

Article

Smartphones in the Fog of War: Civilian Intelligence Apps and the Boundaries of International Humanitarian Law

Berkant Akkus 

Department of Public International Law, School of Law, Inonu University, Malatya 44000, Turkey;
berkant.akkus@inonu.edu.tr

Abstract

This article examines the legal implications of civilian intelligence applications used during armed conflict, focusing on smartphone-based reporting systems deployed in the Russian–Ukrainian war. Applications such as Ukraine’s e-Enemy feature integrated into the Diia platform and the standalone ePPO application have enabled civilians to provide real-time geolocated information concerning troop movements, missile trajectories, and military activities. While these technologies provide substantial operational advantages, they simultaneously challenge foundational principles of International Humanitarian Law (IHL), particularly the distinction between civilians and combatants. The article critically evaluates whether civilians using such applications engage in direct participation in hostilities (DPH) under Article 51(3) of Additional Protocol I, analysing the criteria of threshold of harm, direct causation, and belligerent nexus. It argues that although certain forms of real-time operational reporting may satisfy the DPH threshold in limited circumstances, existing doctrine remains insufficient to address the broader systemic implications of state-organised digital civilian mobilisation. The article further contends that embedding military intelligence functions within civilian digital infrastructure transforms such platforms into potential dual-use objects, thereby engaging state obligations under Articles 48, 52, 57, and 58 of Additional Protocol I, as well as Common Article 1 of the Geneva Conventions. Through doctrinal analysis and the Ukrainian case study, the article proposes the development of a “duty of digital separation” requiring states to maintain clearer distinctions between civilian services and military intelligence systems. It additionally advocates enhanced precautionary duties, informed consent mechanisms, risk disclosure obligations, and governance frameworks for civilian intelligence applications. Ultimately, the article demonstrates that while IHL remains technologically adaptable in principle, interpretative refinement is necessary to preserve civilian protection in the context of digitally mobilised warfare.



Academic Editor: Patricia Easta

Received: 18 May 2026

Revised: 15 July 2026

Accepted: 31 July 2026

Published: 6 August 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: direct participation in hostilities; civilian intelligence applications; dual-use digital infrastructure; digital warfare and civilian protection; international humanitarian law

1. Introduction

While armed conflict has never been immune to technological developments, the contemporary intersection between war and civilian digital infrastructure is particularly prominent. The rapid expansion of smartphone-based wartime applications, particularly in the Russian–Ukrainian conflict, has converted ordinary civilians into potential providers of operational intelligence (Zarembo et al. 2025, p. 307). Ukraine’s introduction of tools such

as the e-Enemy feature within the Diia platform, alongside independent applications such as ePPO, illustrates how States can mobilise mass civilian reporting to support real-time intelligence, targeting and situational awareness (Peperkamp 2024, p. 70). What previously required trained personnel and specialised equipment can now be performed by any person in possession of a smartphone with an internet connection. This practice has given rise to operational benefits for Ukraine. The widespread use of smartphones by civilians does not blur the legal categories of armed conflict under IHL, which remain limited to international and non-international armed conflicts. Rather, it blurs the practical distinction between protected civilians and civilians directly participating in hostilities, thereby complicating the application of the rules governing direct participation in hostilities.

IHL is based on the notion that civilians and combatants have distinct legal roles, and that the protection afforded to civilians is dependent on this distinction (Quéguiner 2016, p. 167). The main challenge to this distinction has arisen in the context of irregular fighters or combatants disguised as civilians (Macak 2023, p. 971). The development of crowdsourced digital participation introduces a distinct, systemic pressure, because such civilians do not join armed groups, carry weapons or engage in kinetic activities. They use everyday technology to feed data into military systems, often at the invitation of the State. This gives rise to a legal dilemma that existing doctrine only partially resolves.

Debate has focused on whether civilians who report enemy activity through apps engage in direct participation in hostilities (DPH) (Peperkamp 2024, p. 70). If reports meet the thresholds of harm, direct causation and belligerent nexus, civilians may lose protection for such time as they participate. Two divergent approaches may be identified in existing literature. The restrictive view argues that civilian reporting only exceptionally satisfies the DPH criteria (Macak 2023, p. 978). The broader view suggests that real-time, geolocated information almost always contributes directly to operational outcomes, rendering civilian reporters closer to artillery spotters than passive observers (Schmitt 2009, p. 703). Both positions are theoretically defensible, and both risk oversimplifying on-the-ground reality, where millions of civilians interact with digital tools that blur these distinctions.

More significantly, the debate conceals a deeper structural issue. Even if it is accepted that many civilians do not individually cross the DPH threshold, States may violate IHL when they build, encourage or rely on systems that foreseeably blur the civilian/combatant divide. Embedding an intelligence collection feature inside Diia effectively transforms a civilian digital system into a dual-use infrastructure. This gives rise to issues surrounding the rules on distinction, precautions and the obligation under Common Article 1 of the Geneva Conventions 1949 (GC) to respect and ensure respect for IHL. It also gives rise to practical concerns, as civilians may not appreciate the legal and operational consequences of reporting military information. They may believe they are performing a harmless civic duty, while their conduct may render them targetable for such time as they directly participate in hostilities, expose them to capture or domestic criminal liability, and place them at heightened risk from opposing forces.

The legal implications are broad. Civilian digital mobilisation interacts with human rights law, particularly the right to life and the duty of the State to warn citizens of foreseeable risks (Benabbass and Zwanenburg 2023, p. 55). It covers privacy, surveillance, attribution of responsibility and the protection of civilian infrastructure in both physical and cyber dimensions. Although IHL is generally understood to apply independently of the means and technologies used in warfare, the scale and speed of smartphone-enabled civilian participation in hostilities expose important practical limits to that technology-neutral approach (Shereshevsky 2022, p. 2144). The boundaries between military and civilian roles were not drafted with mass networks of voluntary civilians in consideration.

Existing academic debate has largely centred on whether civilians who use smartphone applications to transmit military-relevant information directly participate in hostilities and, if so, when such participation begins and ends, while the corresponding obligations of States have remained largely unexplored. The consequences of embedding military functions within civilian cyber infrastructure have received minimal attention. System design choices are rarely analysed through the lens of IHL obligations. As a result, the law risks focusing narrowly on the actions of individual civilians while overlooking the structural decisions that shape their participation. This article addresses this gap. With reference to the Ukrainian experience as a case study, it examines whether and how IHL regulates the development, deployment, and use of civilian intelligence applications in armed conflict, and the responsibilities that States bear when they mobilise civilians through such tools. It assesses whether civilian users engage in DPH, and also situates such inquiry within a broader assessment of State duties relating to distinction, precautions, digital infrastructure design, risk communication and the protection of civilians. It conducts an evaluation of whether the current legal framework is adequate and proposes interpretative and policy approaches that may better account for civilian digital participation in modern warfare.

1.1. Research Aims and Objectives

The key research question is: How should IHL regulate the development, deployment, and use of civilian intelligence applications in armed conflict, and what obligations do States bear when mobilising civilians through such digital tools? This gives rise to a range of research aims and objectives:

1. To identify the conditions under which civilians who use mobile intelligence applications engage in direct participation in hostilities.
2. To critically examine whether the systematic encouragement of civilian reporting implicates State obligations under IHL.
3. To identify and analyse the responsibilities of States to warn, educate and protect civilians who may expose themselves to foreseeable risks through the use of intelligence apps.
4. To explore how IHL should approach the integration of intelligence-gathering tools within civilian digital infrastructure, such as the embedding of e-Enemy within Diia.
5. To determine which accountability mechanisms or design principles can ensure responsible deployment of such technologies.
6. To critically examine whether existing IHL rules are adequate for regulating civilian intelligence apps, or whether they require interpretative development to account for the realities of digital civilian mobilisation.

Collectively, these questions guide the doctrinal analysis, shape the evaluation of the Ukrainian case study and frame the proposals advanced in the article.

1.2. Methodology

This article employs a qualitative doctrinal (legal-dogmatic) methodology, examining treaty law, customary international law, judicial decisions, and authoritative academic commentary to identify and interpret the applicable legal framework. The legal-dogmatic approach is particularly suited to emerging technological practices, because it enables new factual developments to be interpreted through the established structure of IHL rather than treated as exceptional cases (Majeed et al. 2023, p. 561). Core materials include the GC, Additional Protocol I (API I) (McDonald and Swaak-Goldman 2000), commentaries and guidance of the International Committee of the Red Cross (ICRC), and case law that sheds light on civilian harm, precautionary duties and the treatment of dual-use objects. The

doctrinal analysis provides the basis for evaluation of how civilian intelligence apps fit or strain the existing regulatory framework.

To ground the legal assessment within a specific, observable practice, the article utilises the Ukrainian experience between 2022 and 2025 as a case study. Ukraine is the most developed and information-rich example of a State deliberately mobilising civilians through digital intelligence tools. The case study focuses on three elements: (a) the integration of the e-Enemy reporting feature inside Diia, a platform typically dedicated to civilian administrative functions, (b) the contrasting design of the ePPO application, which operates as a more clearly separated and purpose-built reporting tool, and (c) domestic criminal proceedings involving civilians accused of transmitting targeting information by phone. Such examples provide factual material and illustrate how technological design choices map onto legal obligations.

The article also employs a comparative analysis of competing interpretations of direct participation in hostilities, alongside a normative assessment of the adequacy of the current legal framework. This involves evaluating whether existing IHL principles and the DPH framework provide a sufficiently clear and coherent legal basis for regulating civilian intelligence applications while preserving the balance between military necessity and civilian protection, or whether further interpretative refinement is required. The analysis develops potential doctrinal pathways and principles that could more effectively integrate digital civilian participation into the protective logic of IHL.

The article commences with examination of the IHL principles relevant to civilian participation, including direct participation in hostilities, distinction, precautionary duties and state obligations, highlighting key debates. Section 3 proceeds to analyse civilian intelligence apps in practice, with Ukraine as a case study. It analyses platforms such as Diia/e-Enemy and ePPO, illustrating operational use, risks to civilians and systemic implications for IHL compliance. Section 4 critically evaluates the DPH doctrine as applied to civilian reporting apps, weighing restrictive versus expansive interpretations and highlighting doctrinal ambiguities. Section 5 focuses on state duties to ensure respect for IHL, the precautionary obligations, duty to warn and educate civilians, and accountability for the design and deployment of digital tools. Section 6 assesses gaps in the current legal framework, explores interpretative paths such as dual-use classification and duty of digital separation, and proposes policy and governance measures.

