CROWDSOURCED WAR

Oona A. Hathaway,* Inbar Pe'er,†
Catherine Vera‡

Today, civilians can participate in war as never before. Through smartphones and the internet, civilians can now contribute directly to military operations, whether they are in an active conflict zone or on the other side of the globe. A civilian can, for example, use an app to help military forces intercept threats, join a virtual network of volunteers that conduct cyberoperations against a party to an armed conflict, or use a crowdfunding site to donate funds to provide weapons to combatants. We call this revolution in war fighting "Crowdsourced War." This Article identifies this growing phenomenon, demonstrates how it creates extraordinary new risks for civilians, and recommends critical steps that States like the United States must take to address those risks.

In the wake of the September 11, 2001, attacks on the United States, new interpretations of the law governing armed conflict took shape. Applying these new interpretations to Crowdsourced War, this Article shows how civilians today may unknowingly forfeit their protected status and be regarded as legitimate military objectives under international law. Civilians participating in Crowdsourced War not only unwittingly endanger themselves, they also endanger civilians living and working alongside them. The spread of Crowdsourced War can also lead combatants to suspect all civilians of being participants in war—and thus lawful targets.

To address these problems, we argue it is time to adopt new rules for Crowdsourced War. States, including the United States, should revisit broad interpretations of the law first adopted for a different kind of conflict—interpretations that now make vast numbers of civilians newly vulnerable. States must also take greater responsibility when they invite civilians to participate in Crowdsourced War, including by ensuring that they do not put civilians at unnecessary risk and by informing them of the consequences they may face. Finally, international humanitarian law must be revised to account for this sea change in the way wars are fought. The International Committee for the Red Cross, together with States like the United States that are committed to the rule of law, should renew efforts to tighten standards for targeting civilians. This is necessary to ensure that the era of Crowdsourced War does not become the era in which the distinction between civilian and combatant completely evaporates.

* Gerard C. and Bernice Latrobe Smith Professor of Law, Yale Law School.

† J.D. 2025, Yale Law School.

‡ J.D. Candidate, 2026, Yale Law School. We thank Konstantin Starikov for translating Ukrainian language sources. We thank Gabriela Blum, Connor Brashear, Sarah Donilon, Federica Du Pasquier, Cindy Garay, Fred Halbhuber, Remington G. Hill, Samantha Kiernan, Gabriel Klapholz, Dr. Alexa K. Koenig, Dan Maurer, Ian Park, Eli Scher-Zagier, Carter Squires, Kevin Zhang, and especially Isabel Gensler and Madeline Babin for their very helpful comments and feedback.

Introduction

On October 22, 2022, civilians in southern Ukraine heard the sound of an engine overhead and looked up to see a low-flying object. It was a Russian Kalibr missile, which typically flies at low altitudes—making it difficult to detect by radar, but readily seen by observers on the ground.[1] Several observers took out their cell phones and, using the "ePPO" app, pointed their phones in the direction of the object and clicked on the app's big red button. The app then used their phones' GPS and compass functions to record the geolocation and compute the trajectory of the object.[2] Within two to seven seconds, the information was available

[1] *See* Dan Sabbagh, *Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks*, Guardian (Oct. 29, 2022), https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo [https://perma.cc/Z42W-YLA4]; Michael N. Schmitt & William C. Biggerstaff, *Ukraine Symposium—Are Civilians Reporting with Cell Phones Directly Participating in Hostilities?*, Lieber Inst.: Articles War (Nov. 2, 2022), https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities [https://perma.cc/588G-ZLN7]; Michael N. Schmitt, *Ukraine Symposium—Using Cellphones to Gather and Transmit Military Information, A Postscript*, Lieber Inst.: Articles War (Nov. 4, 2022), https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript [https://perma.cc/ULE4-MEP5]; Lludmyla Tiahnyriadno, *Seven Seconds from Smartphone to Air Defense Maps: How One App Unites Millions to Shoot Down Russian Missiles*, Rubryka (Apr. 3, 2023), https://rubryka.com/en/article/seven-seconds-to-air-defense-maps [https://perma.cc/JJZ7-W7DQ]; *Ingenious Mobile App Helps Down First Russian Missile in Ukraine*, Ukrinform (Oct. 26, 2022) [hereinafter *Ingenious Mobile App*], https://www.ukrinform.net/rubric-ato/3601566-ingenious-mobile-app-helps-down-first-russian-missile-in-ukraine.html [https://perma.cc/YKZ2-YLKY]; *The ePPO Application Has Started Working in Ukraine: How to Notify the Armed Forces of Ukraine About a Missile or a Drone*, Visit Ukr. (Oct. 7, 2022) [hereinafter *The ePPO Application*], https://visitukraine.today/blog/1083/the-eppo-application-has-started-working-in-ukraine-how-to-notify-the-armed-forces-of-ukraine-about-a-missile-or-a-drone?srsltid=AfmBOorG9icvc0Gx_1q-BLud8sJdFNHQ7Fd1h2za5rc2-7dnKcIMvY_p [https://perma.cc/H2SB-XM24]; Danylo Kramarenko & Daryna Vialko, *Ballistic and Cruise Missiles, Drones, and Other Weaponry: What Russia Uses to Attack Ukraine*, RBC Ukr. (Dec. 20, 2024), https://newsukraine.rbc.ua/analytics/ballistic-missiles-drones-and-cruise-missiles-1734721150.html [https://perma.cc/268Z-5SPR].

[2] *See* Sabbagh, *supra* note 1; Schmitt & Biggerstaff, *supra* note 1; Tiahnyriadno, *supra* note 1; *Ingenious Mobile App*, *supra* note 1; *The ePPO Application*, *supra* note 1.

to air defense stations throughout Ukraine.[3] The Ukrainian military responded by shooting down the target "without too much trouble, just like on the simulator."[4] This marked the first successful use of the ePPO mobile app in combat,[5] demonstrating how civilian reports can directly contribute to air defense operations. The app's developer envisions enlisting "the entire population" as partners of the Ukrainian military in what is described as a "web-centric war" where civilians use their smartphones to support military defense efforts.[6]

The rise of digital tools like the ePPO app has fundamentally transformed modern warfare, extending combat engagement far beyond the traditional military forces and physical battlefields. The ePPO app is not alone in enlisting civilians in war. Through smartphones and internet connectivity, civilians can now contribute directly to military operations, whether they are in the middle of a conflict zone or on the other side of the globe. This shift is evident in both local actions, like civilians using apps to help intercept aerial threats, and global initiatives, where international volunteers form virtual networks to conduct coordinated cyberoperations against adversaries.

We call the technological integration and participation of civilians in an armed conflict "Crowdsourced War." Specifically, Crowdsourced War, as we define it, has six key features: (1) A party to an armed conflict; (2) calls on civilians; (3) to support or assist a task or project relating to the armed conflict; (4) where each civilian is usually providing a small contribution in relation to the overall effort; (5) using technology that enables contribution and coordination at a distance; (6) by people who have little direct contact with one another.[7] The rise of Crowdsourced

---

3 *See* Tiahnyriadno, *supra* note 1.

4 *See Ingenious Mobile App*, *supra* note 1; *see also* Tiahnyriadno, *supra* note 1; *The ePPO Application*, *supra* note 1.

5 *The ePPO Application*, *supra* note 1.

6 *See* Sabbagh, *supra* note 1; Schmitt & Biggerstaff, *supra* note 1.

