN THE RUSSIA-UKRAINE ARMED CONFLICT*

*Tamar Chkhitunidze***

Introduction

Interstate armed conflicts continue to pose a major threat to international security in the twenty-first century, as technological advancements reshape the traditional dynamics of warfare. Although civilians have traditionally not directly participated in hostilities,[1] the 'digitalization' and 'civilianization' of warfare has made modern conflict 'without bystanders'.[2] As early as eight decades ago, Hersch Lauterpacht warned of the growing difficulty in distinguishing between combatants and civilians amid evolving military technologies.[3] Today, the unprecedented scale and scope of civilian involvement in contemporary conflicts represent one of the most significant changes in modern warfare, bringing the issue under intense scrutiny within International Humanitarian Law (IHL) discourse.[4]

---

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

** 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] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) 38–39; 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) 327; David A Wallace, Shane Reeves and Trent Powell, 'Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines' (2021) 12 Harvard National Security Journal 164.

[2] Kubo Mačák, 'Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield' (2023) 105 International Review of the Red Cross 965, 966; Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the Twenty-First Century* (1st edn, Oxford University Press 2022) 47. By 'bystanders', this paper aligns with the definition provided by Ford and Hoskins, indicating individuals who, through the networking of their digital devices, become participants in and subjects of warfare (this involves civilians recording events, sharing information, and contributing to military operations).

[3] Hersch Lauterpacht, 'The Law of Nations and the Punishment of War Crimes' (1944) 21 British Yearbook of International Law 58, 74–75.

[4] Michael N Schmitt, '"Direct Participation in Hostilities" and 21st Century Armed Conflict', *Krisensicherung und Humanitärer Schutz/Crisis Management and Humanitarian Protection: Festschrift für Dieter Fleck* (Berliner Wissenschafts-Verlag 2004) 512–513; Michael N Schmitt, 'Humanitarian Law and

The ongoing Russia-Ukraine armed conflict demonstrates the evolving role of civilians in modern warfare.[5] Following the Russian invasion, Ukraine announced the formation of an 'IT Army',[6] comprising of more than 400,000 Ukrainian and international volunteer hackers (hacktivists) engaged in targeting Russian infrastructure and websites.[7] Furthermore, the Ukrainian government's 'Дія' ('Diia') mobile application (app),[8] used by over 18 million citizens at the time for accessing government services, has integrated a new feature, 'єВорог' ('eEnemy'), which allows users to report the movements of invading forces.[9] Additionally, a separate mobile app 'єППО' ('ePPO')[10] has been developed, enabling civilians to use their cell phones to pinpoint and report the locations of incoming missiles and other aerial threats.[11]

Prior to Russia's full-scale invasion, Ukraine boasted an advanced information infrastructure. As of 2021, 83 per cent of Ukrainian households had internet access; 79

Direct Participation in Hostilities by Private Contractors or Civilian Employees' (2005) 5 Chicago Journal of International Law 511.

[5] While cyber warfare has been a significant aspect of the conflict since 2014, this paper specifically addresses events post-2022 invasion.

[6] '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.

[7] 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.

[8] 'Дія - Державні послуги онлайн [Diia - Government Services Online]' (*Дія*) <https://diia.gov.ua> accessed 30 April 2024.

[9] Laurens Gaukema, 'GovTech Incubator Launched at the 2023 Digital Government Summit' (*Joinup*, 30 May 2023) <https://joinup.ec.europa.eu/interoperable-europe/news/govtech-incubator-launched-2023-digital-government-summit> accessed 7 January 2024; Lisa O'Carroll, 'Meet Diia: The Ukrainian App Used to Do Taxes … and Report Russian Soldiers' *The Guardian* (26 May 2023) <www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers> accessed 7 January 2024.

[10] 'єППО - Система Єдиної Протиповітряної [ePPO - Unified Air Defense Complex]' (*ePPO*) <https://eppoua.com/> accessed 9 January 2024.

[11] Dan Sabbagh, 'Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks' *The Observer* (29 October 2022) <www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo> accessed 7 January 2024; Michael N Schmitt and William Casey Biggerstaff, 'Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?' (*Lieber Institute*, 2 November 2022) <https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/> accessed 7 January 2024; Mary Ilyushina, 'Russia Asks Citizens to Use New App to Report Drones and Other Attacks' *Washington Post* (21 September 2023) <www.washingtonpost.com/world/2023/09/20/russia-app-drone-citizens-war/> accessed 7 January 2024.

per cent of the population were using the internet; 91 per cent owned a mobile phone; and 92 per cent of people were covered by at least a 4G network.[12] Thus, for Ukrainians, the battleground became a swipe away. They evolved into 'spotters' who enhance targeting processes (using smartphones for the first time in military history as potent tools, comparable in impact to traditional weapons)[13] while also exposing themselves to potential enemy action.[14]

This paper intends to address the central question: *In the context of the ongoing Russia-Ukraine armed conflict, what is the legal status of civilians who use mobile apps to transmit intelligence to government forces?* This is particularly urgent given the growing operational role of civilians in digital warfare and the legal ambiguity surrounding their status under IHL. Typically, civilians are protected from being directly targeted, but this immunity can be forfeited if their actions align with those of combatants, thus making them legitimate targets. The question of whether civilians engaged in cyber operations during armed conflicts meet the Direct Participation in Hostilities (DPH) criteria is both contentious and crucial for upholding the 'cardinal' principle of distinction. In the present case, this issue becomes more critical considering that Russia views cyberspace as a '*de facto* legal vacuum', a status it believes will persist until a comprehensive international legal agreement is established to define and regulate state conduct in this domain.[15]

What is even more concerning is that on the battlefield, Russian military units have access to the Leer-3 Electronic Warfare system. This technology can detect and engage with mobile phone communication systems to disrupt or specifically target individuals using

[12] 'ITU Datahub' <https://datahub.itu.int/data/?e=UKR> accessed 27 September 2025.
[13] Tim Judah, 'How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders' *Financial Times* (10 April 2022) <www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8> accessed 9 January 2024.
[14] Matthew Ford, 'The Smartphone as Weapon Part 2: The Targeting Cycle in Ukraine' (2022) 1,3 <www.academia.edu/76011845/The_Smartphone_as_Weapon_part_2_the_targeting_cycle_in_Ukraine> accessed 30 April 2024; Pontus Winther and Per-Erik Nilsson, 'Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare' (2023) 2 <https://hcss.nl/report/smart-tactics-or-risky-behaviour-the-lawfulness-of-encouraging-civilians-to-participate-in-targeting-in-an-age-of-digital-warfare/> accessed 17 April 2024.
[15] Russian Federation, 'Commentary of the Russian Federation on the Initial "Pre-Draft" of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' <https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf> accessed 7 January 2024.

their devices.[16] Reports surfaced early in the conflict that Russian troops had targeted and sometimes fatally wounded civilians caught with smartphones, a fact acknowledged by the Russian authorities.[17] A defector from Russia, stationed in Bucha, disclosed that his unit was explicitly ordered to eliminate anyone transmitting information regarding their location, regardless of whether they were combatants or civilians.[18] He starkly noted: 'If someone had a phone – we were allowed to shoot them'.[19]

The application of the DPH rule requires careful, individual assessment. Consequently, the Russian armed forces' strategy of targeting civilians simply because they possess a mobile phone, based on the broad assumption that these civilians are actively involved in hostilities, represents both a misunderstanding and a breach of the DPH rule.[20] Such actions could also rise to the level of war crimes of 'intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities'.[21]

To assess how existing IHL applies to civilian involvement in cyber operations, this paper adopts a doctrinal legal research methodology. It combines legal analysis of primary sources such as the Fourth Geneva Convention relative to the Protection of Civilian Persons in Time of War (GCIV) 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).

---

[16] 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.

[17] Judah (n 13); Matthew Ford, 'The Smartphone as Weapon Part 3: Participative War, the Laws of Armed Conflict and Genocide by Smartphone' (2022) 1 <www.academia.edu/77205229/The_Smartphone_as_Weapon_part_3_participative_war_the_laws_of_armed_conflict_and_genocide_by_smartphone> accessed 30 April 2024; Matthew Ford, 'Ukraine, Participation and the Smartphone at War' [2023] Political Anthropological Research on International Social Sciences 1, 3.

[18] Fred Pleitgen, Claudia Otto and Ivana ottasová, '"There Are Maniacs Who Enjoy Killing," Russian Defector Says of His Former Unit Accused of War Crimes in Bucha' (*CNN*, 14 December 2022) <www.cnn.com/2022/12/13/europe/russian-defector-war-crimes-intl-cmd/index.html> accessed 16 April 2024.

[19] ibid.

[20] Winther and Nilsson (n 14) 6.

[21] Rome Statute of the International Criminal Court 1998 art 8(2)(b)(i).

This paper begins by examining the widespread use of mobile applications by civilians in the Russia–Ukraine armed conflict (Section 1.1.) and then assesses the applicability of current IHL to cyber operations, with particular attention to the principle of distinction (Sections 1.2. and 1.3.). It goes on to analyse the DPH criteria, namely the threshold of harm, direct causation, and belligerent nexus, and applies them to civilian app users (Section 2.1.), before considering the temporal scope of DPH and the 'revolving door' phenomenon (Section 2.2.). The analysis concludes that such app users may qualify as directly participating in hostilities, thereby temporarily forfeiting their protection under IHL, and observes that in the absence of a universally accepted interpretation, state practice can significantly extend the period during which civilians are lawfully targetable.

1. Civilian Participation and Legal Challenges in Cyber Warfare

1.1. Ukraine's Use of 'Diia' and 'ePPO' Apps

Following Russia's full-scale invasion of Ukraine, a significant aspect of Ukraine's digital strategy involves the innovative use of mobile apps. Launched in 2020, the 'Diia' app has revolutionised the way Ukrainian citizens access government services online. As of now, the app is used by over 22 million users.[22] The significance of the 'Diia' platform escalated notably following the onset of Russia's full-scale invasion in February 2022. Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, noted that during the initial days of the invasion, the platform was instrumental in issuing evacuation documents and facilitating the reporting of property damage.[23] Post-invasion, 'Diia' has been adapted to include additional functionalities; among these is the 'eEnemy' chatbot.[24] This feature allows Ukrainian civilians to act as 'spotters' by using the chatbot to inform the Ukrainian military about enemy movements, activities, and possible collaborators. Hosted on the

[22] Ben Morris, 'Ukraine: Why It Has One Of The Most Digital Governments' (*BBC*, 17 June 2025) <www.bbc.com/news/articles/cm234l04xmro> accessed 27 September 2025.
[23] Anatoly Motkin, 'Ukraine's Diia Platform Sets the Global Gold Standard for E-Government' (*Atlantic Council*, 30 May 2023) <www.atlanticcouncil.org/blogs/ukrainealert/ukraines-diia-platform-sets-the-global-gold-standard-for-e-government/> accessed 20 July 2024.
[24] 'Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог [Help the Armed Forces of Ukraine Destroy the Occupier: the Ministry of Digital Transformation Launches the eEnemy Chatbot]' (*Міністерство цифрової трансформації України*, 10 March 2022) <https://thedigital.gov.ua/news/dopomozhi-zsu-znishchiti-okupanta-mintsifra-zapuskae-chatbot-evorog> accessed 30 April 2024; Lukasz Olejnik, 'Smartphones Blur the Line Between Civilian and Combatant' (*Wired*) <www.wired.com/story/smartphones-ukraine-civilian-combatant/> accessed 10 January 2024.