The article ultimately concludes that civilian intelligence applications significantly blur the traditional boundary between civilians and combatants, giving rise to both operational advantages and legal risks. Analysis of the DPH doctrine demonstrates that while civilian reporting can substantially support military operations, ambiguity persists regarding immediacy, causation and belligerent nexus. Embedding military functions within civilian platforms foreseeably exposes participants to harm and raises obligations under IHL, including the duty to respect, precautionary duties and the duty to warn. The article argues in favour of doctrinal evolution, including recognition of the dual-use digital infrastructure, creation of a duty of digital separation, and implementing governance measures such as informed consent, transparency and oversight.

2. Conceptual & Legal Foundations

IHL is founded upon the distinction between civilians and combatants, who have distinct legal status and, therefore, different degrees of protection in armed conflict. This is enshrined in Article 48 AP I, which frames the objective of IHL as ensuring “respect for and protection of the civilian population and civilian objects”. Article 51(3) AP I provides that civilians “shall enjoy the protection afforded by this Section, unless and for such time

as they take a direct part in hostilities". The exceptional nature of DPH is therefore at the centre of any inquiry into civilian use of intelligence applications.

The meaning and limits of DPH have given rise to the need for considerable interpretive effort (Schmitt 2009, p. 699). The ICRC's Interpretive Guidance on DPH articulates a threefold functional test based on threshold of harm, direct causation and belligerent nexus, while emphasising the need for a limited and practicable approach to depriving civilians of protection (Melzer 2009, pp. 47–60). Although it does not have status as treaty law, the Guidance is highly influential in that it interprets the Article 51(3) AP I exception and is frequently invoked in doctrinal and judicial reasoning (*Prosecutor v Bosco Ntaganda* 2019). Its emphasis on a cautious, context-sensitive application of DPH (*ibid.*, pp. 27, 35) has influenced academic claims against expansive readings which would risk the undue erosion of civilian protection (Dinstein 2022, pp. 123–27). However, it has also been contended that certain forms of real-time, geolocated reporting are functionally equivalent to traditional battlefield roles and therefore fall within the scope of DPH (Williamson 2009, p. 460). The tension between these restrictive and expansive approaches is central to the legal problems that smartphone-enabled reporting creates.

While the debate surrounding DPH places primary focus on the status of individual civilians, IHL features parallel obligations that directly affect the legality of State practices in mobilising civilian reporting. The duty to distinguish, the requirement to take precautions in attack, and the obligation to protect civilians against the effects of hostilities impose positive responsibilities on parties to a conflict that delve beyond the status of discrete actors. Article 48 AP I establishes the general duty to distinguish, while Article 57(2)(a)(i) AP I obliges planners and decision-makers to "do everything feasible" to verify that targets are military objectives and to choose means and methods of attack to avoid or minimise incidental civilian harm. Article 58 AP I requires parties to take practicable measures to remove civilians from danger and protect them from the effects of attacks. These provisions demand anticipatory, systemic decision-making by State actors whose policies or platforms foreseeably expose civilians to risk.

The legal consequences of embedding military functionality in civilian infrastructure are demonstrated by Article 52(2) AP I, which strictly limits attacks to military objectives and establishes a presumption that objects ordinarily dedicated to civilian purposes are civilian (Droege 2012, p. 548). When a State incorporates a feature of intelligence gathering into a multipurpose civilian platform, the design choice alters the factual context upon which the presumption operates. The platform may become dual-use in practice, and the protective assumptions that typically attach to civilian objects become complicated (Capone 2025, p. 82). Article 52 AP I has a protective aim; therefore, blurring the civilian/military distinction requires careful scrutiny of the State's conduct. Common Article 1 GC complements these provisions by imposing a duty to "respect and to ensure respect" for the GC. This obligation requires States to adopt measures that prevent violations, including those that may arise from state-sanctioned mobilisation of civilians. Common Article 1 GC encompasses not only the conduct of armed forces but also the policies, communications and technological platforms through which a State organises civilian conduct in armed conflict (Focarelli 2010, p. 134). Essentially, the question of whether civilians lose protection through DPH cannot be separated from the question of whether the State's design and deployment of digital reporting tools itself violates IHL duties to protect civilians and avoid turning civilian infrastructure into military objectives.

Judicial practice in international criminal tribunals demonstrates the balance between individual and systemic accountability. The International Criminal Tribunal for the former Yugoslavia (ICTY) has repeatedly affirmed the foundational importance of this distinction and has examined the elements of intent, causation and the targeting of civilians in the

context of sustained bombardment and urban warfare. Although ICTY judgments are not binding sources of IHL, they are widely regarded as persuasive authority for interpreting and applying its rules. Cases such as *Prosecutor v Tadić* (*Prosecutor v Dušan Tadić* 1999) and *Prosecutor v Galić* (*Prosecutor v Dragomir Galić* 2003) illustrate how evidence of deliberate targeting is approached, the foreseeability of civilian harm, and the criminal responsibility of military and political leaders for attacks that fail to respect the civilian/military divide. These judgments do not directly address the novel issue of smartphone reporting, although they offer a background for assessing whether a State's operational choices, such as embedding reporting tools in civilian platforms, may render civilians more vulnerable and thus engage IHL protections and obligations.

This section has outlined the regulatory architecture that forms the basis for the remainder of the article. Article 51(3) AP I provides the legal basis for inquiry into individual civilian participation, while Articles 48, 52, 57 and 58 AP I, with Common Article 1 GC, provide the tools for evaluating State conduct and system design. The ICRC's Interpretive Guidance on DPH and tribunal jurisprudence reveal the interpretive approach. However, the specific phenomenon of mass, smartphone-enabled civilian reporting highlights the need for an integrated analysis that focuses on the individual DPH question and the systematic obligations of the State when it designs and promotes digital tools that invite civilians into the battlespace.

3. Civilian Intelligence Apps in Practice: The Ukrainian Case Study

The ongoing conflict in Ukraine has illustrated the practical challenges and opportunities that arise in the context of civilian intelligence applications. Such technologies occupy an unprecedented space between civilian digital infrastructure and military operations, giving rise to both operational and legal questions. The Ukrainian experience offers a rich case for examination of how such platforms function, the risks they generate and their implications under IHL.

3.1. Diia, e-Enemy and ePPO

The Diia platform, launched as a comprehensive civilian services hub, provides Ukrainian citizens with access to identity documents, healthcare records, taxation services and other essential administrative functions. In 2022, the government introduced the e-Enemy feature into the platform, enabling civilians to report enemy troop movements, missile trajectories and other battlefield information in real time (Steinbrink et al. 2025, p. 12). This had the effect of transforming a civilian-focused digital infrastructure into a dual-use system, merging public service functionalities with military intelligence capabilities.

The embedding of military functions within a civilian platform has significant implications for the classification of infrastructure under IHL. Article 52 AP I stipulates that civilian objects are those that "are not military objectives" and that attacks must be strictly limited to legitimate military targets. When a civilian platform is supplemented by features that contribute directly to military operations, this blurs the boundary between civilian and military objects and potentially increases the risk of lawful targeting. The dual-use nature of Diia complicates operational targeting decisions and the protective obligations of the State under Articles 57 and 58 AP I, which require all feasible precautions be taken to safeguard civilians and civilian objects (Breeze 2024, p. 319). Furthermore, the integration raises questions of State responsibility because civilians using such applications may become lawful targets for such time as they directly participate in hostilities, thereby exposing them to risks that they may not fully appreciate. In this context, Common Article 1 requires States not merely to encourage compliance with IHL, but also to take reasonable

measures to ensure respect for its rules by informing users of the legal consequences and operational risks associated with the application, providing clear guidance on conduct that may amount to direct participation in hostilities, and, where feasible, minimizing the integration of military functions into civilian digital infrastructure (Capone 2025, p. 56).

In contrast, the ePPO application illustrates an alternative design approach, because it is a standalone mobile application developed to facilitate civilian reporting specifically for air defence operations (Biggio 2024, p. 144). Unlike Diia, ePPO requires separate registration and operates independently from broader civilian services. Its narrower operational scope reduces the ambiguity associated with dual-use platforms and limits the potential exposure of civilians to battlefield risks. From a legal perspective, the ePPO model mitigates certain risks that plague the integrated Diia/e-Enemy feature. Separating military reporting from general civilian infrastructure can assist states in maintaining clearer distinctions between civilian and military objects, promoting compliance with the principle of distinction under Article 48 AP I. Furthermore, the narrower purpose and isolated deployment of ePPO can enhance the State's ability to provide targeted warnings, education and precautionary measures to participants, aligning with the protective duties under Articles 57 and 58 AP I. The contrast between Diia/e-Enemy and ePPO thus highlights the implications that design choices have for legal risk. While integrated platforms maximise accessibility and potentially operational intelligence, standalone applications preserve structural separation and reduce exposure to direct participation or targeting liability (Peperkamp 2024, p. 70).

3.2. Real-World Incidents and Operational and Legal Insights

The Ukrainian context provides concrete examples that highlight the legal and practical implications of civilian intelligence mobilisation. There is a very real potential for ordinary users to be implicated in direct participation in hostilities (Hogue 2023, p. 110). This raises the question regarding Article 51(3) AP I and the circumstances under which civilians lose protection from attack. It also underscores the blurred boundaries between voluntary participation, State encouragement, and operational consequences. Military forces can actively monitor app usage to assess operational information, demonstrating that civilian contributions can have immediate strategic consequences (Ford 2024, p. 1540). This emphasises the practical significance of the DPH debate, illustrating how civilians' collection and transmission of military-relevant information through smartphone applications can materially influence hostilities while simultaneously exposing them to legal and physical risks.