7 This definition draws on a variety of definitions of "crowdsourcing" in the scholarly literature, as summarized in Mahmood Hosseini, Alimohammad Shahri, Keith Phalp, Jacqui Taylor & Raian Ali, *Crowdsourcing: A Taxonomy and Systematic Mapping Study*, 17 Comput. Sci. Rev. 43, 63 (2015). Crowdsourced War is a precise term that systematizes much of what has been loosely referred to as "civilianization of warfare" or "participative warfare." *See* Jethro Norman, *War Volunteers in the Digital Age: How New Technologies Transform Conflict Dynamics*, Danish Inst. Int'l Stud.: Pol'y Brief (July 1, 2024), https://www.diis.dk/en/research/war-volunteers-in-the-digital-age-how-new-technologies-transform-conflict-dynamics [https://perma.cc/XLY4-NYD8]; *see also* Jethro Norman, Matthew Ford & Signe Marie Cold-Ravnkilde, *The Crisis in the Palm of Our Hand*, 100 Int'l Affs. 1361 (2024) (examining the impact of the rapid global proliferation of smartphones on global crises); Lonneke Peperkamp, *Technology and the Civilianization of Warfare*, 38 Ethics & Int'l Affs. 64 (2024) (evaluating the normative dimensions of growing civilian participation in hostilities); Kubo Mačák & Mauro Vignati, *Civilianization of Digital Operations: A Risky Trend*, Lawfare Inst. (Apr. 5, 2023), https://www.lawfaremedia.org/article/

War risks undermining the critical protections for civilians during armed conflict that the four 1949 Geneva Conventions and their additional protocols were meant to provide.[8]

Crowdsourced War is not entirely new—non-State actor groups, for example, have fundraised through online platforms for at least a decade.[9] In the last few years, the war in Ukraine has revealed the myriad new ways in which Crowdsourced War can entangle civilians in waging war as never before. It is a phenomenon that will only become more prevalent as technologies continue to proliferate and become more sophisticated. For a State like Ukraine facing a much more powerful and better-resourced foe, access to Crowdsourced War is a godsend. But there is extreme danger to this shift in the nature of warfare: By participating in Crowdsourced War, civilians may unknowingly forfeit their protected status and be treated as legitimate military objectives under international law. Such threats are not hypothetical. In the Ukrainian village of Motyzhyn, Hennadiy Merchynskyi was executed after Russian troops found pictures of their tanks on his phone.[10] Civilians participating in Crowdsourced War not only endanger themselves, they may also endanger the civilians living and working alongside them and lead combatants to suspect all civilians of being participants in war—and thus lawful targets.

Part I begins by examining five examples of Crowdsourced War—(1) e-Enemy, ePPO, and related apps; (2) the group of volunteer hackers for Ukraine that have been dubbed the "IT Army"; (3) social media

---

civilianization-digital-operations-risky-trend [https://perma.cc/BM2T-32BX] (examining three scenarios of civilian involvement in hostilities through participation in digital operations).

[8] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 50, Aug. 12, 1949, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 1, Aug. 12, 1949, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War art. 1, Aug. 12, 1949, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 50(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) art. 50(1), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

[9] *See* Nicki Kenyon & Josh Birenbaum, *Terrorist Use of Crowdfunding: Terror Finance Watchdog Issues Report About Popular Fundraising Vehicle*, Found. for Def. Democracies (Nov. 29, 2023), https://www.fdd.org/wp-content/uploads/2023/11/fdd-memo-terrorist-use-of-crowdfunding.pdf [https://perma.cc/VB6Q-QG2K].

[10] Tim Judah, *How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders*, Fin. Times (Apr. 10, 2022), https://www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8 [https://perma.cc/F696-92TV]; *see also One Year On, Ukraine War Characterized by Systematic Targeting of Civilians*, Ctr. for Civilians Conflict (Feb. 20, 2023), https://civiliansinconflict.org/press-releases/one-year-on-ukraine-war-characterized-by-systematic-targeting-of-civilians [https://perma.cc/3Z7F-9H7M].

recruiting and online crowdfunding used by both organized armed groups and States; (4) open-source intelligence reporting; and (5) Starlink. Each demonstrates the current use—and future potential—of Crowdsourced War. Part II then turns to the legal framework for targeting civilians in war. It shows that there are many critical areas of disagreement between what we call the "narrow" and the "broad" interpretations of international humanitarian law rules regarding when civilians can be targeted. In Part III, we show that these interpretive debates have major stakes for Crowdsourced War—stakes that those who helped shape the current interpretations almost certainly did not anticipate. These definitions, after all, took shape in the years immediately following the 9/11 attacks in which civilians participating in building and deploying improvised explosive devices (IEDs) were the paradigmatic example. The broad approach developed during that time to define which civilians are targetable now threatens to make immense numbers of civilians into legitimate targets—including Ukrainians who download ePPO and e-Enemy apps, volunteer hackers for the IT Army, American contributors to crowdfunding accounts, civilians who report information they find on the internet to armed forces, and perhaps even Elon Musk.

In Part IV, we argue that the rise of Crowdsourced War poses a range of dangers. Civilians with very limited connection to an armed conflict may unwittingly become classified as targetable civilians directly participating in hostilities or as members of an organized armed group. Once that happens, members of armed forces may regard them as targetable military objectives rather than as civilians entitled to the protections of international humanitarian law. They may also potentially be detailed as unprivileged combatants in armed conflict, denied the protections to which prisoners of war are entitled. These dangers of violence extend beyond the civilians participating—those around them are newly vulnerable as well. If civilians participating in Crowdsourced War are no longer considered civilians but lawful military objectives, their family members, coworkers, and neighbors are at risk of getting caught up in the violence. These dangers are not limited to the countries in which there are armed conflicts—Crowdsourced War allows civilians from around the world to participate in war, and it therefore brings risks to civilians worldwide.

To address these dangers, we argue, it is time to adopt new rules for Crowdsourced War. States, including the United States, should revisit broad interpretations of the law first adopted for a different kind of conflict—interpretations that now make vast numbers of civilians newly vulnerable. States must also take greater responsibility when they invite civilians to participate in Crowdsourced War—including by ensuring that they do not put civilians at unnecessary risk and informing them

of the consequences they may face. Finally, international humanitarian law must be revised to account for this sea change in the way wars are fought. The International Committee for the Red Cross, together with States that are committed to the rule of law, should renew efforts to tighten standards for targeting civilians, to ensure that the era of Crowdsourced War does not become the era in which the distinction between civilian and combatant evaporates.

I
Crowdsourced War

States at war have long relied on their citizens to assist in the war effort to varying degrees. Civilians have contributed indirectly, by manufacturing weapons and military equipment, or by providing economic, administrative, or political support. Civilians have also been involved in more direct ways, such as by acting as lookouts or reporting tactical information about enemy movements. But modern technology has transformed when and how civilians participate in armed conflict, expanding the capacity for civilian engagement in the day-to-day waging of war. Technology now enables civilians to provide real-time intelligence with highly accurate data collection through GPS and other technologies. These capabilities are enhanced further through direct integration between civilian reporting systems and military operations, often facilitated by user-friendly apps and platforms that make participation remarkably accessible. This new phenomenon of Crowdsourced War blurs the line between civilian and combatant in novel ways. This shift carries with it potentially devastating consequences for the civilians involved, who may not fully understand the risks participating in Crowdsourced War entails. Here we introduce several emerging examples of Crowdsourced War to offer a fuller picture of when and how civilian involvement in warfare has transformed in recent years.