Telegram messaging service, the 'eEnemy' chatbot enables users to share photos, videos, geolocations, and detailed descriptions of any suspicious activities they observe.[25]

Another innovative 'spotting' tool available to Ukrainian civilians is the smartphone app 'ePPO', which enables users to report air threats by aiming their phone at the threat and pressing a red button. Developed in 2022 by Technari, a design group that is part of the local volunteer community Odesa Defence 2.0, 'ePPO' integrates tightly with the digital ecosystem for enhanced security.[26] Users must verify their identity through the 'Diia' public services app to prevent the dissemination of false alarms that could assist enemy forces.[27]

According to Gennady Suldin, co-developer of 'ePPO', the app serves as an auxiliary tool for air reconnaissance, enhancing the military's capability to detect aerial targets and complementing traditional radar systems, especially in areas with radar visibility issues.[28] To use 'ePPO', the user simply opens the app, selects the type of incoming threat – whether it be a plane, helicopter, missile, or drone – and presses the prominently displayed red button.[29] The app's system then verifies the reported information by cross-referencing the geolocation of the user's smartphone with the location of the nearest mobile base station and comparing this data with reports from other users.[30] If the report is verified as accurate, the information is swiftly relayed to the command post of the Ukrainian Armed Forces. Here, military specialists calculate the flight path of the incoming threat and coordinate a response.[31] The entire process, from sending data to

[25] 'Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог [Help the Armed Forces of Ukraine Destroy the Occupier: the Ministry of Digital Transformation Launches the eEnemy Chatbot]' (n 24).
[26] Interview with Gennady Suldin, 'Seven Seconds from Smartphone to Air Defense Maps: How One App Unites Millions to Shoot Down Russian Missiles' (3 April 2023) <https://rubryka.com/en/article/seven-seconds-to-air-defense-maps/> accessed 15 April 2024.
[27] Focus, 'Приложение "єППО" Помогло ВСУ Сбить Иранские Дроны Shahed (Видео) [The "ePPO" Application Helped the Armed Forces of Ukraine Shoot Down Iranian Shahed Drones (Video)]' (*ФОКУС*, 3 January 2023) <https://focus.ua/uk/digital/543578-prilozhenie-yeppo-pomoglo-vsu-sbit-iranskie-drony-shahed-video> accessed 17 April 2024.
[28] Interview with Suldin (n 26).
[29] 'єППО - Система Єдиної Протиповітряної [ePPO - Unified Air Defense Complex]' (n 10).
[30] Focus, 'The "ePPO" Application Helped the Armed Forces of Ukraine Shoot down Iranian Shahed Drones' (n 27).
[31] ibid. '"єППО": В "Дії" Появится Новый Сервис, Который Поможет Военным Сбивать Ракеты РФ ["ePPO": A New Service Will Appear in "Diia" That Will Help the Military Shoot Down Russian Missiles]' (*ФОКУС*, 16 September 2022) <https://focus.ua/uk/digital/529595-yeppo-v-diji-poyavitsya-novyy-servis-kotoryy-pomozhet-voennym-sbivat-rakety-rf> accessed 16 April 2024.

'ePPO' to the appearance of this information on the air-defence maps of all relevant military officers, takes between two to seven seconds.[32]

The adoption of advanced technologies, including the 'Diia' and 'ePPO' apps, has significantly enabled Ukraine to offset Russia's conventional military advantages.[33] Reports indicate that Ukrainian forces have effectively used data from the 'ePPO' app to intercept and destroy Russian missiles.[34] The use of these apps demonstrates how civilians, equipped merely with a smartphone, can transition from passive observers to active participants in the conflict, and even integrate into the military's 'kill chain'.[35]

Amid exploring the complex role of Ukrainian civilians using digital tools to support military efforts, the urgent need to reassess their legal status under international law becomes apparent. This evaluation is crucial not only to ensure the 'cardinal' principle of distinction is upheld but also to navigate the nuances of cyber warfare where traditional legal frameworks are often stretched to their limits.

1.2. The Legal Conundrum of Cyber Warfare

International jurisprudence is notably lacking in the realm of cyber warfare, mainly due to the absence of a specialised legal framework and definitive case law. While some state practices are observed, the requisite *opinio juris* for establishing normative customary international law in this context remains largely unestablished. Consequently, the scope and limits of the international legal framework that governs cyber warfare remain unclear and are a matter of various interpretations and disagreements.

This challenge is evident when considering the DPH doctrine. The concept of DPH has always posed a significant challenge in regulating traditional battlefield conduct.

---

[32] Interview with Suldin (n 26).
[33] 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.
[34] Ukrinform, 'Ingenious Mobile App Helps Down First Russian Missile in Ukraine' (*Ukrinform*, 26 October 2022) <www.ukrinform.net/rubric-ato/3601566-ingenious-mobile-app-helps-down-first-russian-missile-in-ukraine.html> accessed 10 January 2024; Focus, 'The "ePPO" Application Helped the Armed Forces of Ukraine Shoot down Iranian Shahed Drones' (n 27); Focus, 'Приложение с ИИ помогло сбить российские ракеты: воспользоваться может любой украинец [An AI Application Helped Shoot Down Russian Missiles: Any Ukrainian Can Use It]' (*ФОКУС*, 27 July 2023) <https://focus.ua/uk/digital/581805-dodatok-iz-shi-dopomig-zbiti-rosijski-raketi-skoristatisya-mozhe-bud-yakij-ukrayinec> accessed 16 April 2024.
[35] Ford, 'Ukraine, Participation and the Smartphone at War' (n 17) 3.

Nonetheless, some scholars have defended the adequacy of the framework provided by IHL and the ICRC guidelines, contending that they reinforce the application of the principle of distinction and, by extension, civilian protection.[36] Despite this, DPH remains one of the most debated concepts to date, and its determination becomes even more complex in the context of cyber operations. Other scholars contend that the legal constructs, designed originally for traditional warfare, do not neatly apply to cyber warfare.[37] This misalignment is often likened to 'pouring new wine into an old bottle'.[38] Despite these complexities, it is imperative to recognise that 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.[39]

IHL is guided by the principle that parties to a conflict are not at liberty to employ any means and methods of warfare; there are limitations which apply.[40] The ICRC firmly asserts that IHL imposes constraints on cyber operations during armed conflicts, just as

---

[36] Nils Melzer, 'The ICRC's Clarification Process on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (2009) 103 Proceedings of the Annual Meeting (American Society of International Law) 299, 306; Nils Melzer, 'Keeping the Balance Between Military Necessity and Humanity – A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities' (2010) 42 New York University Journal of International Law and Politics 831.

[37] Randall Bagwell and Molly Kovite, 'It Is Not Self-Defense: Direct Participation in Hostilities Authority at The Tactical Level' (2016) 224 Military Law Review 1, 2; Michael N Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) 1 Harvard National Security Journal 5; William Boothby, 'Direct Participation in Hostilities – A Discussion of the ICRC Interpretive Guidance' (2010) 1 Journal of International Humanitarian Legal Studies 143; Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (2014) 96 International Review of the Red Cross 189, 190; 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; Christopher E Bailey, 'Cyber Civilians as Combatants' (2016) 8 Creighton International and Comparative Law Journal 4.

[38] American University National Security Law Brief, 'Fall Cyberwar Symposium Panel 1: When Is a Virus a War Crime - Targetability and Collateral Damage Under the Law of Armed Conflict' (2012) 3 National Security Law Brief as cited in Christopher P Toscano, '"Pouring New Wine into Old Bottles": Understanding the Notion of Direct Participation in Hostilities within the Cyber Domain' (2015) 64 Naval Law Review.

[39] 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.

[40] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict 1977 art 35(1).

it restricts the use of any other weapons, means, and methods of warfare, whether they are traditional or newly developed.[41] This stance is supported by the International Court of Justice's (ICJ) *Advisory Opinion on Nuclear Weapons*, which emphasises that the rules of IHL apply to all forms of warfare and all weapons, including those that may be developed in the future.[42] Indeed, IHL treaties are crafted with provisions to adapt to evolving warfare and ensure their applicability to new means and methods of warfare.[43] Thus, the broad application of IHL underscores its object and purpose: to regulate conduct in conflicts that could arise after treaty adoption.

Alongside the ICRC, both the scholarly community and an increasing number of states and international organisations recognise that the existing rules of IHL apply to cyber operations during armed conflicts.[44] Reflecting this consensus, various international and national efforts have aimed to refine the rules that govern armed conflicts in cyberspace. Notably, the Tallinn Manual, compiled by an international group of experts, stands out by grounding its guidelines in *lex lata* without proposing *lex ferenda*.[45] Although non-binding, the Tallinn Manual is significant as it reflects customary IHL.[46] While the drafting of the Tallinn Manual highlighted broad consensus among experts regarding the applicability of IHL to cyberspace, discrepancies remain in how certain IHL rules are interpreted within this domain, with ongoing debates and under-explored areas. As such, even with general agreement on IHL's applicability to cyberspace, questions persist regarding how its core principles should be interpreted and applied in the cyber domain. Before delving into the concept of DPH and assessing the extent to which app users may

[41] ICRC, 'ICRC Position Paper' (n 39) 4.
[42] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* [1996] ICJ Reports (International Court of Justice) [86].
[43] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 36; See also Saint Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight 1868 see where it states that 'The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity'.
[44] 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, 299–300.
[45] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017).
[46] ibid 4.

fall under this category, the following section examines the foundational principle underpinning this discussion: the principle of distinction.

1.3. The Principle of Distinction in IHL

In International Armed Conflicts (IAC), individuals are classified as combatants or civilians, meaning they are either legitimate military targets or protected persons.[47] The critical nature of this principle was underscored by the ICJ's *Advisory Opinion on Nuclear Weapons*, where the Court affirmed that the principle of distinction constitutes a 'cardinal' and 'intransgressible' principle that forms the 'fabric' of IHL.[48]

Under the principle of distinction, an individual identified as a combatant can be targeted without specific provocations unless they are non-combatant members of the armed forces,[49] or are *hors de combat*.[50] Once captured, combatants receive prisoner of war (POW) status,[51] granting them immunity from criminal prosecution under domestic law for their actions.[52] Conversely, a civilian is not only assured of their life, health, and dignity, similar to the protections given to POWs, but also their liberty, which cannot be restricted (through detention) without justification.[53] However, this status is not unconditional; civilians maintain the protection afforded by the international law of armed conflict (LOAC) 'unless and for such time as they take a direct part in hostilities'.[54] This 'bifurcation' between combatants and civilians thus ensures any IAC is waged solely among the combatants of belligerent states, with civilians only losing protected status should they actively participate in hostilities.[55]

---

[47] Nils Melzer explains that these two categories must be 'mutually exclusive, as well as absolutely complementary' to eliminate any ambiguity. See Melzer, 'The Principle of Distinction Between Civilians and Combatants' (n 1) 297.
[48] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* (n 42) [78–79].
[49] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, vol 1 (Cambridge University Press 2005) r 3; Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1949 art 28(2); Convention (III) Relative to the Treatment of Prisoners of War 1949 art 33(1).
[50] Henckaerts and Doswald-Beck (n 49) r 47; Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 41.
[51] Convention (III) Relative to the Treatment of Prisoners of War (n 49).
[52] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 43(2).
[53] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (4th edn, Cambridge University Press 2022) 50.
[54] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 51(3).
[55] Dinstein (n 53) 46.