Examination of these platforms reveals significant insights. The first is that civilian intelligence apps provide considerable operational value. Crowdsourced information enhances situational awareness, supports targeting decisions and facilitates rapid military responses. This demonstrates the increasingly central role played by civilians in modern digital conflicts as active contributors whose information materially influences operations (Hogue 2023, p. 110). The second is that these examples highlight the ways in which States operationalise civilian digital labour. By integrating military reporting into accessible platforms such as Diia or developing narrowly purposed applications such as ePPO, States achieve civilian participation while navigating associated legal responsibilities (Horbyk 2022, p. 18). The design of applications such as Diia and ePPO directly affects compliance with IHL because it determines how civilians collect and transmit military-relevant information, the degree to which they are integrated into military operations, and whether they receive adequate warnings regarding the legal consequences and targeting risks associated with direct participation in hostilities. Finally, the Ukrainian case study underscores the complexities involved in the application of traditional IHL principles to contemporary digital tools. The dual-use nature of Diia/e-Enemy illustrates potential conflicts with the

principle of distinction and the obligation to avoid civilian harm, while ePPO demonstrates that technical and procedural design choices can mitigate these conflicts (Hathaway et al. 2024, p. 2647). There are immediate legal and ethical consequences for civilians, reinforcing the need for clarity regarding direct participation, state responsibility and the integration of civilian infrastructure into military operations.

Ultimately, the Ukrainian experience reveals a range of legal and operational considerations that serve to inform the broader debate. It demonstrates that civilian intelligence apps are instruments through which states mobilise civilian populations, reshape battlefield dynamics and engage with the protective frameworks established under IHL. This provides a foundation for the following sections, which evaluate the adequacy of existing law and explore potential developments to govern civilian participation in digital conflict environments.

4. Do Civilians Using Intelligence Apps Engage in Direct Participation in Hostilities?

At the core of the question as to whether civilians who use smartphone intelligence applications may be lawfully targeted lies Article 51(3) AP I, which subjects protection afforded to civilians to the condition that they not “take a direct part in hostilities”. The consequence of the exception to the civilian rule is severe, and it is therefore applied narrowly and with caution (Schmitt 2010, p. 8).

Application of the DPH criteria to app reporting commences with the threshold of harm. According to the ICRC’s Interpretive Guidance, the act in question must reach a degree of harm that is of a “specifically military nature” or otherwise meet a quantitative or qualitative threshold to the extent that it meaningfully contributes to military action (Melzer 2009, p. 47). A single, vague sighting submitted via an app such as ‘two trucks on the road’, will typically fall short of this threshold, whereas a real-time, geolocated report that identifies a weapons system with coordinates and timing may likely reach it. The practical difficulty is that the threshold is not fixed; it depends on the specificity, timeliness, and intended use of the information. The Guidance therefore instructs a case-by-case assessment that focuses on the foreseeable military effect of the act at the time and place it occurred (ibid., p. 50).

The second element of the test, direct causation, assesses whether the civilian’s act directly and immediately causes harm to the adversary (ibid., pp. 52–53). It is here that the technological capabilities of smartphones have significance. Modern reporting apps can transmit geolocation metadata, photos and video streams that are processed in near real-time by military systems. When a civilian’s report is incorporated into a targeting cycle that results, within a short causal chain, in a kinetic strike, the causal link to harm is materially stronger than when the report enters a slow, aggregated intelligence process (ibid., p. 54). This does not suggest that Ukrainian targeting decisions are based solely on civilian reports. Rather, the argument is that the legal assessment of causation may differ where civilian-provided information is promptly verified and incorporated into the targeting cycle as one element of a broader intelligence assessment. Temporal immediacy is of significance, in that the closer in time and mechanism a civilian’s communication is to the use of force, the more it resembles classical acts of participation.

The third element of the test, belligerent nexus, requires that the act be meaningfully connected to hostilities between the parties; it must “be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another” (ibid., p. 58). A generalised expression of support or a report intended for public safety purposes lacks such a nexus, while a clearly military report sent through a state-sanctioned channel assigned for operational use has it. The nexus

assessment therefore draws on the context of the reporting environment, such as whether the app is explicitly designed and marketed as an intelligence channel for military use, whether the State encourages or integrates the data into operational systems, and whether the user understands the likely end use. The ICRC Guidance emphasises that the nexus cannot be inferred solely from the existence of a conflict; it depends on whether the contribution is “part of” the hostilities in a functional sense (*ibid.*).

Collectively, the three criteria create a range of conceivable legal outcomes rather than a simple binary outcome. Several arguments support the claim that app reporting can constitute DPH. Firstly, where reporting is precise, real-time and expressly routed into targeting cycles, it can materially and immediately affect the conduct of hostilities. The realities of digital battlefields enable civilians to occupy roles that essentially perform the same military function as combatants engaging in direct targeting support (Schmitt 2009, p. 700). Secondly, an app that is formally embedded in a State’s platform and accompanied by official encouragement or instruction increases the likelihood that a civilian’s report will have an immediate causal effect. This is relevant due to the functional nature of the DPH test. If State design choices convert ordinary bystanders into operational sensors, the content and channel of their communications become legally relevant to their status.

There also exist compelling arguments for a restrictive reading that would vindicate most app users from DPH. The Interpretive Guidance warns against expansive interpretations that would strip civilians of protection on the basis of loosely connected or indirect acts (Melzer 2009, pp. 52–53). A key justification for such caution is the limited agency and control that civilians typically have over how their information is processed. Many app users do not direct targeting decisions, in that they do not choose the time, weapon or method of attack. Where information is aggregated, verified or transformed by military analysts prior to becoming actionable, the causal contribution of an individual report may be too weakened to qualify as DPH (Giovannelli 2025, p. 119). Moreover, many reports are imprecise, unverifiable or motivated by public safety rather than operational support. To classify such acts as DPH would risk overly broad deprivation of civilian protection.

These two approaches produce distinct consequences. If widespread app reporting routinely qualifies as DPH, then large numbers of civilians could lose protection for the duration of their engagement in reporting. This would create practical challenges for attacking forces required to identify and verify the status of potential targets. Article 51(3) AP I roots the limitation in the requirement that loss of protection only apply for the duration of the participation. However, determining when participation begins and ends is extremely difficult in the digital context. Identification problems are also apparent, in that the anonymity of digital submissions and the use of third-party platforms render it difficult for attackers to determine whether a particular individual is an active participant at the precise moment of attack (Melzer 2009, paras. 32–34). Such issues support the claim against over-expansive applications of DPH.

A further difficulty concerns the evidentiary threshold required before an individual may lawfully be regarded as targetable. In practice, the mere observation that a civilian is using a smartphone or digital application cannot, without more, establish that the individual is transmitting operationally relevant information amounting to direct participation in hostilities. As Melzer observes, civilians who participate on a sporadic and unorganized basis may only be attacked while preparing for, carrying out, and returning from a specific hostile act, making accurate identification of both the individual’s conduct and the temporal scope of participation indispensable (Melzer 2008, p. 337). Where an attacker cannot distinguish between ordinary civilian phone use and the transmission of targeting information through a military reporting application, uncertainty should not be converted into a legal basis for targetability. This conclusion is consistent with the Israeli Supreme

Court's judgment in *Public Committee Against Torture in Israel v Government of Israel*, which stressed that reliable information regarding both the identity of the individual and the nature of the allegedly hostile activity must be carefully verified before targeting decisions are made. The Court further emphasized that the loss of protection is confined to the period of direct participation and that, where feasible, less harmful measures than lethal force should be preferred (*Public Committee Against Torture in Israel v Government of Israel* 2006, paras. 40, 60). Accordingly, the inherent evidentiary limitations associated with app-based reporting provide a further reason to resist an overly expansive interpretation of direct participation in hostilities.

A further consequence of the broad application of DPH to app users is the chilling effect on behaviour and the risk of indiscriminate or disproportionate targeting. States may treat entire user groups or geographic areas as suspect, potentially violating precautionary obligations under Articles 57 and 58 AP I. On the other hand, a restrictive approach preserves civilian protections, but may reduce the capacity of militaries to respond to rapidly emerging threats that depend on civilian reporting. This reveals a structural problem, whereby rules focused on individual liability are not appropriate for phenomena that are fundamentally systemic and design-driven.

Ultimately, cautious application of the DPH criteria may justify treating app-based reporting as DPH where civilians intentionally provide real-time targeting information, troop locations, or other operationally significant intelligence concerning identifiable military objectives, and that information is sufficiently closely connected to a specific military operation. The legal and practical limits outlined in the ICRC Guidance caution against presuming that ordinary users directly participate in hostilities merely because they use such applications. Whether a particular user amounts to direct participation depends on the specific circumstances of the activity in question. However, given that the DPH framework is primarily focused on the status of individuals rather than the responsibilities of States, relying on it as the sole regulatory instrument risks ignoring the system-level questions posed by State-designed civilian reporting platforms. Focus must therefore shift from exclusive adjudication of individual status under Article 51(3) AP I to assessment of State obligations under the principles of distinction, precautions and the duty to ensure respect for IHL.

Direct participation applies exclusively to civilians acting individually or in an unorganized manner. By contrast, combatants and members of organized armed groups (OAGs) are generally regarded as lawful military objectives throughout the duration of their membership. The ICRC argued in its *Interpretive Guidance* that only those OAG members who perform a "continuous combat function" should be treated in this way, whereas individuals performing exclusively political, financial, or administrative roles should retain civilian protection except when directly participating in hostilities. This interpretation has attracted substantial criticism (US Department of Defense 2023, para. 5.8.2.1; Watkin 2010, p. 683), and persuasive arguments suggest that the ICRC's position is overly restrictive. For present purposes, however, the distinction has limited practical significance because the legal implications of using the ePPO application primarily concern civilians who are not members of organized armed groups. Given the application's intended civilian user base, this is likely to describe the overwhelming majority of its users.

Greater complexity arises when considering the temporal dimension of the rule, since civilians lose protection from direct attack only for the duration of their direct participation. Consequently, two issues require examination: first, the point at which participation begins and ends, and second, how the law addresses civilians who engage in repeated acts of participation (Boothby 2010, p. 768).