A. e-Enemy and ePPO

Ukraine responded to Russia's invasion by deploying several novel open-source digital tools for Ukrainian citizens to use to report and record evidence of the war.[11] At the most basic level, these apps

[11] Regarding ePPO, see generally *supra* note 2. Regarding e-Enemy, see generally Vera Bergengruen, *How Ukraine Is Crowdsourcing Digital Evidence of War Crimes,* Time (Apr. 18, 2022), https://time.com/6166781/ukraine-crowdsourcing-war-crimes [https://perma.cc/DR74-7U87]; Yaroslav Druziuk, *A Citizen-Like Chatbot Allows Ukrainians to Report to the Government When They Spot Russian Troops—Here's How It Works*, Bus. Insider (Apr. 18, 2022), https://www.businessinsider.nl/a-citizenr [https://perma.cc/U535-UTUC]; *How a Chatbot Has Turned Ukrainian Civilians into Digital Resistance Fighters*, Economist (Feb. 22, 2023),

guide users through the process of geo-tagging and time-stamping their footage so that it can be used in future prosecutions. The apps, chatbots, and websites deployed by the Ukrainian government feed the user-provided data into one centralized database set up by the office of Ukraine's Prosecutor General, where the data are categorized and preserved.[12] In addition to recording data for possible later prosecutions, several of these apps enable the Ukrainian military to use civilian-provided data to mount attacks on Russian positions in real-time. Ukrainian civilians using e-Enemy and ePPO have enabled the Ukrainian military to successfully destroy Russian military assets in Ukraine, often within a few seconds of when a civilian uploaded the crowdsourced data.[13]

Both the e-Enemy and ePPO apps reside on the Diia platform, which was created by the Ukrainian government before the war as part of Ukraine's project to digitize the country's government services, increase transparency, and reduce corruption.[14] A critical feature of Diia is that it was designed to rigorously authenticate a user's identity to confirm that they are a Ukrainian citizen.[15] Consequently, when Ukraine was invaded, Diia was an ideal, ready-made platform for hosting war-related apps because it was secure and already in widespread use among Ukrainians.[16] As of 2023, the Diia app was installed on nineteen million Ukrainian smartphones, or about seventy percent of all smartphones in the country.[17]

---

https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters [https://perma.cc/HD46-7VFB]; Drew Harwell, *Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War*, Wash. Post (Mar. 24, 2022), https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion [https://perma.cc/9V6U-VW49]; Lisa O'Carroll, *Meet Diia: The Ukrainian App Used to do Taxes . . . and Report Russian Soldiers*, The Guardian (May 26, 2023), https://www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers [https://perma.cc/PY4S-WHK4]; Lukasz Olejnik, *Smartphones Blur the Line Between Civilian and Combatant,* Wired (June 6, 2022), https://www.wired.com/story/smartphones-ukraine-civilian-combatant [https://perma.cc/NH8H-7MES].

12 Bergengruen, *supra* note 11.

13 *See id.*; Tiahnyriadno, *supra* note 1.

14 The Diia platform was funded by twenty-five million dollars from the U.S. Agency for International Development. *See* Bret Stephens, *Can Samantha Power Win the Battle for Ukraine's Future?*, N.Y. Times (Sept. 13, 2023), https://www.nytimes.com/2023/09/13/opinion/power-ukraine-foreign-aid.html [https://perma.cc/EUS2-6546].

15 *See* O'Carroll, *supra* note 11. Using Diia, a citizen may apply for government benefits, file their tax returns, renew their passports, or claim a free student bus fare. *Id.*

16 After the invasion, Diia incorporated tools to help citizens survive in wartime, such as a tool to create a digital "evacuation document" combining all personal information in one place to "accelerate identification at checkpoints"; an "e-aid" financial support application for small businesses "to keep the economy going"; applications for State-backed mortgages for military and key workers, etc. *Id.*

17 *Id.*

1. e-Enemy

The Ukrainian government rolled out the e-Enemy app ("e-Vorog" in Ukrainian) to the Diia platform in March 2022, just weeks after Russia invaded.[18] e-Enemy provides a convenient way for Ukrainian citizens to gather and preserve open-source evidence relating to Russian aggression. Users can submit footage and enter information to characterize the incident (such as sightings of Russian military equipment in civilian areas; killing or physical violence against civilians by Russians; property damage; looting; any identifying personal characteristics of the Russian soldiers involved; etc.), and e-Enemy will automatically record the geolocation coordinates and other relevant data and transmit them to the Ukrainian government.[19] The user's verified identity is also captured and stored in a centralized database.[20] After a user submits data through the app, they receive a message saying "[e]ach of your shots in this bot means one less enemy."[21]

An example of e-Enemy's efficacy was reported early in the war, when Russian armored vehicles with missile launchers drove into a neighborhood in southern Ukraine. From their headquarters in Kyiv, the Digital Ministry monitored dozens of e-Enemy chatbot reports from residents. Minister Fedorov stated, "Almost every apartment sent us a report . . . . So we could geolocate them to almost every apartment on those two streets."[22]

The Ukrainian government actively encourages citizens to use e-Enemy, stating: "Thanks to your photos and videos, our army will be able to see the enemy's movement in real time and fight it. Help the army—help Ukraine."[23] Indeed, the Ukrainian Digital Minister specifically put out a request for residents of occupied Crimea to use the e-Enemy app to send photos and information about Russian Bastion coastal missile systems located in the occupied territory, requesting their location, refueling stations, and Russian military personnel involved in Bastion system maintenance.[24] The Minister explained that

---

[18] *How a Chatbot Has Turned Ukrainian Civilians into Digital Resistance Fighters*, *supra* note 11.

[19] Bergengruen, *supra* note 11.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *See Ministry of Digital Transformation Launched Telegram Chatbot "eVoroh" (The Enemy Is Here)*, LB.ua (Mar. 10, 2022), https://en.lb.ua/news/2022/03/10/10646_ministry_digital_transformation.html [https://perma.cc/T4ZZ-LLFH].

[24] *Digital Minister Urges Residents of Occupied Crimea to Share Information on Bastion Systems*, New Voice Ukr. (Apr. 9, 2024), https://english.nv.ua/nation/ukraine-is-actively-searching-for-bastion-coastal-missile-systems-in-temporarily-occupied-crimea-50408556.html [https://perma.cc/3S8Q-GQU7].

information on the Bastion systems "is very important . . . . If they are destroyed, it will be a minus for the Russians' ability to strike Ukrainian cities."[25] The Minister also made clear that anyone who provided such information should then delete their messages with the chatbot, as well as any photos and videos.[26] Notably, none of the official announcements from the Ukrainian government appear to contain any specific warnings that use of e-Enemy might subject civilians to higher risk for "directly participating in hostilities," although the recommendation to delete photos and videos after they have been uploaded is an implicit acknowledgement that there is risk involved. As of late 2024, Ukrainian citizens had utilized the e-Enemy app more than 628,000 times.[27]

2. ePPO (e-Air Defense)

Another app that resides on the Diia platform is ePPO.[28] Developed by Ukrainian programmers, the app allows users to record the flight of incoming Russian aircraft, missiles, and drones.[29] A user selects the object from a menu of options (helicopter, drone, missile, explosion, etc.), points their phone in the direction of the object, and presses a single button. The app uses the cell phone's GPS system and compass to send the location and the object's trajectory data to the Ukrainian air defense units.[30] Once alerted to the presence of enemy aircraft, the Ukrainian military may use the data to supplement their targeting radars and then to fire upon the object.[31] According to a developer of the system, it takes about two to seven seconds from the time a user uploads the data to ePPO to when it becomes visible on the maps of all air defense stations throughout Ukraine.[32]

The Strategic Communications Department of the Office of the Commander-in-Chief of the Armed Forces of Ukraine has said that with the ePPO app, "every citizen of Ukraine can join the anti-missile and anti-aircraft defense of our sky."[33] By using the app, "[a]ir

---

25 *Id.*

26 *Id.*

27 Lilia Podolyak, *Ukrainians Sent 628+ Thousand Messages via eVorog Chatbot*, Ukr. News Network (Nov. 1, 2024), https://unn.ua/en/news/ukrainians-sent-628-thousand-messages-via-evorog-chatbot [https://perma.cc/4ZMG-YYSD].