The principle of distinction is based on the understanding that actions in armed conflict should solely aim to weaken an enemy's military capacity.[56] It requires a clear definition of military objectives, delineating who can be legitimately targeted and who can partake in hostilities without facing repercussions under domestic law.[57] However, the evolution of warfare over the past century has significantly challenged the practical application of this principle.

The customary principle of distinction obligates all parties to a conflict to differentiate between civilians and combatants at all times, a requirement reinforced in treaty law.[58] In IACs, the principle of distinction, encapsulated in Article 48 of the API, compels parties to not only distinguish between civilians and combatants but to also exclusively target combatants.[59] While treaty IHL applicable in Non-International Armed Conflict (NIAC) does not employ the term 'combatant,' the principle of distinction still applies based on the same criteria used to define that category in IAC.[60]

Protecting civilians is a fundamental aspect of the LOAC, yet it does not define the term 'civilian' explicitly. The GCIV does not specify what constitutes a civilian but instead describes 'protected persons'.[61] These are individuals who 'at a given moment and in any manner whatsoever, find themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals'.[62] APII also refers to civilians but also without defining them.[63] It is in the API where we find the first codified definition of a 'civilian'. According to Article 50(1) of this protocol, a civilian is defined negatively, as 'any person who does not belong to one of the categories of persons referred to in Article 4(A)(1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol'. Article 4(A) of the Third Geneva Convention, which outlines the conditions

[56] Saint Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (n 43).
[57] While the term 'military objective' is typically used for objects, Article 52(2) of Additional Protocol I clarifies its applicability to persons as well. See Melzer, 'The Principle of Distinction Between Civilians and Combatants' (n 1) 297 fn 2.
[58] Henckaerts and Doswald-Beck (n 49) r 1.
[59] ibid; Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 51.
[60] Melzer, 'The Principle of Distinction Between Civilians and Combatants' (n 1).
[61] Convention (IV) Relative to the Protection of Civilian Persons in Time of War 1949 art 4.
[62] ibid.
[63] Additional Protocol (II) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict 1977 art 13(1).

for acquiring POW status[64] and reflects customary international law,[65] includes the most widely accepted criteria for combatant status. This article categorises combatants to include members of regular and irregular armed forces as well as inhabitants of a non-occupied territory who spontaneously take up arms to resist the invading forces without time to organise into regular units.[66] Therefore, civilians are those persons who are neither members of the armed forces of a party to the conflict nor participants in a *levée en masse*. Additionally, in situations where there is any doubt, an individual should be presumed to be a civilian.[67]

Today, the very foundation of the principle of distinction is being challenged by the evolving nature of warfare, notably through the increasing involvement of civilians in armed conflicts. This principle operates most effectively when only those with combatant privileges engage in hostilities. However, the trend of civilian participation in combat roles is undermining this critical distinction,[68] and, in the opinion of some scholars, it violates the state's obligation to uphold that principle.[69]

The 'civilianization' of warfare leads to the concept of DPH. Typically, civilians are protected from being directly targeted, but this immunity can be forfeited if their actions align with those of combatants, thus making them legitimate targets. IHL does not preclude any individual from engaging in cyber operations.[70] However, such participants may become legitimate targets of attack, should they be classified as combatants, members of an organised armed group, or civilians directly participating in hostilities. In the present case, individuals using mobile applications to transmit intelligence are, without question, civilians under IHL. As such, this analysis does not engage with the

---

[64] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Kluwer Academic Publishers 1987) para 1677.
[65] Henckaerts and Doswald-Beck (n 49) rr 3, 11, 13.
[66] Convention (III) Relative to the Treatment of Prisoners of War (n 49) art 4(A).
[67] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 50.
[68] Giulio Bartolini, 'The Participation of Civilians in Hostilities' in Michael Matheson and Djamchid Momtaz (eds), *Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts* (Brill Nijhoff 2010); and Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019) as cited in Kubo Mačák, 'Unblurring the Lines: Military Cyber Operations and International Law' (2021) 6 Journal of Cyber Policy 411, 421.
[69] Lindsey Cameron and Vincent Chetail, *Privatizing War: Private Military and Security Companies Under Public International Law* (Cambridge University Press 2013) as cited in Mačák (n 68) 421.
[70] *Tallinn Manual* (n 45) r 86.

concept of combatant status. Rather, the focus lies on whether such individuals may be considered civilian DPH, thereby potentially losing their protection from direct attack for the duration of such participation.

2. The Legal Status of Ukraine's Mobile App Users

2.1. Contextualising Direct Participation in Hostilities

Under IHL, civilians are protected against attacks 'unless and for such time as they take a direct part in hostilities'.[71] The term 'Direct Participation in Hostilities' refers to distinct hostile acts performed by individuals within the framework of combat operations among conflicting parties.[72] Thus, the DPH standard is a 'refinement of the principle of distinction and more immediately of civilian status'.[73]

The notion of DPH has significantly gained traction in modern warfare, especially since the onset of the twenty-first century. This topic was intensely scrutinised within the US-led 'war on terror', which tackled the dilemma of civilians who 'engage[d] in military raids by night, while purporting to be an innocent civilian by day'.[74] Moving forward, it is essential to understand that IHL neither explicitly forbids nor favours civilian DPH. While DPH remains unprohibited under international law, it typically results in legal proceedings under national laws.[75]

---

[71] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 51(3); Additional Protocol (II) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 63) art 13(3).
[72] *ICRC Interpretive Guidance on DPH* (n 1) 45.
[73] Sean Watts, 'Hays Parks and Direct Participation in Hostilities' (*Liebers Institute*, 7 October 2021) <https://lieber.westpoint.edu/hays-parks-direct-participation-hostilities/> accessed 15 May 2024.
[74] Yoram Dinstein, 'Unlawful Combatancy', *International Law and the War on Terror (International Law Studies)*, vol 79 (US Naval War College 2003) 154; See also Richard Baxter, '"So-Called "Unprivileged Belligerency": Spies, Guerillas and Saboteurs' (1951) 28 British Yearbook of International Law 323 Such discourse led to the conceptualisation of a 'third category' that straddles the line between combatants and civilians, labelled as unlawful/unprivileged combatants by some academics. Although the examination of this 'third category' falls outside the purview of this paper, it is pertinent to acknowledge that the term does not feature in any IHL treaties, nor does it confer any recognised legal status or regime. Instead, it characterizes the unlawful nature of participating in armed conflict.
[75] *ICRC Interpretive Guidance on DPH* (n 1) 83–85; Melzer, 'The Principle of Distinction Between Civilians and Combatants' (n 1) 324; Mačák (n 2) 979.

Although the debate around the concept of DPH intensified in the 2000s, its significant normative implications can be traced further back.[76] The concept of DPH, as it is understood today, stems from Article 3 common to the Geneva Conventions, [77] which resonates with the precedents set by the *Hostages Trial* judgement.[78] Presently, this notion is echoed across various provisions of IHL. Firstly, within IAC, DPH characterises the entitlement of combatants to engage in warfare, as specified in Article 43(2) of the API. Secondly, and most relevant to this paper, the term also pertains to the vulnerabilities of non-combatants who opt to engage directly in hostilities. Article 51(3) of the API states that '[c]ivilians shall enjoy the protection […], unless and for such time as they take a direct part in hostilities'.[79] Thirdly, the notion extends to the treatment of individuals captured by an opposing force after having participated in hostilities.[80]

Notwithstanding the significance of accompanying consequences, treaty-based IHL does not define the notion of DPH, and no clear and uniform definition has been developed in state practice either. According to the commentary on additional protocols, 'to restrict this concept to combat and to active military operations would be too narrow, while extending it to the entire war effort would be too broad, as in modern warfare the whole population participates in the war effort to some extent, albeit indirectly'.[81] The commentary further clarifies that in the case of both IAC and NIAC, DPH implies a direct causal relationship between the activity engaged in and its immediate consequences.[82]

---

[76] The formal acknowledgement of DPH can be traced back to 1863 with the Instructions for the Government of Armies of the United States in the Field (Lieber Code) - the first written set of rules that were binding for soldiers - underlining the recognition of the principle from the very inception of codified international humanitarian rules. See Instructions for the Government of Armies of the United States in the Field (Lieber Code) 1863 art 82; The United Nations War Crimes Commission, 'Law Reports of Trials of War Criminals' (1949) VIII <https://tile.loc.gov/storage-services/service/ll/llmlp/Law-Reports_Vol-8/Law-Reports_Vol-8.pdf> accessed 17 April 2024.
[77] *ICRC Interpretive Guidance on DPH* (n 1) 43.
[78] The United Nations War Crimes Commission (n 76) 58.
[79] This clause is echoed in Article 13(3) of the APII relevant to NIACs, underlining a loss of immunity from attack while they participate directly in conflict activities.
[80] Article 43(1) of the API offers a rebuttable presumption of Prisoner of War status to a 'person who takes part in hostilities and falls into the power of an adverse Party' applicable when such a person claims this status, seems entitled to it, or when the adverse party recognises it. Should there be any ambiguity, the detaining power must treat the individual as a POW until a competent tribunal, as outlined in Article 5 of the GCIII, determines their status. There are additional references to DPH within treaty law, such as Article 77 of API, which pertains to the participation of children under 15 years old in hostilities.
[81] Sandoz, Swinarski and Zimmermann (n 64) para 1679.
[82] ibid 1679, 4787.

As highlighted, determining whether an individual directly participates in hostilities is highly contextual and generally requires a case-by-case analysis. The International Criminal Tribunal for the former Yugoslavia (ICTY) in the *Tadić* judgement underscored this point by stating:

> It is unnecessary to define exactly the line dividing those taking an active part in hostilities and those who are not so involved. It is sufficient to examine the relevant facts of each victim and to ascertain whether, in each individual's circumstances, that person was actively involved in hostilities at the relevant time.[83]

This approach allows courts and tribunals to operate without a predefined notion of direct participation, enabling them to assess situations *a posteriori* and on an individual basis.[84] However, the absence of a clear definition poses challenges during armed conflicts, particularly for military commanders as 'it leaves military commanders operating in situations of armed conflict without satisfactory guidance as to the legal standards governing the force used in response to civilian violence',[85] requiring a more definitive explanation or clarification of this concept. This necessity underpins why the ICRC initiated a reflection on this notion. Despite facing criticism,[86] the most useful instrument for addressing this ambiguity is the ICRC's Guidance, which is used with the Tallinn Manual to analyse civilians' actions and determine their legal status. According to the ICRC, for conduct to qualify as DPH, it must satisfy three criteria simultaneously: the threshold of harm, direct causation, and belligerent nexus.[87] That is the case in the context of cyber operations as well.[88] Thus, to provide a comprehensive framework for the analysis, the subsequent subsections focus on these three DPH criteria.

---

[83] *Prosecutor v Dusko Tadic a/k/a/ 'Dule' (Opinion and Judgment)* [1997] International Criminal Tribunal for the Former Yugoslavia (ICTY) (IT-94-1-A) [616].
[84] ibid.
[85] Nils Melzer, 'Civilian Participation in Armed Conflict', *Max Planck Encyclopedias of International Law* (2010) <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1674> accessed 29 April 2024.
[86] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37); Turns (n 39); William Boothby, 'And for Such Time as: The Time Dimension to Direct Participation in Hostilities' (2010) 42 New York University Journal of International Law and Politics 741; Dinstein (n 53).
[87] *ICRC Interpretive Guidance on DPH* (n 1) 46.
[88] *Tallinn Manual* (n 45) r 97 para 5.