There is little doubt that a civilian actively using the application to report military information falls within the period of direct participation. More difficult, however, is determining the temporal boundaries of that participation. Does the relevant period commence when the application is downloaded, when the user completes authentication, when the application is opened, or only when it is actually employed to transmit information? Similarly, does participation cease immediately after a report is submitted, upon closing the application, or only once it has been permanently removed from the device?

A broadly accepted proposition is that direct participation is not confined to the execution of the hostile act itself but also encompasses preparatory activities. According to the ICRC, preparatory conduct falls within direct participation when it possesses a specifically military character and is sufficiently connected to the execution of a particular hostile act to constitute an integral component of that operation (Melzer 2009, p. 65). Nevertheless, the precise scope of qualifying preparation remains contested.

The ICRC adopts a restrictive interpretation, distinguishing between preparations undertaken for a particular hostile act and measures intended merely to create a general capability to engage in future hostile activities (Melzer 2009, p. 66). Applying this reasoning, civilians who simply install the application or leave it operating in anticipation of a possible opportunity would not ordinarily lose protection. Rather, the threshold would likely be crossed only once the individual begins actively searching for enemy military assets or is already engaged in transmitting a report concerning a specific target. At that stage, the conduct is no longer merely preparatory in a general sense but forms part of a concrete reporting activity.

An alternative interpretation would afford a broader temporal reach to the phrase “for such time.” Dinstein argues that the relevant period should extend a reasonable distance both before and after the hostile act itself, capturing conduct occurring “upstream” and “downstream” of the engagement (Dinstein 2016, p. 176). While this broader approach is persuasive in principle, it should arguably remain confined to exceptional situations. For example, where an individual downloads the application with the specific intention of embarking on a deliberate mission to locate and report enemy military equipment, direct participation could reasonably begin before the individual physically sets out to perform that task.

The same reasoning applies once the reporting activity has concluded. The ICRC considers withdrawal from the location where the hostile act occurred to remain part of direct participation where such movement constitutes an integral element of the overall operation (US Department of Defense 2023, para. 5.8.4.1; Melzer 2009, p. 67). Consistent with this view, protection would ordinarily be restored once the civilian has ceased searching for military objectives and completed any reporting activity associated with the observed target.

A separate issue concerns civilians who repeatedly engage in acts amounting to direct participation. The question is whether each isolated reporting activity should be treated independently or whether repeated conduct creates a continuous period during which the individual remains targetable.

The ICRC’s Interpretive Guidance relies on the wording “for such time” to conclude that civilians alternately lose and regain protection as they move in and out of direct participation (Melzer 2009, p. 70). Accordingly, a civilian would only be lawfully targetable while actively locating military objectives or transmitting a report concerning them. Once that activity ends, protection against direct attack is restored until another qualifying act begins. In the ICRC’s view, this so-called “revolving door” is an intended feature of international humanitarian law rather than a defect within it (Melzer 2009, p. 70).

In our assessment, the revolving-door approach is neither operationally practical nor legally convincing. A civilian who repeatedly engages in hostilities should remain a lawful military objective until the individual clearly withdraws from participation, either by an extended period of non-participation or through an unequivocal act demonstrating permanent disengagement (US Department of Defense 2023, para. 5.8.4.2). Under this approach, a civilian who establishes a recurring practice of using the application to identify and report enemy military systems would remain targetable from the commencement of the initial qualifying act until participation had genuinely and permanently ceased.

Difficulties nevertheless arise where an individual privately decides to discontinue reporting but takes no outward steps to communicate that decision—for example, by retaining the application without deleting it. Legally, direct participation would end once the person had genuinely abandoned further involvement. However, any uncertainty arising from the participant's failure to make that withdrawal objectively apparent should be borne by the participant rather than by the opposing force (Schmitt 2010, p. 38). This conclusion reflects a basic premise of international humanitarian law: civilians possess no entitlement to participate directly in hostilities, and the legal framework governing armed conflict proceeds on the assumption that civilians ordinarily remain outside the conduct of hostilities.

The foregoing discussion naturally leads to a further question: does the use of the ePPO application by Ukrainian civilians to report Russian military assets constitute a breach of international law? A common misconception is that civilians who directly participate in hostilities necessarily commit an internationally wrongful act.

Such an interpretation is not supported by international humanitarian law. Although civilians are not granted the combatant's privilege to engage in hostilities, IHL does not establish a general prohibition against civilian participation in military activities. Rather, the principal legal consequence is the temporary loss of protection from direct attack while the requirements for direct participation are satisfied. Consequently, where civilians provide intelligence that enables Ukrainian forces to locate, damage, or destroy legitimate military objectives—or even contribute to attacks against Russian armed forces—they are not, solely for that reason, acting unlawfully under international law.

The position may differ, however, under domestic criminal law. Whether civilians may face prosecution for conduct amounting to direct participation depends upon the applicable national legal framework and the lawful exercise of criminal jurisdiction by the prosecuting State. Relevant considerations include the extent to which domestic legislation provides for extraterritorial jurisdiction, the legal basis for prescriptive and adjudicative jurisdiction, and any limitations arising from international human rights obligations. As these issues involve complex questions extending beyond international humanitarian law, they fall outside the scope of the present discussion.

Another issue that remains controversial concerns the legal status of civilians who are captured after directly participating in hostilities. Scholars continue to disagree regarding the protective regime applicable in such circumstances. One approach characterizes these individuals as unlawful combatants who are entitled neither to prisoner-of-war status under Geneva Convention III nor, except within occupied territory, to the protections afforded to civilians under Geneva Convention IV (Baxter 1951, pp. 342–45). Under this view, the safeguards available to them derive primarily from the fundamental guarantees contained in Article 75 of Additional Protocol I. This interpretation broadly reflects the position adopted by the United States (US Department of Defense 2023, para. 10.3). By contrast, numerous commentators maintain that civilians who directly participate nevertheless retain their civilian status upon detention and therefore continue to benefit from the protections established by Geneva Convention IV (Pejic 2007, pp. 338–49).

From an operational perspective, the introduction and widespread deployment of the ePPO application offer clear military advantages. The system has already assisted Ukraine in identifying and responding effectively to Russian military operations, and civilians who use the application to report military objectives are not, by that conduct alone, acting contrary to international law.

At the same time, the creation of what effectively functions as a contemporary civilian observation network carries significant legal consequences. Individuals volunteering to perform this role surrender the protection from direct attack that civilians would ordinarily enjoy while their activities amount to direct participation in hostilities. Furthermore, if the broader interpretation rejecting the so-called revolving-door approach is adopted, that loss of protection may continue for a considerably longer period than the reporting activity itself. As a consequence, these civilians face increased exposure to lawful military attack, and their involvement may also influence the application of other IHL rules, including proportionality and the obligation to take feasible precautions in attack.

These considerations become particularly significant if the reporting application is intended for widespread use across the civilian population. Such a policy inevitably increases the number of civilians who may lose protection from direct attack under IHL. While a State confronted with an adversary that has consistently disregarded civilian protection may conclude that these operational benefits justify the accompanying risks, any decision to expand civilian participation should be made with a full appreciation of the legal and practical consequences arising under the law of armed conflict.

One of the clearest contemporary illustrations of civilian involvement in hostilities concerns Ukrainian volunteer drone reconnaissance units operating in areas close to the front line. Public reporting has repeatedly indicated that civilians have used commercially available drones to collect real-time battlefield intelligence and relay it directly to Ukrainian armed forces. For example, on 7 July, the Telegram channel *Our Wars Today* circulated footage allegedly depicting a Russian military position in the Kherson region being destroyed shortly after Ukrainian forces received targeting information. Although the precise circumstances surrounding the incident cannot be independently verified, numerous reputable media outlets, including the *Financial Times* and the *New Statesman*, have documented the role of civilian drone operators in Ukraine's defence efforts. These reports further indicate that reconnaissance data are frequently transmitted through communication systems such as Elon Musk's Starlink before reaching Ukrainian military units (Thornhill 2022).

Applying the ICRC's Interpretive Guidance, this activity readily satisfies the first constitutive element of direct participation in hostilities. The intelligence collected by civilian drone operators facilitates attacks directed against military objectives and may ultimately result in the destruction of military assets or the death of enemy personnel. The Guidance explains that the required threshold of harm encompasses acts producing adverse military effects, including interference with military communications or logistics (Silvestri 2019). Consequently, conduct enabling kinetic strikes against Russian forces exceeds this threshold without difficulty.

The requirement of direct causation is likewise fulfilled. The reconnaissance mission itself forms an integral component of the specific military operation, with the information gathered being transmitted directly to forces responsible for executing the attack. Such conduct differs fundamentally from more remote forms of support, including industrial production, infrastructure maintenance, political advocacy, fundraising, or other activities that merely sustain the broader war effort. Instead, there exists a sufficiently close causal connection between the reconnaissance activity and the resulting military harm.

Importantly, the existence of direct causation does not depend upon the reconnaissance information being indispensable to the attack. The ICRC expressly rejects such a

restrictive approach, observing that individuals acting as lookouts during an ambush directly participate in hostilities even where the attack could have proceeded using information obtained from another source. In other words, the relevant inquiry is whether the individual's conduct forms part of the causal chain leading to the military operation, rather than whether that contribution is irreplaceable. Accordingly, even where several civilian reconnaissance teams provide overlapping intelligence, each may independently satisfy the causation criterion.

The final cumulative requirement—belligerent nexus—is equally straightforward. The intelligence is intentionally collected and transmitted for the benefit of Ukrainian armed forces and with the objective of facilitating military action against Russian forces. Its purpose is therefore intrinsically linked to the conduct of hostilities and designed to disadvantage one party to the armed conflict while assisting the other.

Taken together, these three elements strongly support the conclusion that civilian front-line drone reconnaissance teams directly participate in hostilities under international humanitarian law. If the reported operation were carried out by members of the civilian drone unit *Aerorozvidka*, their activities would almost certainly fall within the concept of direct participation. A separate question, beyond the scope of this discussion, concerns whether the organisational structure and operational role of *Aerorozvidka* could qualify some of its members as performing a continuous combat function (Henry 2018, p. 273), thereby rendering them targetable on a continuous rather than merely temporary basis.