28 PPO refers to the Ukrainian air defense forces. *See Ingenious Mobile App*, *supra* note 1. *See generally supra* note 1.

29 *See Ingenious Mobile App*, *supra* note 1.

30 Sabbagh, *supra* note 1; Schmitt & Biggerstaff, *supra* note 1; Tiahnyriadno, *supra* note 1; *Ingenious Mobile App*, *supra* note 1; *The ePPO Application*, *supra* note 1.

31 *Id.*

32 Tiahnyriadno, *supra* note 1.

33 *Using the ePPO Application, Ukrainians Can Help Air Defense Units Shoot Down Enemy Drones and Missiles*, Ukr. Ministry Def. (Oct. 13, 2022), https://gur.gov.ua/content/

defense specialists will see a mark on the map, it will supplement the radar information and the flying death will be shot down."[34] Again, none of the official announcements appear to warn users about the risk of being classified as direct participants in hostilities or the potential consequences to themselves and those nearby.

The ePPO app has been very useful to the Ukrainian war effort. The drones and missiles commonly used by Russia are small and typically fly at low altitude, and therefore are difficult to detect using conventional radar; however, their low altitude and loud noise make them readily observable to ePPO users on the ground.[35] As noted in the Introduction, the first combat use of ePPO took place on October 22, 2022, when the Ukrainian military shot down an incoming Russian missile after being alerted to it by several citizens using ePPO.[36] Since then, information submitted through ePPO has continued to help the Ukrainian military to destroy many incoming Russian airborne objects, although few details have been released due to security concerns.[37] As of 2023, the ePPO app has been downloaded more than 330,000 times.[38]

3. Other Apps

While e-Enemy and ePPO are the leading Crowdsourcing War apps, several others are also significant. The Stop_Russian_War bot is "an official bot that can be used to report the movement of Russian saboteurs and enemy military equipment."[39] This bot "received thousands of messages about enemy positions and equipment from the first days of the full-scale Russian invasion."[40] The "Bachu.info" app offers similar functionality as e-Enemy, but it works without an internet connection.[41] The Telegram chatbots "russian_war_tribunal_bot" and

---

ukraintsi-cherez-zastosunok-ieppo-mozhut-dopomohty-zenitnykam-zbyvaty-vorozhi-drony-ta-rakety.html [https://perma.cc/X8UA-W2JK]. We thank Konstantin Starikov, PhD, MLIS, Head of Access Services at the Yale Law School Lillian Goldman Law Library, for translating this page for us from its original Ukrainian.

[34] *Id.* (translated by Konstantin Starikov).

[35] *See* Sabbagh, *supra* note 1; Schmitt & Biggerstaff, *supra* note 1; Kramarenko & Vialk, *supra* note 1.

[36] *See Ingenious Mobile App*, *supra* note 1.

[37] Sabbagh, *supra* note 1; *How a Chatbot Has Turned Ukrainian Civilians into Digital Resistance Fighters*, *supra* note 11.

[38] *The "ePPO" App Has Already Been Downloaded by* 330,000 *Ukrainians—Developers*, Ukr. Media Ctr. (Mar. 30, 2023), https://mediacenter.org.ua/the-eppo-app-has-already-been-downloaded-by-330-000-ukrainian-developers [https://perma.cc/L8NQ-7YJB].

[39] *Ukrainian Military Innovations Proved Effective – and They're Changing Modern Warfare. Here Is How*, Off. Website Ukr. (Jan. 31, 2023), https://war.ukraine.ua/articles/ukrainian-innovations-are-changing-approaches-to-modern-warfare [https://perma.cc/2BGF-4TMJ].

[40] *Id.*

[41] *See* StrategEast, Ukrainian Digital Resistance to Russian Aggression 9 (2022).

"warcrime_bot," developed by the Security Service of Ukraine and the Ministry of Justice of Ukraine, can collect evidence of war crimes committed by Russian forces.[42]

As Ukraine began striking Russian territory, Russia also developed an app for Russian civilians to use. The Russian app "Radar" was introduced by the Russian government in late 2023 on the government's main portal. The Russian announcement proclaimed: "Help in the fight against dangerous drones! The Radar app can be used to report suspicious drones or other terrorist emergencies."[43] Radar's interface and functionality are purportedly almost exactly the same as ePPO. The Russian app also comes with a warning, unlike the Ukrainian version, but it is not a warning about the consequences of direct participation in hostilities (DPH). Instead, the warning alerts users that it is a crime to knowingly submit false information via the app, indicating that Russia is concerned about users submitting false reports in an effort to mislead the Russian military rather than about protecting its citizens from the potential consequences of aiding it.[44]

Seeing how useful phone apps have been for Ukraine in combating Russian forces, the United States has begun to test its own smartphone app to combat enemy drones. The app, known as CARPE Dronvm, is designed to allow users to take photos of drones and feed that information to aid defense systems.[45] It is initially intended to be deployed to U.S. forces, but the technology could potentially be shared with partner forces, including non-State actor groups and civilians as well. Indeed, the app developer, MITRE Corp., advertises that the app "empowers military personnel *and first responders* to rapidly identify and report suspicious drone activity."[46] As first responders are usually civilians—including firefighters, law enforcement officers, and

---

[42] *Id.* at 11.

[43] Mary Ilyushina, *Russia Asks Citizens to Use New App to Report Drones and Other Attacks*, Wash. Post (Sept. 20, 2023), https://www.washingtonpost.com/world/2023/09/20/russia-app-drone-citizens-war [https://perma.cc/V94F-2H96]; *see also* David Hambling, *Russians Claim to Develop Smartphone App to Locate Ukrainian Artillery*, Forbes (Jan. 26, 2023), https://www.forbes.com/sites/davidhambling/2023/01/26/russian-smartphone-app-to-locate-ukrainian-artillery [https://perma.cc/XL73-Z2VT].

[44] *See* Ilyushina, *supra* note 43.

[45] *See* Jon Harper, *US Military Tests New Smartphone App That Could Help Shoot Down Drones*, DefenseScoop (July 20, 2023), https://defensescoop.com/2023/07/20/us-military-tests-new-smartphone-app-that-could-help-shoot-down-drones [https://perma.cc/A2ZH-G8LN].

[46] *MITRE Licenses CARPE Dronvm Technology to AeroParagon for Advanced Drone Detection and Response*, MITRE (Sept. 10, 2024) (emphasis added), https://www.mitre.org/news-insights/news-release/mitre-licenses-carpe-dronvm-technology-aeroparagon-advanced-drone [https://perma.cc/322K-EE69].

emergency medical professionals—this statement suggests that the app will soon be made available to civilians.

B. IT Army

The IT Army of Ukraine was created by the Ukraine Ministry of Digital Transformation two days after the Russian invasion as a vehicle for volunteer IT professionals in Ukraine and worldwide to target Russian infrastructure and websites.[47] The IT Army's mandate is to "help Ukraine win by crippling aggressor economies, blocking vital financial, infrastructural and government services, and tiring major taxpayers."[48] Its goal is for "every resident of aggressor countries to feel and tire from their state's aggression."[49]

Thus far, the IT Army's main weapon has been Distributed Denial-of-Service (DDoS) attacks, a hacking attack which overwhelms the targeted website by flooding it with an unmanageable volume of requests.[50] To run these attacks, IT Army volunteers utilize cloud services and tools hosted on repositories such as GitHub,[51] which is owned by Microsoft.[52] Researchers at the Center for Strategic and International Studies estimate that around 2,000 attacks were launched between February and June 2022 and that the IT Army has successfully shut down the websites of Russian government agencies, media, and banking.[53] Among these were the websites for the Moscow stock exchange and Russia's largest lending bank, which were both shut down by the IT Army just a few days after the invasion.[54] The IT Army was also reportedly able to hack into the computer systems of Loesk, an electrical utility, and succeeded in shutting down power to

---

47 *See Ukranian IT Army*, Council on Foreign Rel., https://www.cfr.org/cyber-operations/ukrainian-it-army [https://perma.cc/3WSY-LCXZ]; William Casey Biggerstaff, *The Status of Ukraine's "IT Army" Under the Law of Armed Conflict*, Lieber Inst.: Articles War (May 10, 2023), https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict [https://perma.cc/7BVU-9XMB].