2.1.1. Threshold of Harm

Legal Context

The threshold of harm criterion stipulates that 'the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack'.[89]

The classification of action as DPH does not necessitate the actual *materialisation* of harm that reaches a specific threshold; it only requires the objective *likelihood* that such harm will ensue.[90] Consequently, the crucial threshold determination must hinge on 'likely' harm, namely, the harm that can reasonably be anticipated to result from an action under the prevailing circumstances.[91] Therefore, harm of a military nature should be interpreted broadly to include not just the infliction of death, injury, or destruction on military personnel and objects, but any outcome that adversely impacts the military operations or military capacity of a conflict party.[92]

Furthermore, specific acts may still be considered part of hostilities even if they do not directly harm the military operations or capacity of a party to the conflict. In scenarios where such military harm is absent, the act in question must at least be likely to cause death, injury, or destruction.[93] The most unequivocal examples of actions qualifying as DPH, even without military harm, are those directed against civilians and civilian objects.[94]

This perspective has faced criticism from scholars. Schmitt, for instance, questions why the ICRC Guidance insists on harm in scenarios that do not involve civilians or civilian objects.[95] He provides an example, questioning whether forcing inhabitants of a specific ethnic group to leave an occupied area during a conflict where ethnicity plays a role would count as direct participation.[96] A more effective criterion, as Schmitt suggests, would

[89] *ICRC Interpretive Guidance on DPH* (n 1) 46.
[90] ibid 47 (emphasis in original).
[91] ibid.
[92] ibid.
[93] ibid 49.
[94] ibid.
[95] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 28.
[96] ibid.

differentiate actions that are directly linked to the armed conflict from those that are purely criminal.[97]

Additionally, Rule 97 of the Tallinn Manual, while mirroring Article 51(3) of the API, delineates several distinctions from the ICRC Guidance. In contrast to the ICRC's approach, which focuses on the *likelihood* of harm, the Tallinn Manual adopts the criterion of 'intended or actual effect' for assessing the threshold of harm.[98] This means that the standard for harm does not necessarily rely on the objective *likelihood* of harm. Rather, the presence of actual harm or even the *intent* to inflict such harm is sufficient, which represents a lower standard than that advocated by the ICRC. Under Tallinn Manual's standard, as noted by Allan, even a civilian who intends to cause significant harm and launches a poorly executed cyber-attack that ultimately fails to impact the intended target could still lose protection from direct attacks.[99]

Application to Mobile Intelligence App Users

Providing strategic insights into the movements and resources of Russian forces to the Ukrainian military could meet the threshold of harm criterion, as it is *likely* to negatively impact Russian military capabilities. Yet, some scholars argue that most information shared with the military through applications such as 'ePPO' would likely be too generic or insignificant to meet this standard.[100] They assert that the common understanding in traditional kinetic warfare – that 'civilians merely answering questions from passing military personnel' does not constitute DPH[101] – is also relevant to the sharing of digital intelligence.[102]

However, the functionality of the mobile apps Ukraine uses is distinct from the scenario of civilians simply responding to inquiries from transient military personnel. Unlike the relatively passive nature of civilians answering questions from soldiers, applications

---

[97] ibid.
[98] *Tallinn Manual* (n 45) r 97 para 5.
[99] Collin Allan, 'Direct Participation in Hostilities from Cyberspace' (2013) 54 Virginia Journal of International Law 173, 182.
[100] Kubo Mačák and Mauro Vignati, 'Civilianization of Digital Operations: A Risky Trend' (*lawfaremedia.org*, 5 April 2023) <www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend> accessed 9 January 2024.
[101] ICRC and TMC Asser Institute, 'Second Expert Meeting - Direct Participation in Hostilities under International Humanitarian Law' (2004) (Summary Report) 5.
[102] Mačák and Vignati (n 100).

created or adapted for military purposes, such as the 'ePPO' app and the 'eEnemy' feature of the 'Diia' app, involve a more active role. Ukrainian civilians' proactive and independent identification and transmission of information via these apps arguably make them a military sensor. Additionally, the threshold of harm criterion does not necessitate that the provided information actually affects Russian military operations; it requires only an 'objective *likelihood*' of harm, not its 'actual *materialization*'.[103] Thus, by demonstrating that the apps' use by civilians leads to the disclosure of Russian troop locations to the Ukrainian military, there is a basis to argue for an objective likelihood of harm. Indeed, some scholars argue that since qualifying acts encompass any action adversely impacting enemy operations or capacity including providing information that can be immediately used to direct an attack, the use of 'ePPO' clearly meets this criterion.[104] Moreover, considering that the app is designed to hinder Russian attacks by assisting Ukrainian air defences.

Reports indicate that Ukrainian forces have successfully used data from the 'ePPO' app at least in several instances to shoot down missiles and drones. On 22 October 2022, a Russian missile was shot down for the first time with the assistance of the 'ePPO' app after citizens reported it flying in their area.[105] Anti-aircraft units received targeting information in 'a few seconds' and successfully downed the Kalibr missile.[106] The second reported instance of 'ePPO' successful combat use occurred in early 2023, during the shelling on 31 December 2022 and 1 January 2023, when the app helped track and shoot down two Iranian Shahed kamikaze drones.[107] Additionally, on 26 July 2023, during a massive shelling, the 'ePPO' app assisted Ukrainian air defence forces in shooting down 36 Kalibr and X-101 missiles launched by Russia.[108] According to a representative of the app development group, 530 Ukrainians used the app when they saw or heard low-flying Russian missiles.[109] There have also been reported instances of successfully using information shared through the 'Diia' app's 'eEnemy' chatbot.[110] Relying on the evidence

[103] *ICRC Interpretive Guidance on DPH* (n 1) 47 (emphasis in original).
[104] Schmitt and Biggerstaff (n 11).
[105] Ukrinform (n 34).
[106] ibid.
[107] Focus, 'The "ePPO" Application Helped the Armed Forces of Ukraine Shoot down Iranian Shahed Drones' (n 27).
[108] Focus, 'An AI Application Helped Shoot Down Russian Missiles: Any Ukrainian Can Use It' (n 34).
[109] ibid.
[110] Focus, 'єВорог: Украинцы Сняли и Выдали ВСУ Позиции Десятков Вражеских Станций Связи (Фото) [eVorog: Ukrainians the Positions of Dozens of Enemy Communication Stations Were Filmed and

of successful use by Ukrainian forces of information shared via 'ePPO' to shoot down missiles and drones, app usage by civilians in these contexts meets the threshold of harm criterion. This prompts an examination of whether these instances meet the remaining DPH criteria.

2.1.2. Direct Causation

Legal Context

The direct causation criterion stipulates that 'there must be a direct causal link between the act and the harm likely to result either from that act or from a coordinated military operation of which that act constitutes an integral part'.[111]

According to the ICRC, for an act to qualify as 'direct' rather than 'indirect' participation in hostilities, it must have a *'sufficiently close'* causal relationship with the resultant harm.[112] Although ICRC indicates that DPH necessitates a sufficiently close causal connection between the act and the resulting harm, the degree of required causal closeness is uncertain. In the current discussion, direct causation should be interpreted to mean that the harm must be brought about in a single causal step.[113] As such, individual actions that merely build or maintain a party's capacity to inflict harm on its adversary, or those that cause harm only indirectly, do not fall under the DPH scope.[114]

Furthermore, to meet the criterion of direct causation, an act need not be indispensable to the causation of harm. It is neither a necessary nor a sufficient condition.[115] Additionally, the standard of direct causation should be interpreted to include actions that cause harm in conjunction with other acts.[116] More specifically, even if a particular act does not independently cause the required threshold of harm, it would still meet the

Handed over to the Armed Forces of Ukraine (Photo)]' (*ФОКУС*, 12 April 2022) <https://focus.ua/uk/digital/512104-yevorog-ukraincy-snyali-i-vydali-vsu-pozicii-desyatkov-vrazheskih-stanciy-svyazi-foto> accessed 28 July 2024.

[111] *ICRC Interpretive Guidance on DPH* (n 1) 46.

[112] ibid 52 (emphasis added).

[113] ibid 53.

[114] ibid.

[115] ibid 54.

[116] ibid 54–55.

requirement of direct causation if it forms an essential part of a specific and coordinated tactical operation that directly results in such harm.[117]

This viewpoint has also faced criticism.[118] Additionally, it shall be noted that the Tallinn Manual adopts a distinctive stance on the concept of direct causation as well, applying an intent standard similar to its approach to the threshold of harm.[119] The lower standard in the Tallinn Manual, due to its intent-based criterion, leads to distinct legal outcomes in its application, potentially affecting the legal assessment in cyber warfare scenarios.

Schmitt specifically challenges the ICRC Guidance's insistence on harm occurring in a single causal step and criticises the ICRC's classification of the assembly and storage of improvised explosive devices (IED) as indirect participation.[120] Here, an interesting point is that according to the Tallinn Manual's interpretation, the individual who assembles and stores an IED, or its cyber equivalent, would meet the direct causation requirement for DPH since this individual harbours the same harmful intent as the person who arms and detonates the device.[121] Schmitt also uses another example to illustrate his point, particularly relevant to ongoing discussions about the legal status of civilians who use mobile apps to share intelligence information.[122] Schmitt describes a scenario where a civilian collects data on the movements of specific forces and sends this to an intelligence fusion centre. This centre then analyses the data and forwards the insights to a mission planning cell, which may opt to monitor these forces further before deciding on an attack based on factors such as risk and asset availability. Although the causal chain extends over several steps, the initial gathering and reporting of the information, as Schmitt suggests, are critical to any resulting attack, and therefore, should be considered direct participation.[123]

Application to Mobile Intelligence App Users

[117] ibid.
[118] Watkin Kenneth, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance' (2010) 42 New York University Journal of International Law and Politics 641, 658; Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 29–30.
[119] *Tallinn Manual* (n 45) r 97 para 5.
[120] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 29–30.
[121] Allan (n 99) 186.
[122] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 29–30.
[123] ibid; See also Kilovaty (n 37) 13.

Targeting Russian missiles involves a process where civilians collect and share information through a mobile app, which is then processed by Ukrainian military personnel to target enemy forces. Since this process involves multiple individuals, a single act may not independently lead to the necessary threshold of harm. However, the direct causation criterion can still be met if the act 'constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm'.[124]

Some scholars argue that if the civilians using the app are not collecting and sharing information as part of a coordinated effort for a specific attack, their participation would not meet the direct causation criterion.[125] Yet, although the degree of required causal closeness is uncertain, in cases under discussion, this link can be significantly strong. Indeed, ICRC includes the 'transmission of tactical intelligence to attacking forces' as an example of an activity within a collective operation that fulfils the requirement for direct causation.[126] This highlights that the act's role in a broader strategic context is sufficient to meet this standard. Furthermore, the ICRC Guidance clarifies that an act does not need to be indispensable to meet the requirement for direct causation.[127] It points out that 'a person serving as one of several lookouts during an ambush would certainly be taking a direct part in hostilities although his contribution may not be indispensable to the causation of harm'.[128] This underscores the notion that participation in a collective effort, such as cases of mobile app usage by civilians, can meet the criteria for direct causation even if the act alone is not critical to the outcome.