A different category of civilian intelligence applications is represented by Sentry, a platform developed during the Syrian conflict to provide early warning of imminent Syrian and Russian air strikes. Created by two American developers working closely with Syrian civilians, the application emerged from the perception that indiscriminate aerial bombardment constituted one of the gravest threats facing the civilian population (Dadouch 2018).

The application relies on reports submitted by users who identify military aircraft, describe their observable activities, and indicate their direction of travel. After processing these reports, the system predicts the likely flight path of the aircraft and rapidly disseminates warnings through multiple communication channels, including Facebook, Telegram, Twitter, and local siren systems. These alerts enable civilians expected to be within the danger zone to seek shelter before an attack occurs. At the same time, rescue organisations such as the White Helmets receive advance notification of the anticipated strike location, allowing emergency responders and medical facilities to prepare for casualties and coordinate humanitarian assistance.

The legal difficulty arises from the fact that these warnings may also incidentally benefit military forces. Advance notice of an air strike may enable air defence units to respond more effectively or permit military personnel to evacuate facilities before they are targeted. The resulting question is whether civilians who contribute information through the application thereby engage in direct participation in hostilities. Direct participation requires the cumulative fulfilment of three criteria: the threshold of harm, direct causation, and belligerent nexus. Although aspects of the Guidance remain controversial, these three elements provide a useful analytical framework.

The threshold of harm is readily satisfied. Under the Interpretive Guidance, the relevant conduct must be capable of adversely affecting the military operations or military capacity of a party to the conflict or, alternatively, causing death, injury, or destruction to persons or objects protected from direct attack (Melzer 2009, p. 46). This standard requires only a likely adverse impact upon military operations rather than proof of actual military loss. Information transmitted through the application may clearly frustrate the effectiveness of an anticipated strike. Military personnel who receive advance warning may relocate or

seek protection before the attack is executed, thereby diminishing the operational value of the strike.

The second requirement, direct causation, is likewise fulfilled. The causal relationship between the civilian report and the military response is immediate rather than indirect. Once information concerning an approaching aircraft is submitted, the system rapidly generates warnings that enable defensive measures to be taken within moments. The civilian's contribution therefore forms an integral component of the causal chain connecting the initial report to the subsequent military response (Melzer 2009, p. 52).

The more difficult question concerns the existence of a belligerent nexus. The Interpretive Guidance explains that the relevant conduct must be objectively designed to produce the requisite harm in support of one party to the conflict and to the detriment of another (Melzer 2009, p. 46). Importantly, this assessment focuses on the objective function of the conduct rather than the subjective motivation of the individual performing it. A civilian compelled to fight, for example, remains a direct participant despite acting without any personal desire to harm the opposing force because the conduct itself is objectively directed toward that end.

Applying this approach, the purpose underlying the Sentry application differs fundamentally from applications such as Ukraine's ePPO platform. The latter was specifically created to enhance the operational effectiveness of the Ukrainian armed forces by facilitating the interception of incoming attacks, making its military purpose unmistakable. Sentry, by contrast, was designed primarily to safeguard civilians exposed to aerial bombardment. Although military forces may derive incidental benefits from the warnings generated by the application, those benefits are secondary to its humanitarian function. In this respect, reporting the presence of hostile aircraft through Sentry closely resembles notifying civil defence authorities of an impending air raid. Such communication undoubtedly assists civilian protection, even if military personnel may incidentally benefit from the resulting warning. It would be difficult to maintain that a civilian telephoning civil defence authorities thereby becomes a lawful military target merely because military forces might also react to the warning.

This conclusion is reinforced by the protections afforded to civil defence activities under Additional Protocol I. Article 61 grants civil defence personnel special protection by requiring that they be respected and permitted to perform their humanitarian functions. The protection also extends to civilians who undertake civil defence tasks under the direction of competent authorities, even where they are not formal members of recognised civil defence organisations. Such protection is forfeited only when individuals engage in acts beyond their civil defence responsibilities that are harmful to the adversary. Even in situations where no formal governmental appeal has been issued, the underlying object and purpose of these provisions is to maximise civilian protection against the effects of attack and to facilitate humanitarian response. Characterising the ordinary use of an application such as Sentry as direct participation would therefore be difficult to reconcile with both the structure and the humanitarian rationale of these rules.

Nevertheless, the objective purpose of an act is not necessarily singular. Conduct may simultaneously serve different functions depending upon the manner in which it is employed. Although Sentry was designed for humanitarian purposes, it could intentionally be employed to provide military forces with operational warning. Where a civilian deliberately uses the application for that purpose, the objective character of the conduct changes, and the civilian may satisfy the belligerent nexus requirement by directly contributing to military operations.

Questions concerning objective purpose inevitably give rise to evidentiary uncertainty. Whenever doubt exists regarding whether particular conduct satisfies the requirements of

direct participation, decisions must be made in good faith on the basis of the information reasonably available at the time (US Department of Defense 2023, para. 5.4.3.2). Even so, factual uncertainty may remain.

In the context of the Russia–Ukraine conflict, both parties are bound by Article 50(1) of Additional Protocol I, which requires that any doubt as to whether an individual is a civilian be resolved in favour of civilian status. Although the U.S. Department of Defense disputes the customary status of this rule (US Department of Defense 2023, para. 5.4.3.2), it remains binding upon both Russia and Ukraine. The presumption is particularly relevant where the issue is whether a civilian has become targetable through direct participation in hostilities.

That presumption, however, should not be regarded as irrebuttable. The legal significance of doubt depends upon the operational circumstances of each case. The assessment requires a contextual balancing of factors, including the anticipated military advantage, the quality of available intelligence, and the degree of residual uncertainty surrounding the individual's conduct.

In practice, however, genuine uncertainty will often be limited. Applications specifically designed to support military operations, such as ePPO, ordinarily satisfy the beligerent nexus requirement. Humanitarian warning applications such as Sentry generally do not. Only where credible evidence indicates that such a platform is being deliberately exploited to provide operational warning to military forces does the question of direct participation become genuinely contestable.

5. State Responsibility and System-Level Obligations

IHL also imposes duties on States that are distinct from the issue of individual status. Such duties, rooted in the principle of distinction, rules on precautions and protection of civilians, and the overarching obligation in Common Article 1 GC, require States to act in a manner that minimises foreseeable risks to civilians (Henckaerts and Doswald-Beck 2005, pp. 46–60). The design, promotion and operational integration of civilian intelligence applications are state acts for which responsibility must be assessed under the IHL regime and general rules of state responsibility.

Embedding military functionality in platforms primarily constituting civilian infrastructure creates a foreseeable risk of blurring the civilian/military divide (Capone 2025, p. 48). Article 48 AP I codifies the duty to distinguish between civilians and combatants, while Article 52(2) AP I establishes the presumption that objects typically dedicated to civilian purposes are civilian. When a State integrates an intelligence-gathering feature into a multi-purpose civilian service, the factual basis for such protections changes. The dual-use character of the platform may expose users and the infrastructure itself to attack in manners that would not arise for purely civilian services. IHL bases protection on the factual and normative separation of roles and objects. A State that intentionally collapses such a separation by design choices therefore creates conditions in which civilians are more likely to be placed at risk. Courts and tribunals have repeatedly rooted scrutiny of conduct within foreseeability and the factual environment in which military operations occur (*Prosecutor v Blaškić* 2000; *Prosecutor v Kupreškić et al.* 2000). The issue in this context is whether such foreseeability is sufficient to render a State's policy choice unlawful under IHL.

Because civilian intelligence applications generate information that directly enhances military operations, they may qualify as military objectives under Article 52(2) of Additional Protocol I (Doswald-Beck 1995, para. 40). The intelligence they collect contributes effectively to military action, while disabling or destroying such applications may provide a concrete military advantage. Consequently, their development and deployment must comply with

the obligation imposed by Article 58(a) and (b) of Additional Protocol I, which requires parties to an armed conflict, whenever feasible, to separate military objectives from civilians and civilian objects (*Prosecutor v Kupreškić et al.* 2000, para. 180; *Prosecutor v Kordić and Čerkez* 2001, para. 182). In relation to civilian intelligence applications, this obligation operates at two interconnected levels.

The first concerns the communication networks through which these applications function. Since digital communications rely heavily on infrastructure that simultaneously serves civilian and military purposes, intelligence transmitted through these applications will inevitably travel across dual-use systems, including civilian satellite networks. At present, a complete separation between military and civilian cyber networks is technologically unattainable (Roscini 2014, p. 237). Nevertheless, Article 58 does not impose an absolute obligation; rather, it requires segregation only to the maximum extent feasible. Given the current technological realities, the use of civilian communication networks for the operation of civilian intelligence applications should therefore not, in itself, be regarded as inconsistent with this obligation.

A separate issue arises in relation to the architecture of the application itself. Compliance with Article 58 also depends on whether military functionality has been integrated into civilian digital infrastructure where such integration could reasonably have been avoided. Ukraine's e-Enemy application illustrates this concern. Rather than existing as an independent platform, it was incorporated into Diia, the state's digital governance application, which provides essential civilian services such as tax administration and passport renewal. Embedding a military-relevant application within a platform dedicated to civilian functions undermines the principle of separation because any lawful attack directed against the military functionality could simultaneously affect the broader civilian system. As a result, operations targeting the e-Enemy application may generate collateral damage affecting critical civilian infrastructure and the civilian data maintained within it. Since there was no apparent technical obstacle preventing the creation of a standalone application, reliance on the qualification "to the maximum extent feasible" appears difficult to justify in these circumstances.

The contrast with Ukraine's ePPO application is instructive. Designed to enable civilians to record incoming Russian missiles so that Ukrainian forces can calculate their trajectories, ePPO operates as an independent application available through conventional app stores. Because it is not embedded within a broader civilian digital platform, any military action directed against it is less likely to jeopardise unrelated civilian cyber infrastructure. Its standalone design therefore better reflects the precautionary objective underlying Article 58 by reducing the potential for incidental harm to civilian digital systems.