48 IT Army of Ukr., https://itarmy.com.ua/?lang=en [https://perma.cc/H5RV-9FUP].

49 *Id.*

50 *See* David Kirichenko, *Ukraine's Volunteer IT Army Confronts Tech, Legal Challenges*, CEPA: Bandwidth (Nov. 27, 2023), https://cepa.org/article/ukraine-volunteer-it-army-confronts-tech-legal-challenges [https://perma.cc/Q85L-7H9D].

51 Aiden Render-Katolik, *The IT Army of Ukraine*, CSIS (Aug. 15, 2023), https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine [https://perma.cc/46JM-QAP7].

52 *Id.*

53 *Id.*

54 *Id.*; Sarah Coble, *Moscow Exchange Downed by Cyber-Attack*, Infosecurity Mag. (Feb. 28, 2022), https://www.infosecurity-magazine.com/news/moscow-exchange-cyber-attack [https://perma.cc/Q4N8-QW7N]. After the IT Army claimed credit for these shutdowns, Ukrainian Minister Mykhailo Fedorov on social media stated: "The mission has been accomplished! Thank you!" *Id.*

the Leningrad region of Russia.[55] Furthermore, targets have reportedly included the Russian space program and the banking system.[56] While most of the IT Army's attacks to date have been against Russian civilian sites, the IT Army has also targeted websites of government bodies, including the FSB, the United Russia party, and the Ministries of Defense and Foreign Affairs.[57] The IT Army has also purportedly helped thwart Russian cyberattacks against Ukraine, which might be considered a military action if done to defend against attacks on military objectives.[58]

By June 2022, analysts believe the IT Army had evolved into two sections: a public call to action, mobilizing anyone willing to participate in coordinated DDoS attacks against Russian infrastructure targets, and an in-house team supposedly consisting of Ukrainian defense and intelligence personnel, which focuses on defending Ukraine from Russian cyberattacks.[59]

There are numerous other loosely organized hacking groups who sometimes target military assets and could therefore be considered to be directly participating in hostilities. For example, the group Anonymous has "doxed" Russian soldiers in Ukraine by publishing the soldiers' names and other personal identifying information.[60] Doxing could be considered analogous to revealing actionable intelligence about military assets, given that the information might enable military operations against the identified soldiers.

---

55 *Ukrainian Hackers Switched Off Electricity for Leningrad Region in Russia*, Technology.org (Oct. 16, 2022), https://www.technology.org/2022/10/16/ukrainianZswe [https://perma.cc/DT7S-M2NT].

56 Shaun Waterman, *Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts*, Newsweek (Feb. 27, 2023, 6:02 PM), https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970 [https://perma.cc/7LAG-9G8R]. To the extent the Russian space program is used for military purposes, it could be a lawful military objective. There is an ongoing debate about whether "war-sustaining" objects—including the financial system—are lawful military objectives in situations of armed conflict. *See, e.g.*, Oona A. Hathaway, Azmat Khan & Mara Revkin, *The Dangerous Rise of "Dual-Use" Objects in War*, 134 Yale L.J. 2645 (2025) (explaining the debate over targeting war-sustaining objects).

57 Kyle Fendorf, *The Dynamics of the Ukrainian IT Army's Campaign in Russia*, Lawfare (June 15, 2023, 4:00 AM), https://www.lawfaremedia.org/article/the-dynamics-of-the-ukrainian-it-army-s-campaign-in-russia [https://perma.cc/M3NN-PGRC].

58 Anna Lysenko & Seva Gunitsky, *The Invisible Front: Ukraine's IT Army and the Evolution of Cyber Resistance*, Post-Soviet Affs. (May 15, 2025), https://www.tandfonline.com/doi/full/10.1080/1060586X.2025.2503658 [https://perma.cc/TP9G-RQRS].

59 Render-Katolik, *supra* note 51.

60 Eric Jensen & Sean Watts, *Ukraine Symposium – Doxing Enemy Soldiers and the Law of War*, Lieber Inst. (Oct. 31, 2022), https://lieber.westpoint.edu/doxing-enemy-soldiers-law-of-war [https://perma.cc/93Z6-4SMJ].

C. Social Media Recruiting & Crowdfunding

Digital technologies are not only changing the ways that ordinary civilians within a war zone can participate in the war, but also how foreign war volunteers are recruited to support the war. By the mid-2000s, terrorist groups had become highly adept at using social media to recruit new members. Members of the armed forces of States and non-State actor groups (also referred to as organized armed groups) use social media to recruit war volunteers and raise money through crowdfunding campaigns for military equipment and combat activities.[61] The widespread reach of social media enables these recruiters and financiers to operate from anywhere in the globe, not just from within the conflict zone.[62]

1. Organized Armed Groups

Digital technologies have revolutionized traditional collective fundraising practices. Modern crowdfunding platforms, which emerged in the mid-2000s, allow organizations to aggregate numerous small contributions into substantial funding streams with unprecedented ease.[63] This has not gone unnoticed by military actors: Organized armed groups have increasingly turned to crowdfunding platforms to raise funds, sometimes through organizations that present themselves as legitimate humanitarian charities.[64] These groups may establish nonprofits that conduct genuine humanitarian work while simultaneously directing resources to support military operations.[65] The organizations typically solicit donations for seemingly legitimate causes—such as medical care, community development, or disaster relief—while channeling some portion of the funds to armed activities.[66]

This practice predates modern digital technologies: In 2001, the U.S. government took action against the Holy Land Foundation, then the nation's largest Islamic charity, for "providing material support to Hamas by distributing funds through charity committees in the West Bank that paid stipends to the families of suicide bombers and Hamas

---

61 *See infra* Sections I.C.1–2.

62 *See infra* Sections I.C.1–2.

63 Olga Boichak, *Crowdfunding on the Front Lines in Ukraine*, 360 (Feb. 23, 2024), https://360info.org/crowdfunding-on-the-front-lines-in-ukraine [https://perma.cc/9KM2-NEYY].

64 Nicki Kenyon & Josh Birenbaum, *Terrorist Use of Crowdfunding* 1–2, (Found. for Def. of Democracies, Research Memo, Nov. 29, 2023), https://www.fdd.org/wp-content/uploads/2023/11/fdd-memo-terrorist-use-of-crowdfunding.pdf [https://perma.cc/R8KA-JKHG].