By utilising these apps, Ukrainian civilians effectively become the 'frontline eyes and ears' of the Ukrainian army.[129] Such involvement positions them as active participants in gathering and transmitting crucial intelligence that supports military operations, emphasising their integral role in conflict dynamics. This indicates that their use of the apps is a sufficiently direct cause. Furthermore, as indicated by the co-developer of the 'ePPO' app, the process of sending data through 'ePPO' by Ukrainian civilians to its appearance on the air-defence maps of all relevant military officers takes only two to

[124] *ICRC Interpretive Guidance on DPH* (n 1) 54–55.
[125] Mačák and Vignati (n 100); Mačák (n 2) 974.
[126] *ICRC Interpretive Guidance on DPH* (n 1) 55.
[127] ibid 54.
[128] ibid.
[129] Feldstein (n 33).

seven seconds.[130] In a particular example of 'ePPO's' combat use, Ukraine noted that a Russian missile was targeted a 'few seconds' after receiving data.[131] In this case, a causal relationship is direct, given the limited time to respond to a threat after it is identified.[132]

Moreover, if this time frame was not so constrained, the situation could still satisfy the direct causation criterion, as critics of the ICRC Guidance argue. The scenario outlined by Schmitt should be recalled here.[133] Even though the process Schmitt describes involves several steps – from data collection by a civilian to analysis and potential action by military planners – the initial act of gathering and reporting data is critical for any subsequent military response.[134] This reinforces the argument that such actions, despite the complexities of the decision-making chain, should indeed be considered DPH, aligning with broader interpretations of the direct causation criterion even in less time-sensitive situations.[135] This leads us to examine whether, together with the threshold of harm and direct causation, such activities can meet the third criterion of DPH.

2.1.3. Belligerent Nexus

Legal Context

The belligerent nexus criterion stipulates that 'the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and the detriment of another'.[136]

According to the ICRC, for an act to qualify as DPH, it must not only be '*objectively likely*' to cause harm that satisfies the first two criteria – threshold of harm and direct causation – but it must also be '*specifically designed to do so in support of a party to an armed conflict and to the detriment of another*'.[137] It is important to distinguish belligerent nexus from other concepts such as 'subjective intent' and 'hostile intent', which relate to the mental state of the individual involved. Belligerent nexus, by contrast, concerns the objective

[130] Interview with Suldin (n 26).
[131] Ukrinform (n 34).
[132] Schmitt and Biggerstaff (n 13).
[133] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 29–30.
[134] ibid.
[135] ibid.
[136] *ICRC Interpretive Guidance on DPH* (n 1) 46.
[137] ibid 58 (emphasis in original).

purpose of the act itself.[138] The ICRC uses examples to illustrate this point, noting that even civilians who are coerced into DPH, or children below the lawful recruitment age, may lose their protection against direct attack.[139] Unlike the first two criteria, the Tallinn Manual aligns with the ICRC Guidance regarding the belligerent nexus criterion.[140] However, as explored above, the Tallinn Manual generally applies a lower threshold for deeming civilians as engaged in hostilities via cyber means, thus making them more frequently targetable compared to the ICRC standards.[141]

The belligerent nexus requirement aims to exclude from the DPH definition any activities that, although occurring during an armed conflict and potentially satisfying the threshold of harm, are not related to the conflict itself. Actions such as a bank robbery shootout, unrelated violent crimes, or stealing military equipment for private use, while potentially harmful, would not qualify as DPH.[142] The determination of a belligerent nexus 'must be based on the information reasonably available' to the person making the decision and shall always be inferred from 'objectively verifiable factors'.[143] Consequently, if the actions of a civilian, when evaluated within the context of the circumstances at the time, can be reasonably viewed as being intended to support one party in the conflict by directly inflicting the necessary threshold of harm to another, then such actions establish a belligerent nexus.[144]

Critics highlight substantial disagreement with the requirement that an action must simultaneously harm one party and aid another in the conflict.[145] For instance, they challenge the notion that an Organised Armed Group (OAG) must be affiliated with a recognised party to the conflict to be considered an armed force. Schmitt and others who share his view suggest an alternative framing – 'an act in support or to the detriment of a party' – which, they argue, would accommodate scenarios where an armed group acts against one party without necessarily intending to aid the other.[146] Expanding on this framework, the ICRC also introduces, at least once in its Guidance, the notion of

[138] ibid 59.
[139] ibid 59.
[140] *Tallinn Manual* (n 45) r 97 para 5; See also Kilovaty (n 37) 17; cf Allan (n 99) 188.
[141] Allan (n 99) 186.
[142] *ICRC Interpretive Guidance on DPH* (n 1) 60–61.
[143] ibid 63.
[144] ibid 63–64.
[145] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 33–34.
[146] ibid 34.

alternative rather than cumulative criteria by stating that armed violence which is not intended to harm a party to an armed conflict, *or* which is not designed to support another party, does not qualify as participation in the hostilities occurring between these parties.[147] Despite this, the ICRC continues to follow a path that requires cumulative criteria.

As suggested by the ICRC, when these three criteria – threshold of harm, direct causation, and belligerent nexus – are applied together, they enable a reliable distinction to be made. This distinction separates activities that qualify as DPH from those that, although they occur during an armed conflict, are not part of the actual conduct of hostilities.[148] As a result, the latter activities do not lead to a loss of protection against direct attack.[149] Furthermore, if there is any ambiguity regarding whether a civilian's conduct meets these three DPH criteria, the ICRC Guidance adopts a presumption of non-participation.[150] This means that the civilians retain their protection from attack until proven otherwise, ensuring that the principles of distinction and proportionality, which are central to IHL, are upheld.[151]

Application to Mobile Intelligence App Users

Regarding the fulfilment of the belligerent nexus criterion as previously discussed, much depends on the specific features of the app and the nature of the information disseminated. While reporting military actions to aid one conflict party and harm another meets the belligerent nexus criterion, the same action designed for different purposes does not.[152] Notably, when evaluating belligerent nexus, the objective purpose of an act rather than subjective motives shall be assessed.[153]

In specific cases where Ukrainian citizens use applications such as 'ePPO', the belligerent nexus is met, as scholars suggest.[154] According to Maurer, the 'ePPO' app 'has no other functionality or purpose than to identify, track, and transmit data about enemy weapons

[147] *ICRC Interpretive Guidance on DPH* (n 1) 59 (emphasis added).
[148] ibid 64.
[149] ibid.
[150] ibid 75–76.
[151] ibid.
[152] Mačák (n 2) 975–976.
[153] *ICRC Interpretive Guidance on DPH* (n 1) 59 fn 150.
[154] Schmitt and Biggerstaff (n 11).

of war in real time'.[155] He further notes, even a rifle, which can be used for hunting or self-defence, has secondary purposes. In contrast, the 'ePPO' app lacks any such secondary functionality.[156] Consequently, since the app was specifically created to assist Ukrainian armed forces in defending against Russian attacks, it can be argued that the belligerent nexus criterion is satisfied.

The same argument can be made regarding the 'Diia' app's 'eEnemy' chatbot. While the 'Diia' app possesses various functionalities, the 'eEnemy' feature was specifically integrated in response to the ongoing armed conflict.[157] This adaptation enables Ukrainian civilians to function as 'spotters' by using the chatbot to relay information about enemy movements, activities, and potential collaborators to the Ukrainian military.[158] Designed to directly communicate pertinent information for targeting purposes, the use of the 'eEnemy' chatbot typically supports Ukraine's war efforts while detrimentally affecting Russia's. Consequently, in this case as well, the belligerent nexus criterion is fulfilled.

Having established that the use of mobile apps by civilians can potentially satisfy all three DPH criteria, it becomes crucial to examine the temporal scope of DPH. While the three criteria determine whether a civilian is directly participating in hostilities, the duration of this participation, implicitly linked to DPH, is essential for upholding the principle of distinction. Article 51(3) of API states that civilians are protected against attacks 'unless and for such time as they take a direct part in hostilities'. Therefore, it is important to discuss the duration of 'for such time' and its impact on the legal protections afforded to civilians. The next section delves into the timing of these actions, focusing on when participation begins and ends, and how this affects their classification under DPH and the associated legal protection.

---

[155] Dan Maurer, 'A State's Legal Duty to Warn Its Own Civilians on Consequences of Direct Participation in Hostilities' (*Lieber Institute*, 21 February 2023) <https://lieber.westpoint.edu/states-legal-duty-warn-civilians-consequences-direct-participation-hostilities/> accessed 12 April 2024.
[156] ibid.
[157] 'Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог [Help the Armed Forces of Ukraine Destroy the Occupier: the Ministry of Digital Transformation Launches the eEnemy Chatbot]' (n 24).
[158] ibid.

2.2. Temporal Scope of Direct Participation in Hostilities

The ICRC raises three main issues concerning DPH: identifying who is a civilian, defining what constitutes direct participation, and interpreting the meaning of 'for such time'. The first two issues have been addressed above. The last issue is even more complex and contentious. The analysis indicates that civilians using mobile apps such as 'ePPO' and 'Diia' may meet all three criteria, constituting DPH. Consequently, this results in the loss of legal protection against direct attacks typically afforded to civilians. In this context, the 'for such time' limitation, which was confirmed as customary in the *Targeted Killings case,*[159] becomes particularly challenging.

The concept of a temporal dimension to the DPH is not a recent development. Already the Lieber Code addressed this concept in Article 82, which states that persons:

> [W]ho commit hostilities, […] without being part and portion of the organized hostile army, and without sharing continuously in the war, but who do so with intermitting returns to their homes and avocations or with the occasional assumption of the semblance of peaceful pursuits, divesting themselves of the character or appearance of soldiers […] if captured, are not entitled to the privileges of prisoners of war, but shall be treated summarily as highway robbers or pirates.

As pointed out by Boothby, the mention of 'intermitting returns' not only highlights Lieber's recognition of the 'revolving door' dilemma – where civilians may strategically enter and exit participation in hostilities to manipulate protections while acting as *de facto* combatants on the battlefield – but also his rejection of the intermittent protection this might imply.[160] It can be argued that Lieber's interpretation suggests that 'returns to the home' are merely pauses in a continuous chain of hostilities.

The blurred line between civilians and combatants amplifies a critical issue within DPH, specifically regarding the duration encompassed by 'for such time'. This principle stipulates that the loss of protection only applies during the period of direct participation.

---

[159] *Public Committee Against Torture in Israel v Government of Israel* [2006] Supreme Court of Israel HCJ 769/02 [38].
[160] Boothby (n 86) 744.

However, what amounts to this duration? Do civilians only lose their protections when actively using the app, potentially resulting in a fleeting change in status due to sporadic participation? Or should these civilians be considered legitimate targets until they definitively cease their involvement in hostilities, allowing for targeting even between instances of participation? This section delves into the importance of pinpointing precisely when the loss of protection begins and ends. Initially, it examines the duration of DPH as it is understood in the current framework regulating physical DPH, including preparation, deployment, and return, and how this can be tailored to the cyber context. Then, it discusses the 'revolving door' phenomenon and its implications.