A further issue relates to the obligations of precautions in attack and protection of civilians. AP I requires parties to do everything feasible to verify that targets are military objectives, to select means and methods of attack to minimise incidental harm,¹ and to take practicable measures to remove civilians from the effects of attacks.² These requirements are forward-looking, in that they require planning and mitigation of risk before action is taken. When a State embeds operational reporting within a civilian platform, it must take reasonable measures to reduce the foreseeable risks to civilian users. These include providing clear warnings about the legal consequences and targeting risks associated with direct participation, implementing robust cybersecurity and data-protection measures to safeguard users' identities and locations, and designing the platform so as to minimise unnecessary civilian integration into military operations (Gisel et al. 2020, p. 294). A key legal question in this respect is whether cyber infrastructure can function as a location in

¹ AP I, Article 57.

² AP I, Article 58.

the sense contemplated by Article 58 AP I, giving rise to the duty to remove or protect civilians. A purposive reading of Articles 57–58 AP I suggests that such protection duties are neutral, in that the obligation to take feasible precautions extends to any context in which civilians are foreseeably endangered by operations that the State organises or encourages. If the foreseeability of civilian exposure is high due to platform design, the duty to adopt mitigating measures similarly becomes high.

Where a State deliberately equips civilians with, or actively encourages them to employ, tools capable of disrupting, degrading, obstructing, damaging, or otherwise affecting the military capabilities or military objectives of an opposing State, it should be under an obligation to take all feasible steps to ensure that those civilians understand the potential legal consequences of their conduct. In particular, civilians should be clearly informed that engaging in activities amounting to direct participation in hostilities may result in the temporary loss of the protection against attack ordinarily afforded to them under international humanitarian law. Such a duty arises whenever the State promotes, facilitates, incentivizes, or otherwise encourages civilian conduct that satisfies the threshold of direct participation in hostilities, or where the conduct of those civilians could be attributable to the State under the rules governing State responsibility. Applied to Ukraine's official support for the ePPO application, this approach would require the Ukrainian authorities to provide users with an explicit warning regarding the legal implications of participating in civilian air-defence activities.

Implementing such a warning would present little practical difficulty. The application could simply require users to acknowledge a clear legal notice before installation or activation. For example, the app might state: *"Warning: Using this application for its intended operational purposes may constitute direct participation in hostilities under international humanitarian law and may result in the loss of civilian protection from lawful attack."* Whether such a notice would discourage some individuals from participating is ultimately beside the legal point. Given the existential circumstances confronting many Ukrainian civilians, it is unlikely that a disclaimer alone would substantially reduce participation. Nevertheless, the possibility that some individuals might decide against using the application after becoming aware of the associated legal risks reinforces, rather than weakens, the case for providing such notice. From both a legal and an ethical perspective, civilians should be afforded the opportunity to make an informed decision before voluntarily engaging in conduct that may expose them to lawful targeting.

The duty to warn and educate affected persons is part of the protective architecture of both IHL and IHRL. States cannot rely on the voluntariness of participation to become absolved of the responsibility to inform civilians of foreseeable dangers that State policy creates (Williamson 2009, p. 460). The European Court of Human Rights in *Osman v United Kingdom* (1998, paras. 115–16) expressed a general principle under human rights law that authorities have positive obligations to implement reasonable operational measures to protect an individual whose life is at risk from the criminal acts of another when the authorities know or ought to know of the real and immediate risk. In the current context, this may be used as a basis for the existence of an obligation for States that mobilise civilians through official platforms. Accordingly, when a State's actions foreseeably expose civilians to specific risks, it must provide adequate warnings, guidance and training to enable informed decision-making (Peperkamp 2024, p. 69). Adequate protection would typically require clear user notifications regarding the likely end use of reports, potential targeting consequences, practical instructions for safe reporting, and ongoing public education campaigns. Without such measures, the State's encouragement of reporting risks being interpreted as negligence, if not a breach of protective duties, given that the risk was both foreseeable and created by State policy. Examples include encouraging civilians to submit real-time

targeting information without informing them that such conduct may amount to direct participation in hostilities; collecting precise geolocation data without adequate safeguards; requiring continuous operational reporting that unnecessarily integrates civilians into the targeting process; or failing to implement reasonable technical and organisational measures to protect users' identities and locations from disclosure.

According to this approach, a State does not breach its positive obligation to protect the right to life where civilians voluntarily choose to engage in direct participation in hostilities after having received adequate information from public authorities regarding the legal and practical consequences of such conduct (Macak 2023, p. 990). Nevertheless, voluntary consent is not necessarily determinative. In considering the legality of civilian cooperation with an Occupying Power, the Israeli Supreme Court attributed only limited significance to a civilian's willingness to enter an area affected by hostilities (*Adalah et al v GOC Central Command, IDF et al.* 2005, para. 24). Instead, the Court emphasized that international humanitarian law seeks to keep civilians separated from military operations and relied on the objective risks associated with such involvement, including exposure to combat-related violence and the heightened danger of abuse or ill-treatment faced by individuals perceived as collaborators. This reasoning was adopted in addition to the prohibition on employing protected persons in support of the Occupying Power's military activities, a rule that lacks an equivalent express provision in the legal framework governing non-international armed conflicts.

International human rights law also offers a useful point of comparison when assessing the obligations owed by States to civilians who are encouraged to participate in military activities. Guidance may be drawn from the standards governing a State's responsibility toward its own armed forces. Although the precise extent of the State's duty to safeguard the lives of military personnel remains contested, it is generally understood that States should not expose their soldiers to avoidable or unjustified risks, particularly where such risks lack a legitimate operational rationale. This protective obligation has been interpreted as encompassing the provision of appropriate military instruction and preparation. In *Smith*, for example, it was argued before the UK Supreme Court that inadequate military training could, in certain circumstances, engage State responsibility for violations of soldiers' right to life (*Smith* 2011, [122]). Similar reasoning may apply where civilians are integrated into the military effort. Once a State actively invites civilians to contribute to military operations, it should also assume responsibility for equipping them with the knowledge and skills necessary to undertake those activities safely and in accordance with the applicable legal framework, including through adequate training (Park 2018, pp. 188–89).

International human rights law further strengthens this conclusion by imposing obligations aimed at protecting individuals who may be affected by the actions of civilians participating in military activities. These positive obligations are particularly relevant in relation to the rights to life and personal liberty (Radončić and Stanley-Ryan 2024, pp. 907–10). In this respect, States are required to take reasonable preventive measures whenever there is a foreseeable risk that an individual's life may be endangered. Such risks are not confined to threats posed by State authorities themselves but also encompass dangers arising from the conduct of private actors, organized groups, or foreign States (UN Human Rights Committee 2019, paras. 21–22).

Common Article 1 GC amplifies such obligations by imposing on parties the duty to ensure respect for the GC. This duty is not restricted to prohibiting unlawful acts by combatants; it also includes State regulatory and organisational measures (Robson 2020, p. 111). When a State designs and promotes a civilian reporting application, it is a policy choice that falls within its sphere of control. If the design foreseeably incentivises civilians to engage in acts that may amount to direct participation in hostilities, the State may bear

responsibility for failing to ensure respect for IHL (Radončić and Stanley-Ryan 2024, p. 915). The protective logic of IHL envisages not only punishment for individual wrongdoing but also prevention through organisational restraint. The doctrine of state responsibility (International Law Commission 2001) requires attribution of conduct to the State when organs or entities acting under its authority undertake the relevant acts. A State-organised reporting system is therefore attributable to the State and may give rise to international responsibility if it breaches IHL obligations.

Accountability for digital mobilisation raises a range of challenges. From the perspective of international criminal law, the doctrines of command and superior responsibility³ hold commanders criminally liable for the failure to prevent or punish the crimes of their subordinates that they knew or should have known of. Applying these doctrines to the context of a cyber-enabled civilian mobilisation gives rise to difficult questions surrounding who qualifies as a subordinate and what constitutes the relevant control. However, the core principle remains, which is that leaders who deploy or promote systems that foreseeably expose civilians may incur responsibility if they fail to take measures within their power to prevent resulting violations (Focarelli 2010, p. 147). Additionally, state responsibility for wrongful acts can be triggered by negligent or deliberate design choices that foreseeably produce unlawful outcomes (Sassòli 2002, p. 414). Therefore, attribution becomes straightforward where the reporting system is a state organ or function.

However, there exist evidentiary limits to the assertion of responsibility. Attribution may be challenged where private developers or volunteer networks play significant roles, and causation may be contested where multiple factors contribute to civilian harm (Bassiouni 1999, pp. 112–15). Yet, such practical difficulties do not eliminate the duty of the State to adopt reasonable protective measures. At the very least, where the State commissions or otherwise materially contributes to a reporting infrastructure, it must satisfy a due diligence standard, requiring that reasonably foreseeable risks be identified and mitigated (Dörmann and Serralvo 2014, p. 716). Failure to take such measures may expose the State to international responsibility under IHL and may also trigger obligations under IHRL and obligations to provide remedies and reparations under the State responsibility regime.

Ultimately, this section reveals a significant jurisprudential and policy conclusion. The law should not be reduced to a binary analysis of whether particular app users are temporarily declassified from civilian status under Article 51(3) AP I. Rather, the more prominent question demands focus be placed on the systemic choices made by States. Doctrinal development should therefore recognise a range of state obligations specific to digital mobilisation, based on a duty of digital separation which segregates civilian administrative services from operational reporting, an affirmative duty to warn and educate, a due diligence obligation to assess and minimise foreseeable harms caused by platform design, and accountability mechanisms for failures to respect these duties. This approach reconciles the individual focus of Article 51(3) AP I with the institutional responsibilities that IHL contemplates under Articles 48, 52, 57 to 58 AP I, and Common Article 1. It offers a workable legal framework for preserving civilian protection in the age of smartphone-enabled conflict.

6. The Adequacy of Existing IHL and Proposed Developments

IHL relies on a core set of principles to regulate the conduct of hostilities and protect civilians. These principles provide a robust legal framework for traditional kinetic warfare. However, the emergence of civilian intelligence applications presents new challenges that expose both the strengths and limitations of existing law. This gives rise to the need to

³ Developed in ICTY jurisprudence such as (*Prosecutor v Čelebići, Delalić, and others* 1998).

evaluate the adequacy of the current IHL framework in addressing the deployment and use of civilian intelligence apps and exploring potential developments to reduce gaps.