65 *Id.*

66 *Id.*

prisoners."[67] Two other Islamic charities in the Chicago area were shut down pending investigation under an executive order that was issued after September 11.[68]

The scale and sophistication of online fundraising has grown dramatically. More than 1,400 crowdfunding platforms now operate globally.[69] Social media platforms amplify these fundraising efforts, allowing organizers to reach vast donor networks through multiple channels—from encrypted messaging services that secure financial data and donation instructions to "super chat" features that enable real-time donations during livestreams.[70] As the United Nations (UN) Counter-Terrorism Committee has noted, even seemingly innocent features like YouTube's donate button can be repurposed to channel funds to armed groups.[71]

2. States

States, too, have relied on social media recruiting and crowdfunding to support their war efforts. Perhaps none have done so as prominently and effectively as Ukraine has since the full-scale invasion by Russia in February 2022.[72] Faced with resource constraints and delays in international military assistance, Ukraine has turned to extensive use of online platforms to facilitate an influx of donations from abroad.[73] Immediately following Russia's 2022 invasion, Patreon

---

[67] *Id.* (citing Press Release, U.S. Dept. of the Treasury, Shutting Down the Terrorist Financial Network (Dec. 4, 2001), https://home.treasury.gov/news/press-releases/po841 [https://perma.cc/RK97-T5R9]); *see also No Cash for Terror: Convictions Returned in Holy Land Case*, U.S. Fed. Bureau Investigation (Nov. 25, 2008), https://archives.fbi.gov/archives/news/stories/2008/november/hlf112508 [https://perma.cc/HZ53-TKZG]; Ill. Advisory Comm. to the U.S. Comm'n on C.R., Arab and Muslim C.R. Issues in the Chicago Metro. Area Post-September 11, at 38 (2003), https://www.usccr.gov/files/pubs/sac/il0503/il0503.pdf [https://perma.cc/H9XU-3ZJU] (reporting on Illinois residents' views on government actions toward Chicago-area Islamic charities).

[68] Exec. Order No. 13224, 66 Fed. Reg. 49079 (Sept. 23, 2001), *amended by* Exec. Order No. 13268, 67 Fed. Reg. 44751 (July 2, 2002), *and* Exec. Order No. 13284, 68 Fed. Reg. 4075 (Jan. 23, 2003); *see also* Ill. Advisory Comm. to the U.S. Comm'n on C.R., *supra* note 67, at 38.

[69] Kenyon & Birenbaum, *supra* note 64, at 2.

[70] *Id.*

[71] *Id.* (citing *CTED's Tech Sessions: Highlights on "Threats and Opportunities Related to New Payment Technologies and Fundraising Methods*," UN, https://www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0 [https://perma.cc/P6RN-FTZ5]).

[72] Ukraine is not alone. Israeli soldiers, for example, have also turned to crowdfunding. *See* Asaf Elia-Shalev, *Six Months into War, Israeli Soldiers Still Count on Donations for Basic Supplies. Why?*, Times of Isr. (Apr. 25, 2024, 4:14 AM), https://www.timesofisrael.com/six-months-into-war-israeli-soldiers-still-count-on-donations-for-basic-supplies-why [https://perma.cc/L67C-7A4A].

[73] Boichak, *supra* note 63.

suspended the account of Come Back Alive, a Ukrainian nonprofit that had used the platform to raise over $250,000 for military training and equipment.[74] Another crowdfunding campaign raised over $7.7 million for a fleet of sea drones in merely thirty-six hours.[75] People's Project, a Ukrainian crowdfunding website, collects donations for military equipment including drones, satellite-powered communication centers, and charging stations for the military.[76] Ukraine has even leveraged celebrity support through United24, the official fundraising platform of Ukraine, where public figures like Star Wars actor Mark Hamill serve as ambassadors for specific fundraising streams, including defense-related donations.[77] The social media platform Bluesky has also emerged as a popular vehicle for fundraising appeals.[78]

While Ukraine relies heavily on international support, Ukraine's crowdfunding efforts also rely on Ukrainian civilians. Social media feeds of Ukrainians are regularly filled with requests to support frontline military units by purchasing essential equipment—from bullet-proof vests to drones.[79] Many brigade commanders make direct appeals to their social media followers for supplies.[80] These crowdfunding efforts "have become part of Ukraine's social fabric, with nearly 80 percent of

---

74 Samantha Cole, *Patreon Banned a Campaign Funding Ukrainian War Efforts*, Vice (Feb. 25, 2022, 10:21 AM), https://www.vice.com/en/article/patreon-banned-return-alive-foundation [https://perma.cc/4YRA-2Z7H] ("Patreon does not allow any campaigns involved in violence or purchasing of military equipment, regardless of their cause.").

75 Elsa Court, *Ukrainian Crowdfunding Campaign Raises $7.8 Million for Sea Drone Fleet in Record 36 Hours*, Kyiv Indep. (Feb. 23, 2024), https://kyivindependent.com/crowdfunding-campaign-raises-7-8 [https://perma.cc/E7W5-8534]. The thirty five drones produced thanks to the money raised by the crowdfunding campaign were used by Ukraine's military to hit the Crimean Bridge as well as nine Russian ships. *Id.*

76 People's Project, https://www.peoplesproject.com/en [https://perma.cc/U3NK-N34V].

77 United24, https://u24.gov.ua [https://perma.cc/7GSY-VMND].

78 BlueSky accounts frequently used for fundraising appeals for the Ukraine war effort include, for example: Nina (@ninaselina.bsky.social), BlueSky, https://bsky.app/profile/ninaselina.bsky.social [https://perma.cc/4RB6-PVP5]; John Sloski (@nafosloski.bsky.social), BlueSky, https://bsky.app/profile/nafosloski.bsky.social [https://perma.cc/QL2N-3RWV]; Way to Ukraine (@waytoukraine.bsky.social), BlueSky, https://bsky.app/profile/waytoukraine.bsky.social [https://perma.cc/79F2-QB6P]; Drobotun Vitalii (@drobotunv.bsky.social), BlueSky, https://bsky.app/profile/drobotunv.bsky.social [https://perma.cc/CSG6-84H9]; Lion Defence Team (@liondefenceteam.bsky.social), BlueSky, https://bsky.app/profile/liondefenceteam.bsky.social [https://perma.cc/AD3U-B98W]; Alex Bond (@alexbondodua.bsky.social), BlueSky, https://bsky.app/profile/alexbondodua.bsky.social [https://perma.cc/X27L-JZXG]; Oksii (@oksii33.ukr.monster), BlueSky, https://bsky.app/profile/oksii33.ukr.monster [https://perma.cc/QE8Z-KD88].

79 Constant Méheut & Daria Mitiuk, *Crowdfunding, Auctions and Raffles: How Ukrainians Are Aiding the Army*, N.Y. Times (Mar. 7, 2024), https://www.nytimes.com/2024/03/07/world/europe/ukraine-war-donations-crowdfunding.html [https://perma.cc/2BV8-P3TJ].

80 *See, e.g.*, Robert Magyar, Telegram (Dec. 19, 2023), https://t.me/robert_magyar/751 [https://perma.cc/UCZ8-AUX7].

the population now donating."[81] According to Ukraine's government, as of September 2024, civilian crowdfunding had contributed "3 percent of Ukraine's total military spending since the war began."[82]

Ukraine has also used digital means to drive unprecedented civilian mobilization. The conflict has seen a significant influx of international volunteers, who have leveraged online platforms and digital technologies to coordinate their efforts, gather resources and equipment funding, and expand their networks of potential recruits.[83] Ukraine's International Legion of Territorial Defense, a ground unit composed of foreign volunteers, recruits via the Internet.[84] While Ukraine established official channels through the International Legion, limited resources meant many potential volunteers turned to informal digital networks for support.[85] Social media spaces, particularly Telegram channels and Reddit communities, became key resources for individuals seeking practical information about travel logistics and unit placement.[86] Through these networks, volunteers found financial backing via a "sponsor a volunteer program" on Reddit while anonymous Telegram users helped guide them through paperwork requirements.[87]

D. Open-Source Intelligence Reporting

Social media, particularly when utilized in conjunction with high-resolution satellite imagery and other datasets and tools, has revolutionized the investigation of human rights abuses and other serious breaches of international law.[88] Most "open source investigations" focus on journalistic reporting, or on the collection, verification, and preservation of evidence for use in later criminal prosecutions.[89] Such investigations may involve years of meticulous research, such as Bellingcat's open-source investigation of Syrian

---

81 Méheut & Mitiuk, *supra* note 79.

82 *Id.*

83 Boichak, *supra* note 63; Norman, *supra* note 7, at 2–3.

84 *How to Join the International Legion of Defense of Ukraine: Detailed Instructions for Foreigners*, Visit Ukr. (May 5, 2023) [hereinafter *International Legion of Defense*], https://visitukraine.today/blog/1797/how-to-join-the-international-legion-of-defense-of-ukraine-detailed-instructions-for-foreigners [https://perma.cc/Y3GN-F28Y].