2.2.1. Duration of Participation

2.2.1.1. Preparation

According to the ICRC, the notion of DPH encompasses not only the immediate execution phase of a specific act that meets the three criteria of the threshold of harm, direct causation, and belligerent nexus but also the preparatory measures and the movement to and from the execution site, provided these actions are integral to that specific act or operation.[161]

As indicated in the ICRC Guidance, preparatory measures amounting to DPH correspond to what Article 44(3) of API considers as 'military operation preparatory to an attack'.[162] According to the commentary of this paper, this encompasses 'any action carried out with a view to combat', yet the ICRC Guidance narrows down this concept.[163] This being said, the ICRC considers preparatory actions intended to execute a *specific* hostile act as DPH. In contrast, preparatory actions aimed at building the *general* ability to carry out undefined hostile acts do not qualify as such.[164] This determination is criticised by scholars. For example, as Schmitt notes, the ICRC Guidance does not consider the assembly of the IED as direct participation as the ICRC posits that an individual who gathers materials and constructs an IED engages in direct participation only during the final steps required to activate it. However, the alternative perspective shared by Schmitt

[161] *ICRC Interpretive Guidance on DPH* (n 1) 65.
[162] ibid.
[163] Sandoz, Swinarski and Zimmermann (n 64) para 1692.
[164] *ICRC Interpretive Guidance on DPH* (n 1) 66.

suggests that the entire process – from acquiring the necessary materials to building and positioning the device – should be recognised as preparatory actions that fall within the time frame of direct participation.[165]

Moreover, it is not required for qualification as direct participation that a preparatory measure takes place immediately before (temporal proximity) or close to the location (geographical proximity) of a specific hostile act, nor must it be indispensable for its execution.[166] Activities such as the loading of bombs onto an aeroplane for a direct attack on military targets in a conflict zone by the ICRC are identified as the preparation that constitutes DPH.[167] Other preparatory actions that also meet the criteria for DPH include equipping, instructing, and transporting personnel; *gathering intelligence;* as well as the preparation, transport, and placement of weapons and equipment when these actions are specifically aimed at executing a hostile act.[168] The ICRC Guidance suggests that civilians may be targeted only during 'recognizable and proximate preparations', using the example of loading a gun to illustrate this point.[169] Critics, however, contend that this example fails to capture the complexities of various forms of participation in modern warfare, potentially leading to an overly narrow interpretation of DPH.[170]

2.2.1.2. Deployment and Return

Regarding deployment and return, as suggested by the ICRC, deployment and return surrounding a specific DPH act are integral parts of that act if they involve geographic movement necessary for its execution.[171] However, this understanding is also not without a critique.[172] In such situations, deployment begins when an individual physically moves towards carrying out a specific operation, and it ends upon return when the individual has physically disengaged by, for instance, putting away any weapons or equipment used.[173] On the one hand, some contend that preparatory activities undertaken before actual deployment might already qualify as DPH.[174] Hence, it appears justifiable to view

[165] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 37.
[166] *ICRC Interpretive Guidance on DPH* (n 1) 66.
[167] ibid.
[168] ibid (emphasis added).
[169] ibid 67 (fn 182).
[170] Boothby (n 86) 748.
[171] *ICRC Interpretive Guidance on DPH* (n 1) 67.
[172] Boothby (n 86) 750–751.
[173] *ICRC Interpretive Guidance on DPH* (n 1) 67.
[174] Boothby (n 86) 750.

any deployment specifically intended to prepare for an action that constitutes direct participation as itself a form of direct participation.[175] On the other hand, it is also argued that physical separation from the act such as laying down, storing or hiding the weapons shall properly be regarded not as concluding participation but rather as preparatory to the next act of DPH.[176] However, the classification of these movements as direct participation depends on several factors that must be carefully determined based on the circumstances at hand.[177] According to the ICRC, in scenarios where a hostile act does not require geographic movement, such as with cyberattacks or remote-controlled weaponry, direct participation is limited only to the time directly involved in executing the act and any essential preparatory measures.[178]

In applying the concepts of preparation, deployment and return to the cyber context, specifically app usage, preparatory measures are unlikely to extend to civilians who are prepared to report, as merely having an app installed does not suffice for DPH.[179] While it is argued that 'for such time' duration should be interpreted broadly,[180] for civilians to meet DPH criteria, they should, at least, be actively seeking out Russian threats, if not already reporting them. Consequently, the ICRC's narrow interpretation would end the DPH period once the individual stops actively searching for Russian systems to report or has completed reporting one.[181]

Examining the beginning and end of the DPH period highlights the complexity of the temporal scope, especially in the cyber context. This leads us to a discussion of the controversial 'revolving door' phenomenon when a civilian repeatedly loses and regains immunity by engaging in hostilities, stopping such activities, and then re-engaging, thereby raising complex legal issues. Such scenarios raise contentious legal issues regarding the continuous protection of civilians and the challenges faced by military forces in accurately identifying civilian DPH. The following subsection investigates the

[175] ibid 751.
[176] ibid.
[177] *ICRC Interpretive Guidance on DPH* (n 1) 67.
[178] ibid 68.
[179] Schmitt and Biggerstaff (n 11); Olejnik (n 24).
[180] Dinstein (n 53) 202.
[181] *ICRC Interpretive Guidance on DPH* (n 1) 67.

'revolving door' phenomenon and its implications, further elucidating the intricacies of applying IHL to modern cyber warfare.

2.2.2. The 'Revolving Door' and Its Implications

The ICRC Guidance recognises the existence of the 'revolving door' phenomenon and asserts that it is an 'integral part, not a malfunction, of IHL'.[182] It also acknowledges that the 'revolving door' concept complicates the ability of opposing armed forces to effectively counteract the direct participation of civilians in hostilities.[183] Yet, as it highlights, this phenomenon 'remains necessary to protect the civilian population from erroneous or arbitrary attack and must be acceptable for the operating forces or groups as long as such participation occurs on a merely spontaneous, unorganized or sporadic basis'.[184]

Regarding the duration of the loss of protection because of DPH, ICRC concludes that:

> Civilians lose protection against direct attack *for the duration of each specific act* amounting to direct participation in hostilities, whereas members of organized armed groups belonging to a non-State party to an armed conflict cease to be civilians […], and lose protection against direct attacks, for as long as they assume their continuous combat function.[185]

With this explanation, the ICRC maintains that continuous deprivation of protection should only apply to those with a *continuous combat function*, arguing that this is the sole basis for such ongoing loss of protection. In contrast, civilians who engage in DPH lose their protection only during the time they are actively involved:

> As the concept of direct participation in hostilities refers to specific hostile acts, IHL restores the civilian's protection against direct attack each time his or her engagement in a hostile act ends. Until the civilian in question again engages in a specific act of direct participation in hostilities, the use of force against him

[182] ibid 70.
[183] ibid 71.
[184] ibid.
[185] ibid 70 (emphasis added).

> or her must comply with the standards of law enforcement or individual self-defence.[186]

Along with this explanation, the guidance notes commentary of API in the footnotes to further elaborate that 'If a civilian participates directly in hostilities, it is clear that he will not enjoy any protection against attacks for as long as his *participation* lasts. Thereafter, as he no longer presents any danger for the adversary, he may not be attacked'.[187] Critics often point out that this perspective contradicts the position of the ICRC Guidance while acknowledging that the commentary provides a more thorough approach.[188] However, as Boothby notes, the concept of danger linked to potential civilian DPH does not encompass all potential scenarios, particularly those not involving civilians directly engaging in violence.[189] This suggests the debate should focus more on the individual's decision to participate, rather than attempting to justify the response based on the perceived danger.[190]

Many critics have argued that the ICRC Guidance's standards for determining the duration of the loss of protection are too restrictive.[191] Scholars challenge the presence of this concept within customary IHL, arguing instead that civilians who engage directly in hostilities temporarily relinquish their protected status, thereby dismissing the notion of a protective 'revolving door'.[192] Furthermore, they propose that recurrent participation may establish the continuous engagement of an individual, rendering them perpetually vulnerable to attack.[193] For instance, Schmitt who has consistently advocated for a more liberal interpretation of DPH argues that the '[a]pplication of the continuous combat function criterion […] badly distorts the military necessity-humanitarian balance of IHL'[194] and '[a]part from the structural distortion of the revolving door phenomenon, the

[186] ibid 71.
[187] ibid (fn 192).
[188] Boothby (n 86) 756–757.
[189] ibid 756.
[190] ibid 756–757.
[191] Schmitt, '"Direct Participation in Hostilities" and 21st Century Armed Conflict' (n 4); Schmitt, 'DPH by Private Contractors or Civilian Employees' (n 4); Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37); Michael N Schmitt, 'The Law of Cyber Targeting' (2018) 68 Naval War College Review; Schmitt and Biggerstaff (n 11); Boothby (n 86); Wallace, Reeves and Powell (n 1); Dinstein (n 53).
[192] Boothby (n 86) 762–764.
[193] Schmitt, '"Direct Participation in Hostilities" and 21st Century Armed Conflict' (n 4); Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37); Boothby (n 86); Dinstein (n 53).
[194] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 23.

approach makes no sense from a military perspective'.[195] Boothby claims that 'by limiting continuous loss of protection to members of organized armed groups […] the ICRC gives regularly participating civilians a privileged, unbalanced, and unjustified status of protection'.[196] Dinstein also declares that in defining the specific time frame during which a civilian is directly participating in hostilities 'it is necessary to go as far as is reasonably required both 'upstream' and 'downstream' from the actual engagement'.[197] He further asserts that civilians who sporadically engage in hostilities 'must lose protection from attack even during the intermediate periods punctuating military operations'.[198]

While the ICRC's position is ideal and intends to maximise civilian protection, it lacks practical application. The ease with which civilians can transmit tactical information using smartphone apps such as 'ePPO' and 'Diia' underscores the 'revolving door' dilemma that some countries refuse to accommodate.[199] In such scenarios, the lack of a universally agreed-upon position on the temporal scope of DPH affirms the complexities of applying IHL in modern conflicts. Currently, the approach a state adopts towards the 'revolving door' issue could significantly extend the period during which a civilian is vulnerable to targeting. This has profound implications for the implementation of IHL, as it reflects varied interpretations and practices among states.[200] In the case of the Russia-Ukraine armed conflict, the refusal to acknowledge the 'revolving door' phenomenon not only exposes civilians to increased risk but could also potentially legitimise Russian attacks that might otherwise be prohibited by the rules of proportionality and feasible precautions.[201]

Moreover, given the operational realities of armed conflicts, parties often make determinations based on partial information, and IHL acknowledges the inevitability of reasonable factual mistakes.[202] Specifically, the Rome Statute establishes that a mistake

---

[195] ibid 38.
[196] Boothby (n 86) 743.
[197] Dinstein (n 53) 202.
[198] ibid 203.
[199] The U.S. Department of Defense's Office of the General Counsel, *Law of War Manual* (2015) s 5.8.4.2.
[200] Schmitt and Biggerstaff (n 11); Olejnik (n 24); Mačák and Vignati (n 100).
[201] Schmitt and Biggerstaff (n 11).
[202] A party in the conflict is limited to making determinations about an individual's participation on the opposing side based solely on the information from all available sources that it can reasonably interpret at the time the determination is made. See 'Ratification of the Additional Protocols by the United Kingdom of Great Britain and Northern Ireland' (1998) 322 International Review of the Red Cross s (c) as cited in Boothby (n 86) 766.

of fact shall be a ground for excluding criminal responsibility when it negates the mental element required by the crime.[203] For instance, in the case of the wilful killing of civilians, the offence requires that the perpetrator be aware of the factual circumstances that established the protected status of the individuals involved.[204] Thus, a reasonable mistake regarding the 'for such time' aspect of direct participation could absolve a combatant of criminal responsibility if they mistakenly believed the individual was still actively participating in hostilities at the time of the attack.[205] This links to the above discussion about 'revolving door' interpretation and even raises concerns about the potential for exploiting the notion of reasonable mistakes.