6.1. Gaps and Ambiguities

Despite technological innovations, the legal rules governing direct participation in hostilities and the protection of civilians remain applicable in principle. Articles 51(3), 48, 57 and 58 AP I are inherently technologically neutral in that they do not depend on the medium through which hostilities are conducted. The doctrine of direct participation retains applicability, providing a conceptual basis for evaluating whether individuals using intelligence apps materially contribute to hostilities and for assessing the lawful targeting of such individuals (Melzer 2009, pp. 19–30). Therefore, the IHL framework maintains coherence and remains a valid basis for legal analysis, despite the novel context to which it is applied.

There are, however, gaps that plague IHL when applied to the context of civilian digital labour deployed at scale. It provides little guidance on how to treat civilian platforms that embed military reporting functions within broader services (Lavasani 2025, p. 6). While dual-use physical objects are addressed under Article 52(2) AP I, the extension of this concept to digital infrastructure remains unclear. Platforms like Diia, which integrate e-Enemy functionality alongside civilian administrative services, raise questions regarding whether and how the law should classify such systems as dual-use objects, and the protective obligations that follow. Furthermore, the IHL framework does not offer clear mechanisms for assessing direct causation in situations in which data flows through complex processing before influencing military operations (Gisel et al. 2020, p. 302). Traditional artillery spotting features a readily observable causal link to kinetic effects, while digital reporting may be aggregated, filtered or analysed by automated systems before they result in military action. This complicates the determination of direct participation under Article 51(3) AP I, as the immediacy and specificity of the civilian contribution are less tangible. Finally, existing doctrine does not explicitly address the responsibilities of states when they design or deploy systems that foreseeably incentivise civilians to engage in intelligence collection (Voss 2025). While Common Article 1 GC imposes a duty to ensure respect for IHL, the legal framework is silent on how this duty extends to systemic digital mobilisation, raising questions regarding foreseeability and attribution. This lack of context-specific guidance exposes civilians to legal ambiguity and operational risk, particularly where state-promoted apps combine military functions with essential civil services.

6.2. Interpretative, Policy and Governance Proposals

In order to address the ambiguities identified above, conceptual development is both necessary and possible. One potential interpretative approach would be to classify civilian platforms with embedded military functions as dual-use objects, subject to stricter protective measures under Article 52(2) AP I and the precautionary obligations of Articles 57 and 58 AP I. This would establish a legal presumption that states must separate military functionalities and civilian infrastructure to minimise risk. Another approach would be to explicitly clarify that states may not incentivise civilian participation in hostilities without ensuring adequate protections. This would integrate principles of foreseeability from human rights jurisprudence such as *Osman v United Kingdom* (1998) into IHL analysis, emphasising that states may bear responsibility for exposing civilians to harm through policy and design choices that foreseeably encourage DPH. Expanding upon this, a ‘duty of digital separation’ could be developed under Article 58 AP I, requiring states to maintain distinct channels for military intelligence collection and civilian services, similar to the obligation to avoid locating military objectives within or near populated areas. Finally,

further legal criteria could be incorporated into the framework for assessing adequacy of informed consent, risk disclosure and training for civilians participating in digital intelligence activities. This would have the effect of reinforcing protective duties, ensuring that participation does not occur in a legal vacuum and that civilians can make informed choices about the foreseeable consequences of their actions.

From a policy perspective, legal developments should be complemented by practical governance measures. Design principles for civilian intelligence apps could include explicit division of networks, transparency regarding the use of reports, and mandatory risk warnings to participants. Independent oversight mechanisms such as regulatory bodies or review boards could be established to monitor the deployment of wartime digital mobilisation tools, ensuring compliance with precautionary and distinction obligations. Such measures would implement existing IHL principles in the digital context while providing guidance for states seeking to minimise civilian harm.

Ultimately, while existing IHL retains conceptual relevance, its application to civilian intelligence apps reveals both normative and operational gaps. The distinct and explicit treatment of dual-use digital infrastructure, clarification of the limits of incentivising civilian participation, and the development of procedural safeguards are necessary to facilitate the protective objectives of IHL in contemporary conflicts. The integration of doctrinal interpretation with policy-oriented governance will enable states to navigate the challenges posed by digital mobilisation while maintaining compliance with their fundamental legal obligations to civilians and the broader international community.

A civilian report or data-sharing activity is less likely to constitute Direct Participation in Hostilities (DPH) when: the information consists of generic or delayed reports, the data is heavily verified, aggregated, or processed before any operational use, and no traceable link exists between the report and a specific military operation. However, DPH may arise in certain edge cases, particularly where real-time and precise coordinates are provided, the information is used with minimal processing, and clear evidence demonstrates that the report directly enabled a particular strike or military operation.

The “threshold of harm” criterion examines whether the act was capable of causing military harm. Relevant evidence may include: the content of the report, such as the precise location of troops or military equipment, the military relevance and operational usefulness of the information, temporal proximity between the report and the subsequent operation, and internal assessments identifying the information as operationally valuable.

“Direct causation” requires a sufficiently close link between the act and a specific military operation. Evidence relevant to this assessment may include: digital logs, metadata timestamps, GPS records, and message identifiers; chain-of-custody records demonstrating how the information moved through the system; operational or targeting logs referring to the report; communications showing reliance on the information for a particular strike; and strong temporal and geographic correlation between the report and the military action. Where substantial delays exist, the information is heavily aggregated from multiple sources, and no traceable operational link can be established, the activity is less likely to amount to DPH.

The “belligerent nexus” criterion evaluates whether the act was specifically intended to support one party to the conflict and harm another. Relevant indicators may include: statements, messages, or instructions issued by the individual, use of official or state-endorsed platforms, the broader context of the armed conflict and the known purpose of the platform, and repeated or systematic conduct aligned with the military objectives of one party.

Additional considerations include: the specificity, immediacy, and operational value of the information, whether the information served as a decisive input or merely one source

among many, and whether the conduct was continuous and systematic rather than isolated or incidental.

7. Conclusions

The rapid integration of civilian intelligence applications into contemporary conflict environments has introduced significant legal and practical challenges, destabilising the traditional boundary between civilians and combatants. Platforms such as the Ukrainian Diia and its e-Enemy feature, alongside standalone systems such as ePPO, demonstrate how the digital mobilisation of civilians can transform ordinary citizens into sources of military intelligence. This raises urgent, important questions under IHL. Such developments reveal the limits of existing legal frameworks, particularly in the contexts of identifying direct participation in hostilities, defining civilian objects, and imposing responsibility for foreseeable harm.

This article has demonstrated that while the doctrine of direct participation in hostilities retains conceptual value, its application to civilian intelligence apps is plagued by a range of ambiguities. Real-time, geolocated reporting may materially contribute to military operations, yet the indirect or aggregated nature of such contributions complicates assessments of immediacy and causation under Article 51(3) AP I. A restrictive interpretation grounded in ICRC guidance placed emphasis on the limited circumstances in which civilian actions will amount to direct participation. An expansive interpretation highlights the operational significance of digital reporting, similar to traditional forward observation. However, conceptual analysis of DPH alone is not able to fully capture the structural and systemic aspects of civilian mobilisation through state-designed platforms.

A central contribution of this article is that it shifts focus from the individual civilian to the design and deployment choices of the state. Embedding military functionalities within civilian infrastructures creates foreseeable risks that give rise to obligations under Articles 48, 57 and 58 AP I, as well as the duty to ensure respect under Common Article 1 GC. States are responsible for preventing violations of IHL by their military forces and are also under a heightened duty to inform, educate and protect civilians when operational systems foreseeably incentivise participation in hostilities. Apart from individual culpability, negligent or imprudent system design can expose civilians to harm and blur the distinction between civilian and military objects, giving rise to both legal and ethical concerns.

The Ukrainian case study emphasises the need for interpretative development of IHL. Recognition of civilian platforms with embedded military reporting as dual-use objects, clarification of limits on incentivising civilian participation, and the development of a 'duty of digital separation' under Article 58 AP I would facilitate clarity and strengthen protective obligations. Policy measures such as network segmentation, informed consent, risk disclosure and independent oversight would operationalise such doctrinal developments, ensuring that the deployment of digital tools does not undermine civilian safety.

Finally, the Ukrainian case study provides a template for future conflicts in which civilians are mobilised through digital platforms. It demonstrates both the operational advantages and the legal vulnerabilities integral to civilian intelligence apps, providing practical grounding for normative analysis. Through the integration of doctrinal refinement with practical governance, states can uphold the protective objectives of IHL while adapting to the technological realities of modern warfare. Looking forward, the main challenge will be to reconcile the efficiency and utility of civilian-sourced intelligence with the enduring obligation to safeguard civilians, ensuring that technological innovation does not come at the cost of fundamental humanitarian principles.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the author.

Conflicts of Interest: The author declares no conflict of interest.