85 Norman, *supra* note 7, at 2.

86 *Id.*

87 *Id.*

88 *See* Christoph Koettl, Daragh Murray & Sam Dubberley, *Open Source Investigation for Human Rights Reporting*, *in* Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability 12, 14–18 (Sam Dubberley, Alexa Koenig, Daragh Murray, eds., 2020) [hereinafter Digital Witness].

89 "Open-source information" refers to publicly available information that anyone can obtain by observation, request, or purchase, and "open-source investigation" is the process of identifying, collecting, and analyzing open-source information as part of an investigative

dictator Bashar al-Assad's use of chemical weapons.[90] They may also involve detailed efforts to analyze and preserve voluminous bodies of evidence regarding allegations of atrocities in areas of conflict, like those committed in Syria,[91] Myanmar,[92] and Ukraine.[93] Open-source investigations may also document the activities of extremist groups,[94] police and State security forces,[95] organized armed groups,[96] specific individuals,[97] or provide fact-checking and debunking of propaganda.[98]

process. *See* Sam Dubberley, Alexa Koenig & Daragh Murray, *Introduction: The Emergence of Digital Witnesses*, in Digital Witness, *supra* note 88, at 3, 5–9.

90 *See* Eliot Higgins, *The Chemical Munitions Used by the Syrian Government 2012–2018*, Bellingcat (June 14, 2018), https://www.bellingcat.com/news/mena/2018/06/14/chemical-munitions-used-syrian-government-2^#^#-8 [https://perma.cc/8S3P-3FG4].

91 *See, e.g.*, The Syrian Archive Project, https://syrianarchive.org [https://perma.cc/YY2E-GGFM]; Bellingcat's investigations into Syria, Bellingcat, https://www.bellingcat.com/category/news/?fwp_tags=syria [https://perma.cc/P26T-GUEW]; *About*, Syrian Just. & Accountability Ctr., https://syriaaccountability.org/about [https://perma.cc/2T4N-Q4ZL]. The UN's independent investigative mechanism also utilizes open-source evidence in its investigation of Syrian war crimes. *See Collection, Investigation & Analysis*, UN Int'l, Impartial & Indep. Mechanism to Assist in the Investigation & Prosecution of Persons Responsible for the Most Serious Crimes under Int'l Law Committed in the Syrian Arab Republic Since March 2011, https://iiim.un.org/what-we-do/information-and-evidence-collection [https://perma.cc/KLL8-5S65].

92 *See, e.g.*, *Myanmar Witness*, Ctr. for Info. Resilience, https://www.info-res.org/myanmar-witness [https://perma.cc/6RUF-KW8C]. The UN's independent investigative mechanism also utilizes open-source evidence in its investigation of Myanmar. *See Collecting, Evidence and Case Building*, UN Indep. Investigative Mechanism for Myanmar, https://iimm.un.org/en/collecting-evidence-and-case-building [https://perma.cc/TZ45-8L8B].

93 *See, e.g.*, *Eyes on Russia*, Ctr. for Info. Resilience, https://www.info-res.org/eyes-on-russia [https://perma.cc/KG7R-8BDT]; *Investigations*, Bellingcat, https://www.bellingcat.com/category/news/?fwp_tags=ukraine [https://perma.cc/Y56H-F67F] (Bellingcat's investigations into Russia's war on Ukraine); *If You Became a Victim or Witness of Russian War Crimes, Record and Send the Evidences!*, Off. Prosecutor Gen., https://warcrimes.gov.ua/en [https://perma.cc/5CFG-LX3B] (Ukraine's own repository for war crimes evidence).

94 *See, e.g.*, *Investigations*, Bellingcat, https://www.bellingcat.com/category/news/?fwp_tags=far-right [https://perma.cc/AX33-TQ5N] (Bellingcat's investigations into far-right groups).

95 *See, e.g.*, *Police Partially Blind Eight People at Protests*, Berkeley Hum. Rts. Ctr. (2020), https://humanrights.berkeley.edu/projects/police-partially-blind-eight-people-at-protests [https://perma.cc/2VFK-2YAE]; Koettl et al., *supra* note 88, at 23–28.

96 *See, e.g.*, Joshua Wallace, *Tracking Tactics of Boko Haram with Open Source Intelligence*, Conversation (May 1, 2014), https://theconversation.com/tracking-tactics-of-boko-haram-with-open-source-intelligence-26076 [https://perma.cc/9HD3-QEU3].

97 The International Criminal Court (ICC) has relied on open-source information in its prosecutions of Ahmad Al-Faqu Al-Mahdi and Mahmoud Al-Werfalli. *See* Alexa Koenig, *Open Source Evidence and Human Rights Cases*, in Digital Witness, *supra* note 88, at 32, 35–42.

98 *See, e.g.*, Michael Sheldon, Giancarlo Fiorella, Jake Godin & Carlos Gonzales, *Russian Missile Identified in Kyiv Children's Hospital Attack*, Bellingcat (July 9, 2024), https://www.bellingcat.com/news/2024/07/09/russian-missile-identified-in-kyiv-childrens-hospital-attack [https://perma.cc/2LGY-QSAT]. This report not only verified the Russian attack, but also refuted Russian claims that Ukraine had launched an American-made missile that struck the hospital. *Id.*

However, some open-source investigations may yield sufficiently accurate and timely military intelligence which could be used in a Crowdsourced War.[99] Specifically, open-source intelligence (OSINT)[100] can provide real-time intelligence about enemy troop locations, movements, and activities; the locations and types of military equipment; the immediate whereabouts of specific individuals; etc.[101] The Ukrainian private intelligence company Molfar is notable for providing the Ukrainian military with tactical intelligence derived from open-source information.[102] In one instance, Molfar utilized open-source geolocation data extracted from a Russian soldier's social media post to identify the location of the soldier's military unit forty miles behind Russian lines; two days after Molfar provided this data to the Ukrainian intelligence service, the Ukrainian Security Service attacked the site.[103] In another instance, Molfar was able to find and corroborate the exact location of the Pyatnashka Brigade, a unit of the Russian ground forces, based largely on videos of the brigade's anniversary celebration posted on its Telegram channel; one month after Molfar shared the location with Ukrainian intelligence, Ukrainian forces reportedly struck the site.[104]

The private-sector OSINT market is booming and is projected to reach $34.9 billion by 2030.[105] While much of this emerging industry likely will be devoted to providing intelligence and research for corporations, some businesses may emulate Molfar to offer actionable military OSINT to governments, including States engaged in war.[106]

---

[99] As discussed above, the e-Enemy app serves the dual purposes of collecting and preserving evidence of Russian war crimes, as well as providing actionable military intelligence. *See supra* Section I.A.1.

[100] OSINT is information collected for the purpose of addressing a specific intelligence requirement. *See* Digital Witness, *supra* note 88, at 9.

[101] *See generally Military Investigation Services*, Molfar, https://molfar.com/en/services/military-research [https://perma.cc/5VGB-BP2X].

[102] *Id.*

[103] Jack Hewson, *A Private Company Is Using Social Media to Track Down Russian Soldiers*, Foreign Pol'y (Mar. 2, 2023, 6:00 AM), https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence [https://perma.cc/XX9M-TTYT]; *see also* Ukrainian Security Service, Telegram (Oct. 14, 2022), https://t.me/operativnoZSU_chat/100143 [https://perma.cc/E3NE-LNG2] (Telegram post from the Ukrainian Security Service, announcing that "the Armed Forces of Ukraine struck a Russian military training ground in the Boykiv district, ±70 km. from Mariupol").