This scenario becomes even more complex considering that in the fog of war, it is conceivable that any civilian with a smartphone could be seen as a potential informant, leading to the possibility that a combatant might target any such individual under the assumption they are relaying critical information to the enemy.[206] For example, there have been reported instances where Russian troops targeted civilians simply for possessing smartphones.[207] These troops were given orders to engage anyone suspected of transmitting information about troop locations, without distinction between combatants and civilians, operating under the rule that possession of a smartphone alone justified engagement.[208] Yet, a cell phone is a dual-use item that may be employed for activities completely unrelated to an armed conflict, unlike more specialised equipment that could be interpreted as exclusively used for military observation in a conflict setting.[209]

---

[203] Rome Statute of the International Criminal Court (n 21) art 32(1).
[204] International Criminal Court, 'Elements of Crime' art 8 (2)(b)(i), 8 (2)(e)(i) as cited in Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 39.
[205] Schmitt, 'The Interpretive Guidance: A Critical Analysis' (n 37) 39.
[206] Mačák and Vignati (n 100); 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; Pontus Winther, 'Military Influence Operations & IHL: Implications of New Technologies' (*Humanitarian Law & Policy*, 27 October 2017) <https://blogs.icrc.org/law-and-policy/2017/10/27/military-influence-operations-ihl-implications-new-technologies/> accessed 11 May 2024.
[207] Judah (n 13); Ford, 'The Smartphone as Weapon - Part 3' (n 17); Ford, 'Ukraine, Participation and the Smartphone at War' (n 17).
[208] Pleitgen, Otto and ottasová (n 18).
[209] Roman Horbyk, '"The War Phone": Mobile Communication on the Frontline in Eastern Ukraine' (2022) 3 Digital War 9.

It is also noteworthy that scholars highlight the accountability of individuals who, through their repeated actions, subject themselves to the risk of direct attack.[210] They argue that, in the absence of an obvious disengagement, the burden falls on these individuals if the opposing side misinterprets their current status in the conflict.[211] Should an error occur where a civilian previously involved in direct participation is attacked after ceasing to participate, as Boothby argues would constitute a wrongful act but not a criminal one.[212] The responsibility for any failure of reasonable precautions to detect a cessation in hostile activities ultimately lies with the individual who once engaged directly in hostilities.[213] In light of these complexities, the debate over the 'revolving door' phenomenon underscores the urgent need for clear, universally agreed-upon standards in IHL to address the challenges posed by modern cyber warfare.

Conclusion

The analysis revealed that civilians using mobile apps such as 'ePPO' and 'Diia' for intelligence sharing may meet the DPH criteria. This is evidenced by reported instances where Ukrainian forces successfully used information provided by citizens through these apps to target and shoot down Russian missiles and drones. These actions demonstrate that providing strategic insights into the movements and resources of Russian forces meets the threshold of harm criterion, as it negatively impacts Russian military capabilities. These individuals not only meet the threshold of harm criterion but also satisfy the required direct causation and belligerent nexus criteria. The rapid response time by Ukrainian forces after receiving information through these apps illustrates a direct causal relationship between the civilians' actions and the military's targeting decisions. This positions civilians as active participants who significantly contribute to military operations by transmitting vital intelligence. Furthermore, the belligerent nexus is straightforward to establish, given that the 'ePPO' and 'Diia's' 'eEnemy' chatbot, are designed specifically for identifying, tracking, and reporting enemy military assets in real-time. Consequently, these apps' exclusive military-focused functions align with the DPH

[210] Boothby (n 86) 760.
[211] ibid.
[212] ibid 761.
[213] ibid.

belligerent nexus criterion. Therefore, individuals using these mobile apps are classified as civilian DPH, thereby temporarily losing their protected status under IHL.

This classification naturally raises important questions about the legal consequences and implications of such a determination. The intricate nature of the temporal scope of DPH highlights the need for IHL to be applied in a nuanced manner. Although the ICRC framework aims to maximise civilian protection, its practical application often falls short, especially when some states refuse to accommodate the 'revolving door' phenomenon. The current lack of consensus and varied interpretations of this concept complicate efforts to safeguard civilians while maintaining operational effectiveness in armed conflicts. As revealed, currently, the approach a state adopts towards the 'revolving door' issue can significantly extend the period during which a civilian is vulnerable to targeting. Consequently, it is crucial to develop clearer guidelines on the conditions under which civilians lose and regain protection to uphold the principle of distinction and avoid arbitrary attacks. While the Tallinn Manual takes an important first step in applying IHL to cyber warfare, it generally sets a lower threshold for classifying civilians as engaged in hostilities via cyber means. This approach increases the frequency with which civilians become targetable compared to traditional warfare, further highlighting the operational challenges and legal ambiguities in current frameworks.

It must be acknowledged that written law often lags behind technological advancements. While IHL treaties are designed with provisions that intend to adapt to evolving warfare and ensure their applicability to new means and methods of combat, traditional legal frameworks are increasingly stretched to their limits by the complexities of cyber warfare. Although mechanisms such as the 'Martens Clause' offer a safety net for scenarios not explicitly covered by existing IHL rules,[214] the current legal framework fails to provide adequate protection against challenges posed by cyber warfare. This gap underscores the urgent need for clearer and more comprehensive regulations.

[214] 'Martens Clause' (principle of humanity), which has acquired the status of a customary rule reads: 'Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of public conscience'. See Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land 1899.

As the nature of warfare evolves, so too must the legal frameworks that govern it, ensuring they are robust enough to tackle the challenges posed by contemporary conflict dynamics. While the ideal solution might be a new treaty addressing cyber warfare, political and practical challenges make this unlikely in the near term. Some scholars have suggested that adopting another additional protocol could be feasible.[215] However, while such instruments may offer flexibility and be easier to negotiate, without state ratification, they lack binding force and therefore may not effect meaningful change. Furthermore, the process of ratification is itself fraught with political challenges, as differing interpretations of existing laws are often deeply connected to these political issues. Thus, this paper argues that the principal issue in the current *lex lata* is not the absence of dedicated laws but rather the lack of consensus on their interpretation.

Therefore, this paper contends that the most practical and necessary solution is the development of a comprehensive state practice for interpreting existing IHL rules in the context of cyber warfare. This approach requires states to engage actively in dialogues to standardise interpretations and applications of IHL to cyber operations in armed conflicts. States play a crucial role in developing laws applicable to cyber warfare. However, as existing practice suggests, they maintain vague stances to retain operational flexibility, which hinders the advancement of existing norms. By building consensus on key issues such as the criteria and duration for DPH in cyberspace, states can create a more predictable and coherent framework. As states develop and document their practices, these can evolve into customary international law, contributing to the formation of binding norms through consistent actions taken out of a sense of legal obligation.

It is noteworthy that, as the research revealed, Ukraine is encouraging its citizens to join the 'IT Army' and use mobile apps to share intelligence without informing them of possible consequences,[216] despite knowing that such activities pose dangers to

[215] Peter Pascucci, 'Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution' (2017) 26 Minnesota Journal of International Law.
[216] There have been numerous instances of such encouragement. For example, see Focus, 'The "ePPO" Application Helped the Armed Forces of Ukraine Shoot down Iranian Shahed Drones' (n 27); Focus, 'єВорог' (n 110); 'We Are Creating an IT Army - Tweet by Mykhailo Fedorov' (n 6).

civilians.[217] While international law does not explicitly state a warning requirement,[218] the involvement of civilians in military operations arguably violates the state's obligation to uphold the principle of distinction.[219] Existing law suggests that parties to the conflict have a general duty to protect civilians, which includes taking *active measures* to safeguard them.[220] This duty is reinforced by the requirements to take constant care as well as all necessary precautions to protect civilians against the dangers resulting from military operations.[221] Although some states interpret all feasible precautions as not requiring 'everything that is capable of being done',[222] such states still recognise that they include 'practicable', 'reasonable', 'due' and 'necessary' precautions, which can accommodate warning duty.[223]

While in Ukraine, such warnings might not significantly alter the population's willingness to support their military, given the strong national commitment to defence, future research should explore the state's responsibility to warn civilians about the potential consequences of such engagement. This includes examining the state's obligation to provide warning, how states can effectively implement such measures, and the legal ramifications of failing to do so.

---

[217] Дія, 'Побачили С400, С300, Буратіно/Солнцепьок Чи Іскандер? Повідомте в Чатбот єВорог [Have You Seen the S400, S300, Pinocchio/Solntsepyok or Iskander? Report to the eEnemy Chatbot] (Telegram Post)' (*Telegram*, 8 February 2023) <https://t.me/diia_gov/2689> See where it is states 'Be sure to take care of your own safety! Carefully remove and clean your phone after using the chatbot. It is necessary to delete shots of occupants or equipment and correspondence with the chatbot. It could save your life' (translated).

[218] Maurer (n 155); Interview with Dan Maurer, 'NSL Unscripted | Episode 6 - LTC Dan Maurer Discusses States Encouraging Direct Participation in Hostilities' (18 April 2023) <https://tjaglcs.army.mil/nsl-unscripted> accessed 1 August 2024; Winther and Nilsson (n 14) 6.

[219] Cameron and Chetail (n 69) 104 as cited in Mačák (n 68) 421.

[220] Winther (n 206) (emphasis in original).

[221] Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (n 40) art 57(1), 58(c); Winther and Nilsson (n 14) 7.

[222] Robert Lawless, 'The U.S. Legal Obligation to Take Precautions to Minimize Civilian Harm' (*Lieber Institute*, 18 February 2022) <https://lieber.westpoint.edu/us-legal-obligation-precautions-minimize-civilian-harm/> accessed 1 August 2024.

[223] The U.S. Department of Defense's Office of the General Counsel (n 199) para 5.3.3.1.

Bibliography

Allan C, 'Direct Participation in Hostilities from Cyberspace' (2013) 54 Virginia Journal of International Law 173

American University National Security Law Brief, 'Fall Cyberwar Symposium Panel 1: When Is a Virus a War Crime - Targetability and Collateral Damage Under the Law of Armed Conflict' (2012) 3 National Security Law Brief

Bagwell R and Kovite M, 'It Is Not Self-Defense: Direct Participation in Hostilities Authority at The Tactical Level' (2016) 224 Military Law Review 1

Bailey CE, 'Cyber Civilians as Combatants' (2016) 8 Creighton International and Comparative Law Journal 4

Bartolini G, 'The Participation of Civilians in Hostilities' in Michael Matheson and Djamchid Momtaz (eds), *Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts* (Brill Nijhoff 2010)

Baxter R, '"So-Called "Unprivileged Belligerency": Spies, Guerillas and Saboteurs' (1951) 28 British Yearbook of International Law 323

Boothby W, 'And for Such Time as: The Time Dimension to Direct Participation in Hostilities' (2010) 42 New York University Journal of International Law and Politics 741

——, 'Direct Participation in Hostilities – A Discussion of the ICRC Interpretive Guidance' (2010) 1 Journal of International Humanitarian Legal Studies 143

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

Cameron L and Chetail V, *Privatizing War: Private Military and Security Companies Under Public International Law* (Cambridge University Press 2013)

Dinstein Y, 'Unlawful Combatancy', *International Law and the War on Terror (International Law Studies)*, vol 79 (US Naval War College 2003)

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

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

Focus, 'єВорог: Украинцы Сняли и Выдали ВСУ Позиции Десятков Вражеских Станций Связи (Фото) [eVorog: Ukrainians the Positions of Dozens of Enemy Communication Stations Were Filmed and Handed over to the Armed Forces of Ukraine (Photo)]' (*ФОКУС*, 12 April 2022) <https://focus.ua/uk/digital/512104-yevorog-ukraincy-snyali-i-vydali-vsu-pozicii-desyatkov-vrazheskih-stanciy-svyazi-foto> accessed 28 July 2024