References

- Adalah et al v GOC Central Command, IDF et al.. 2005. HCJ 3799/02 (Israeli Supreme Court sitting as the High Court of Justice, 23 June 2005). Available online: <https://ihl-databases.icrc.org/en/national-practice/adalah-et-al-v-goc-central-command-idf-et-al-hcj-379902-supreme-court> (accessed on 30 July 2026).
- Bassiouni, M. Cherif. 1999. *Crimes Against Humanity in International Criminal Law*, 2nd ed. Alphen aan den Rijn: Kluwer, pp. 112–15.
- Baxter, Richard R. 1951. So-Called “Unprivileged Belligerency”: Spies, Guerrillas, and Saboteurs. *British Year Book of International Law* 28: 323.
- Benabbass, Sara S., and Marten M. C. Zwanenburg. 2023. The Interaction between the Obligation to Warn and other Rules of IHL. *Journal of International Humanitarian Legal Studies* 15: 52–82. [CrossRef]
- Biggio, Giacomo. 2024. The legal status and targeting of hacker groups in the Russia-Ukraine cyber conflict. *Journal of International Humanitarian Legal Studies* 15: 142–82.
- Boothby, Bill. 2010. “And for Such Time As”: The Time Dimension to Direct Participation in Hostilities. *New York University Journal of International Law and Politics* 42: 741.
- Breeze, Emma J. 2024. Duty to act on knowledge: Precautions, intelligence and the law of armed conflict. *Journal of Conflict and Security Law* 29: 311–29. [CrossRef]
- Capone, Francesca. 2025. *Dual-Use Objects Under International Humanitarian Law: Towards a Paradigm Shift*. The Hague: TMC Asser Press.
- Dadouch, Sarah. 2018. Air strike warning app helps Syrians dodge death from the skies. *Reuters*, September 13. Available online: <https://www.reuters.com/article/world/air-strike-warning-app-helps-syrians-dodge-death-from-the-skies-idUSKCN1LT2J4/> (accessed on 15 July 2026).
- Dinstein, Yoram. 2016. *The Conduct of Hostilities Under the Law of International Armed Conflict*, 3rd ed. Cambridge: Cambridge University Press, p. 176.
- Dinstein, Yoram. 2022. *The Conduct of Hostilities Under the Law of International Armed Conflict*, 4th ed. Cambridge: Cambridge University Press, pp. 123–27.
- Doswald-Beck, Louise, ed. 1995. *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (Prepared by International Lawyers and Naval Experts Convened by the International Institute of Humanitarian Law). Cambridge: Cambridge University Press.
- Dörmann, Knut, and Jose Serralvo. 2014. Common Article 1 to the Geneva Conventions and the obligation to prevent international humanitarian law violations. *International Review of the Red Cross* 96: 707–36. [CrossRef]
- Droege, Cordula. 2012. Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross* 94: 533–78. [CrossRef]
- Focarelli, Carlo. 2010. Common Article 1 of the 1949 Geneva Conventions: A Soap Bubble? *European Journal of International Law* 21: 125–71. [CrossRef]
- Ford, Matthew. 2024. From innovation to participation: Connectivity and the conduct of contemporary warfare. *International Affairs* 100: 1531–49. [CrossRef]
- Giovannelli, Davide. 2025. Handling cyberspace’s state of intermediacy through existing international law. *International Review of the Red Cross* 107: 96–139.
- Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. 2020. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross* 102: 287–334. [CrossRef]
- Hathaway, Oona A., Azmat Khan, and Mara R. Revkin. 2024. The Dangerous Rise of “Dual-Use” Objects in War. *Yale LJ* 134: 2645.
- Henckaerts, Jean Marie, and Louise Doswald-Beck. 2005. *Customary International Humanitarian Law*. Cambridge: Cambridge University Press, pp. 46–60.
- Henry, Sabrina. 2018. Exploring the “Continuous Combat Function” Concept in Armed Conflicts: Time for an Extended Application? *International Review of the Red Cross* 100: 267–85. [CrossRef]
- Hogue, Simon. 2023. Civilian surveillance in the war in Ukraine: Mobilizing the agency of the observers of war. *Surveillance & Society* 21: 108–12. [CrossRef]
- Horbyk, Roman. 2022. The war phone: Mobile communication on the frontline in Eastern Ukraine. *Digital War* 3: 9–24. [CrossRef]

- International Law Commission. 2001. Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. In *Yearbook of the International Law Commission* (UN Doc A/CN.4/SER.A/2001/Add.1 (Part 2)). Geneva: International Law Commission, vol. II, p. 26.
- Lavasani, Somayeh Sadat Miri. 2025. Transformation on the Battlefield: The Impact of Digital Technologies on International Humanitarian Law. *Legal Studies in Digital Age* 4: 1–10. [CrossRef]
- Macak, Kubo. 2023. Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield. *International Review of the Red Cross* 105: 965. [CrossRef]
- Majeed, Nasir, Amjad Hilal, and Arshad Nawaz Khan. 2023. Doctrinal Research in Law: Meaning, Scope and Methodology. *Bulletin of Business and Economics* 12: 559–63. [CrossRef]
- McDonald, Gabrielle Kirk, and Olivia Swaak-Goldman. 2000. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1977. In *Substantive and Procedural Aspects of International Criminal Law*. Leiden: Brill.
- Melzer, Nils. 2008. *Targeted Killing in International Law*. Oxford: Oxford University Press, p. 337.
- Melzer, Nils. 2009. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva: International Committee of the Red Cross.
- Osman v United Kingdom*. 1998. 29 ECtHR 245. Available online: [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-58257%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-58257%22]) (accessed on 30 July 2026).
- Park, Ian. 2018. *The Right to Life in Armed Conflict*. Oxford: Oxford University Press, pp. 188–89.
- Pejic, Jelena. 2007. “Unlawful/Enemy Combatants”: Interpretations and Consequences. In *International Law and Armed Conflict: Exploring the Faultlines, Essays in Honour of Yoram Dinstein*. Edited by Michael N. Schmitt and Jelena Pejic. Leiden: Martinus Nijhoff, p. 335.
- Peperkamp, Lonneke. 2024. Technology and the Civilianization of Warfare. *Ethics & International Affairs* 38: 64–74. [CrossRef]
- Prosecutor v Blaškić*. 2000. (Trial Chamber) ICTY, Case No IT-95-14-T, Judgment, 3 March 2000. Available online: <https://www.icty.org/x/cases/blaskic/tjug/en/bla-tj000303e.pdf> (accessed on 30 July 2026).
- Prosecutor v Bosco Ntaganda*. 2019. (Judgment) ICC-01/04-02/06-2359, Trial Chamber VI, International Criminal Court, 8 July 2019. Available online: <https://www.icc-cpi.int/court-record/icc-01/04-02/06-2359> (accessed on 30 July 2026).
- Prosecutor v Čelebići, Delalić, and others*. 1998. (Trial Chamber) ICTY, Case No IT-96-21-T, Judgment, 16 November 1998. Available online: <https://www.icty.org/x/cases/mucic/tjug/en/> (accessed on 30 July 2026).
- Prosecutor v Dragomir Galić*. 2003. Trial Chamber of the International Criminal Tribunal for the former Yugoslavia, Case No IT-98-29-T, 5 December 2003. Available online: <https://www.icty.org/en/case/galic> (accessed on 30 July 2026).
- Prosecutor v Dušan Tadić*. 1999. Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia, Case No. IT-94-1-A, 15 July 1999. Available online: <https://www.icty.org/en/case/tadic> (accessed on 30 July 2026).
- Prosecutor v Kordić and Čerkez*. 2001. (Judgment) IT-95-14/2-T (ICTY, Trial Chamber, 26 February 2001). Available online: https://www.icty.org/x/cases/kordic_cerkez/tjug/en/ (accessed on 30 July 2026).
- Prosecutor v Kupreškić et al.*. 2000. (Trial Chamber) ICTY, Case No IT-95-16-T, Judgment, 14 January 2000. Available online: <https://www.icty.org/x/cases/kupreskic/tjug/en/kup-tj000114e.pdf> (accessed on 30 July 2026).
- Public Committee Against Torture in Israel v Government of Israel*. 2006. HCJ 769/02 (Supreme Court of Israel, 13 December 2006). Available online: <https://ihl-databases.icrc.org/en/national-practice/public-committee-against-torture-israel-et-al-v-government-israel-et-al-supreme> (accessed on 30 July 2026).
- Quéguiner, Jean-François. 2016. The Principle of distinction: Beyond an obligation of customary international humanitarian law. In *The Legitimate Use of Military Force*. Edited by Howard M. Hensel. Philadelphia: Routledge, p. 167.
- R (Smith) v Oxfordshire Assistant Deputy Coroner (Equality and Human Rights Commission Intervening)* [2010] UKSC 29. 2011. 1 AC 1. Available online: <https://supremecourt.uk/cases/uksc-2009-0103> (accessed on 30 July 2026).
- Radončić, Mina, and Ashley Stanley-Ryan. 2024. Pro patria mori: When States encourage civilian involvement in armed conflict. *International Review of the Red Cross* 106: 897–930. [CrossRef]
- Robson, Verity. 2020. The Common Approach to Article 1: The Scope of Each State’s Obligation to Ensure Respect for the Geneva Conventions. *Journal of Conflict and Security Law* 25: 101–15. [CrossRef]
- Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, p. 237.
- Sassòli, Marco. 2002. State responsibility for violations of international humanitarian law. *International Review of the Red Cross* 84: 401–34. [CrossRef]
- Schmitt, Michael N. 2009. Deconstructing direct participation in hostilities: The constitutive elements. *NYU Journal of International Law and Politics* 42: 697.
- Schmitt, Michael N. 2010. The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis. *Harvard National Security Journal* 1: 5.

- Shereshevsky, Yahli. 2022. International humanitarian law-making and new military technologies. *International Review of the Red Cross* 104: 2131–52. [CrossRef]
- Silvestri, Alessandro. 2019. Direct Participation in Hostilities: Between a Rock and a Hard Place. *Perth International Law Journal* 4: 13.
- Steinbrink, Enno, Laura Gianna Guntrum, and Christian Reuter. 2025. Smartphone and ICT Use among Ukrainian Refugees: Technology Support during War, Flight, and Adaptation in Germany. *Proceedings of the ACM on Human-Computer Interaction* 9: 1–32. [CrossRef]
- Thornhill, John. 2022. Ordinary Ukrainians Wage War with digital tools and drones. *Financial Times*, June 9. Available online: <https://www.ft.com/content/58a5b1a6-bb92-4008-a919-ae6bf73a5419> (accessed on 15 July 2026).
- UN Human Rights Committee. 2019. *General Comment No 36: Article 6 (Right to Life)* (UN Doc CCPR/C/GC/36). Geneva: UN Human Rights Committee.
- US Department of Defense. 2023. *Department of Defense Law of War Manual*; Arlington County: US Department of Defense.
- Voss, Loren. 2025. The overlooked importance of intelligence analysis in IHL. *International Review of the Red Cross* 107: 287–310. [CrossRef]
- Watkin, Kenneth. 2010. Opportunity Lost: Organized Armed Groups and the ICRC “Direct Participation in Hostilities” Interpretive Guidance. *New York University Journal of International Law and Politics* 42: 641.
- Williamson, Jamie A. 2009. Challenges of twenty-first century conflicts: A look at direct participation in hostilities. *Duke Law Scholarship Repository* 20: 457.
- Zaremba, Kateryna, Michèle Knodt, and Jannis Kachel. 2025. Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion. *Media, War & Conflict* 18: 305–24. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.