——, 'Приложение "єППО" Помогло ВСУ Сбить Иранские Дроны Shahed (Видео) [The "ePPO" Application Helped the Armed Forces of Ukraine Shoot Down Iranian Shahed Drones

(Video)]' (*ФОКУС*, 3 January 2023) <https://focus.ua/uk/digital/543578-prilozhenie-yeppo-pomoglo-vsu-sbit-iranskie-drony-shahed-video> accessed 17 April 2024

——, 'Приложение с ИИ помогло сбить российские ракеты: воспользоваться может любой украинец [An AI Application Helped Shoot Down Russian Missiles: Any Ukrainian Can Use It]' (*ФОКУС*, 27 July 2023) <https://focus.ua/uk/digital/581805-dodatok-iz-shi-dopomig-zbiti-rosijski-raketi-skoristatisya-mozhe-bud-yakij-ukrayinec> accessed 16 April 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

——, 'The Smartphone as Weapon Part 2: The Targeting Cycle in Ukraine' (2022) <www.academia.edu/76011845/The_Smartphone_as_Weapon_part_2_the_targeting_cycle_in_Ukraine> accessed 30 April 2024

——, 'The Smartphone as Weapon Part 3: Participative War, the Laws of Armed Conflict and Genocide by Smartphone' (2022) <www.academia.edu/77205229/The_Smartphone_as_Weapon_part_3_participative_war_the_laws_of_armed_conflict_and_genocide_by_smartphone> accessed 30 April 2024

——, 'Ukraine, Participation and the Smartphone at War' [2023] Political Anthropological Research on International Social Sciences 1

Ford M and Hoskins A, *Radical War: Data, Attention and Control in the Twenty-First Century* (1st edn, Oxford University Press 2022)

Gaukema L, 'GovTech Incubator Launched at the 2023 Digital Government Summit' (*Joinup*, 30 May 2023) <https://joinup.ec.europa.eu/interoperable-europe/news/govtech-incubator-launched-2023-digital-government-summit> accessed 7 January 2024

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

Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law*, vol 1 (Cambridge University Press 2005)

Horbyk R, '"The War Phone": Mobile Communication on the Frontline in Eastern Ukraine' (2022) 3 Digital War 9

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

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

——, '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 and TMC Asser Institute, 'Second Expert Meeting - Direct Participation in Hostilities under International Humanitarian Law' (2004) (Summary Report)

Ilyushina M, ‘Russia Asks Citizens to Use New App to Report Drones and Other Attacks’ *Washington Post* (21 September 2023) <www.washingtonpost.com/world/2023/09/20/russia-app-drone-citizens-war/> accessed 7 January 2024

International Criminal Court, ‘Elements of Crime’

Interview with Dan Maurer, ‘NSL Unscripted | Episode 6 - LTC Dan Maurer Discusses States Encouraging Direct Participation in Hostilities’ (18 April 2023) <https://tjaglcs.army.mil/nsl-unscripted> accessed 1 August 2024

Interview with Gennady Suldin, ‘Seven Seconds from Smartphone to Air Defense Maps: How One App Unites Millions to Shoot Down Russian Missiles’ (3 April 2023) <https://rubryka.com/en/article/seven-seconds-to-air-defense-maps/> accessed 15 April 2024

‘ITU Datahub’ <https://datahub.itu.int/data/?e=UKR> accessed 27 September 2025

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

Judah T, ‘How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders’ *Financial Times* (10 April 2022) <www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8> accessed 9 January 2024

Kenneth W, ‘Opportunity Lost: Organized Armed Groups and the ICRC “Direct Participation in Hostilities” Interpretive Guidance’ (2010) 42 New York University Journal of International Law and Politics 641

Kilovaty I, ‘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

Lauterpacht H, ‘The Law of Nations and the Punishment of War Crimes’ (1944) 21 British Yearbook of International Law 58

Lawless R, ‘The U.S. Legal Obligation to Take Precautions to Minimize Civilian Harm’ (*Lieber Institute*, 18 February 2022) <https://lieber.westpoint.edu/us-legal-obligation-precautions-minimize-civilian-harm/> accessed 1 August 2024

Mačák K, ‘Unblurring the Lines: Military Cyber Operations and International Law’ (2021) 6 Journal of Cyber Policy 411

——, ‘Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield’ (2023) 105 International Review of the Red Cross 965

Mačák K and Vignati M, ‘Civilianization of Digital Operations: A Risky Trend’ (*Lawfare*, 5 April 2023) <www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend> accessed 10 January 2024

Maurer D, ‘A State’s Legal Duty to Warn Its Own Civilians on Consequences of Direct Participation in Hostilities’ (*Lieber Institute*, 21 February 2023) <https://lieber.westpoint.edu/states-legal-duty-warn-civilians-consequences-direct-participation-hostilities/> accessed 12 April 2024

Melzer N, 'The ICRC's Clarification Process on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (2009) 103 Proceedings of the Annual Meeting (American Society of International Law) 299

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

——, 'Civilian Participation in Armed Conflict', *Max Planck Encyclopedias of International Law* (2010) <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1674> accessed 29 April 2024

——, 'Keeping the Balance Between Military Necessity and Humanity – A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities' (2010) 42 New York University Journal of International Law and Politics 831

——, '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)

Morris B, 'Ukraine: Why It Has One Of The Most Digital Governments' (*BBC*, 17 June 2025) <www.bbc.com/news/articles/cm234l04xmro> accessed 27 September 2025

Motkin A, 'Ukraine's Diia Platform Sets the Global Gold Standard for E-Government' (*Atlantic Council*, 30 May 2023) <www.atlanticcouncil.org/blogs/ukrainealert/ukraines-diia-platform-sets-the-global-gold-standard-for-e-government/> accessed 20 July 2024

O'Carroll L, 'Meet Diia: The Ukrainian App Used to Do Taxes … and Report Russian Soldiers' *The Guardian* (26 May 2023) <www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers> accessed 7 January 2024

Olejnik L, 'Smartphones Blur the Line Between Civilian and Combatant' (*Wired*) <www.wired.com/story/smartphones-ukraine-civilian-combatant/> accessed 10 January 2024

Pascucci P, 'Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution' (2017) 26 Minnesota Journal of International Law

Pleitgen F, Otto C and ottasová I, '"There Are Maniacs Who Enjoy Killing," Russian Defector Says of His Former Unit Accused of War Crimes in Bucha' (*CNN*, 14 December 2022) <www.cnn.com/2022/12/13/europe/russian-defector-war-crimes-intl-cmd/index.html> accessed 16 April 2024

'Ratification of the Additional Protocols by the United Kingdom of Great Britain and Northern Ireland' (1998) 322 International Review of the Red Cross

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

Russian Federation, 'Commentary of the Russian Federation on the Initial "Pre-Draft" of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'

<https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf> accessed 7 January 2024

Sabbagh D, 'Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks' *The Observer* (29 October 2022) <www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo> accessed 7 January 2024

Sandoz Y, Swinarski C and Zimmermann B (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Kluwer Academic Publishers 1987)

Sassòli M, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019)

Schmitt MN, '"Direct Participation in Hostilities" and 21st Century Armed Conflict', *Krisensicherung und Humanitärer Schutz/Crisis Management and Humanitarian Protection: Festschrift für Dieter Fleck* (Berliner Wissenschafts-Verlag 2004)

——, 'Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees' (2005) 5 Chicago Journal of International Law

——, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) 1 Harvard National Security Journal 5

——, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (2014) 96 International Review of the Red Cross 189

—— (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

Schmitt MN and Biggerstaff WC, 'Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?' (*Lieber Institute*, 2 November 2022) <https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/> accessed 7 January 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

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

The United Nations War Crimes Commission, 'Law Reports of Trials of War Criminals' (1949) VIII <https://tile.loc.gov/storage-services/service/ll/llmlp/Law-Reports_Vol-8/Law-Reports_Vol-8.pdf> accessed 17 April 2024

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

Toscano CP, '"Pouring New Wine into Old Bottles": Understanding the Notion of Direct Participation in Hostilities within the Cyber Domain' (2015) 64 Naval Law Review

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

Ukrinform, 'Ingenious Mobile App Helps Down First Russian Missile in Ukraine' (*Ukrinform*, 26 October 2022) <www.ukrinform.net/rubric-ato/3601566-ingenious-mobile-app-helps-down-first-russian-missile-in-ukraine.html> accessed 10 January 2024

Wallace DA, Reeves S and Powell T, 'Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines' (2021) 12 Harvard National Security Journal 164

Watts S, 'Hays Parks and Direct Participation in Hostilities' (*Liebers Institute*, 7 October 2021) <https://lieber.westpoint.edu/hays-parks-direct-participation-hostilities/> accessed 15 May 2024

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

Winther P, 'Military Influence Operations & IHL: Implications of New Technologies' (*Humanitarian Law & Policy*, 27 October 2017) <https://blogs.icrc.org/law-and-policy/2017/10/27/military-influence-operations-ihl-implications-new-technologies/> accessed 11 May 2024

Winther P and Nilsson P-E, 'Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare' (2023) <https://hcss.nl/report/smart-tactics-or-risky-behaviour-the-lawfulness-of-encouraging-civilians-to-participate-in-targeting-in-an-age-of-digital-warfare/> accessed 17 April 2024

Дія, 'Побачили С400, С300, Буратіно/Солнцепьок Чи Іскандер? Повідомте в Чатбот єВорог [Have You Seen the S400, S300, Pinocchio/Solntsepyok or Iskander? Report to the eEnemy Chatbot] (Telegram Post)' (*Telegram*, 8 February 2023) <https://t.me/diia_gov/2689>

'Дія - Державні послуги онлайн [Diia - Government Services Online]' (*Дія*) <https://diia.gov.ua> accessed 30 April 2024

'Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог [Help the Armed Forces of Ukraine Destroy the Occupier: the Ministry of Digital Transformation Launches the eEnemy Chatbot]' (*Міністерство цифрової трансформації України*, 10 March 2022) <https://thedigital.gov.ua/news/dopomozhi-zsu-znishchiti-okupanta-mintsifra-zapuskae-chatbot-evorog> accessed 30 April 2024

'єППО - Система Єдиної Протиповітряної [ePPO - Unified Air Defense Complex]' (*ePPO*) <https://eppoua.com/> accessed 9 January 2024

'"єППО": В "Дії" Появится Новый Сервис, Который Поможет Военным Сбивать Ракеты РФ ["ePPO": A New Service Will Appear in "Diia" That Will Help the Military Shoot Down Russian Missiles]' (*ФОКУС*, 16 September 2022) <https://focus.ua/uk/digital/529595-yeppo-v-diji-poyavitsya-novyy-servis-kotoryy-pomozhet-voennym-sbivat-rakety-rf> accessed 16 April 2024

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

Prosecutor v Dusko Tadic a/k/a/ 'Dule' (Opinion and Judgment) [1997] International Criminal Tribunal for the Former Yugoslavia (ICTY) (IT-94-1-A)

Public Committee Against Torture in Israel v Government of Israel [2006] Supreme Court of Israel HCJ 769/02

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

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

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1949

Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land 1899

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

Convention (IV) Relative to the Protection of Civilian Persons in Time of War 1949

Instructions for the Government of Armies of the United States in the Field (Lieber Code) 1863

Rome Statute of the International Criminal Court 1998

Saint Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight 1868

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