[104] Jack Hewson, *Ukrainian Company Uses Social Media, Open Source Technology to Counter Russian Invasion*, PBS News (Apr. 19, 2023), https://www.pbs.org/newshour/show/ukrainian-company [https://perma.cc/QZ7J-SW5A].

[105] *See* Hewson, *supra* note 103.

[106] The big five U.S. intelligence conglomerates (Booz Allen Hamilton, CSRA, Leidos, SAIC, and CACI International) are reportedly making significant commitments to open-source intelligence, as are threat intelligence companies, event-detection platforms, and commercial satellite imagery providers. *Id.*

E. Starlink

Just days after Russia's invasion in February 2022, Ukraine requested that Elon Musk activate the services of Starlink—a private satellite internet company wholly owned by SpaceX—to counter widespread internet blackouts.[107] Within months, over 150,000 Ukrainians were using Starlink daily, with the military employing the technology creatively on the battlefield.[108] Ukrainian forces began using Starlink terminals to control unmanned aerial vehicles for surveillance, reconnaissance, and even combat operations, demonstrating the potential military applications of ostensibly civilian satellite networks.

Starlink has become an essential tool for Ukrainian forces. Soldiers upload images of potential targets via the satellite-enabled mobile network, which are then shared with artillery commanders who decide whether and from where to strike.[109] In September 2023, a Ukrainian naval drone with an apparent Starlink terminal was found in Sevastopol, Crimea.[110] The next month, Ukraine used similar drones to attack the Russian naval base there, releasing video footage of the operation.[111] As one Ukrainian soldier put it, "Starlink is our oxygen." Without it, "our army would collapse into chaos."[112]

Though less intuitively obvious than other examples, Starlink fits within our framework. Like e-Enemy and the IT Army, Starlink represents a response to Ukraine's open call for civilian assistance, though in this case through the mobilization of private technological infrastructure rather than individual civilian actions.[113] The fact that

---

107 Amritha Jayanti, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?*, Belfer Ctr. for Sci. & Int'l Affs., (Mar. 9, 2023), https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose [https://perma.cc/FJ6U-WNA5]; *Ukrainian Cities Are Suffering Internet Blackouts*, Economist (Feb. 26, 2022), https://www.economist.com/graphic-detail/2022/02/26/ukrainian-cities-are-suffering-internet-blackouts [https://perma.cc/99N9-829A].

108 Michael Sheetz, *About 150,000 People in Ukraine Are Using SpaceX's Starlink Internet Service Daily, Government Official Says*, CNBC, (May 2, 2022), https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html [https://perma.cc/T3N5-2URV]; *see also* Jayanti, *supra* note 107.

109 *See How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare*, Economist (Jan. 5, 2023), https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare? [https://perma.cc/2EVP-SK8D].

110 *Id.*

111 *Id.*

112 *Id.*

113 Mykhailo Fedorov (@FedorovMykhailo), X (Feb. 26, 2022), https://x.com/FedorovMykhailo/status/1497543633293266944 [https://perma.cc/U6QW-EGN2] ("@elonmusk, while you try to colonize Mars—Russia try to occupy Ukraine! While your rockets successfully land from space—Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand."); *see* Charlie Dunlap,

this assistance came primarily through one company—SpaceX—and its founder does not make it any less an example of Crowdsourced War than a crowdfunding campaign that receives its funding from a single donor. What matters is Ukraine's open call for participation and the mechanisms enabling meaningful civilian contributions, not the ultimate distribution of contributors. Moreover, while Musk made the ultimate decision to provide Starlink services to Ukraine, this required mobilizing hundreds of civilian SpaceX employees to implement and maintain the system,[114] and the company has since created a donation platform enabling individual civilians to fund Starlink terminals for humanitarian causes.[115]

II
Targeting Civilians: Competing Interpretations

The prohibition on targeting civilians is a cornerstone of international humanitarian law. However, this protection is not absolute. This Part examines the complex legal framework governing when civilians may lose their protected status and become legitimate military targets. In international armed conflicts, civilians who directly participate in hostilities temporarily forfeit their immunity from attack, though significant debate exists over what constitutes direct participation and how long targeting authority lasts. In non-international armed conflicts, additional challenges arise concerning how membership in organized armed groups affects targetability.

This Article describes the spectrum of interpretations regarding when civilians qualify as civilians directly participating in hostilities through the lens of two opposing approaches that bookend the range

---

'Dual Use' Commercial Satellites and the International Law of War: A Primer, Lawfire (Oct. 4, 2023), https://sites.duke.edu/lawfire/2023/10/04/dual-use-commercial-satellites-and-the-international-law-of-war [https://perma.cc/W5H4-BVXJ] (discussing the increased use of civilian infrastructure components in space by the United States and its allies in armed conflicts); Graeme Massie, *Elon Musk Helps Ukraine with SpaceX's Starlink Satellites*, The Independent (Feb. 28, 2022), https://www.independent.co.uk/news/world/europe/elon-musk-helps-ukraine-satellites-b2024893.html [https://perma.cc/8VBR-4XGE] ("Starlink terminals are coming to Ukraine! Thank you @elonmusk, thank you everyone, who supported Ukraine!").

114 *See* Sandra Erwin, *Starlink Soars: SpaceX's Satellite Internet Surprises Analysts with $6.6 Billion Revenue Projection*, Space News (May 9, 2024), https://spacenews.com/starlink-soars-spacexs-satellite-internet-surprises-analysts-with-6-6-billion-revenue-projection [https://perma.cc/M8CM-DCX2] (reporting that by 2025 "roughly 3,000 of SpaceX's 13,000 employees are dedicated to Starlink").

115 Michael Kan, *You Can Now Donate a Starlink Dish via SpaceX's New Website*, PC Mag. (Nov. 10, 2022), https://www.pcmag.com/news/you-can-now-donate-a-starlink-dish-via-spacexs-new-website [https://perma.cc/B85V-3ZRC] ("You can now fund a Starlink dish for a charitable cause through a new 'Starlink Donation' website from SpaceX.").

of possible interpretations: what we call the "narrow" approach and the "broad" approach. While actual State practice and scholarly interpretation exist along a spectrum, examining these bookend approaches helps illuminate the practical implications of different interpretations of direct participation in hostilities. The narrow approach is generally paradigmatic of the position taken by the ICRC in its Interpretive Guidance on Direct Participation in Hostilities. This approach emphasizes maintaining civilian protection whenever possible and interprets the conditions for DPH strictly. Meanwhile, the broad approach is exemplified by (but not limited to) the U.S. Department of Defense Law of War Manual and the scholarship it draws upon. It takes a more expansive view of what activities constitute DPH. We apply a similar approach to identifying civilians that can be targeted in NIACs. Here, too, there are a range of interpretations bookended by what we identify as a "narrow" approach and a "broad" approach—again, frequently identified with the ICRC and U.S. Department of Defense Law of War Manual, respectively.

This Part analyzes these interpretive debates and their practical implications for the pool of targetable individuals and the duration during which these individuals remain targetable. Reviewing these interpretive debates makes clear that interpretations of the Law of Armed Conflict developed in the post-9/11 era, largely in the context of the U.S. war against terrorist groups in the Middle East, has significant implications today for the growing phenomenon of Crowdsourced War.

A. Civilians Directly Participating in Hostilities

The principle of distinction forms the foundation of international humanitarian law and is considered essential and inviolable.[116] It mandates that parties to a conflict distinguish between civilian populations and combatants at all times and only direct attacks against

[116] *See, e.g.*, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78–79 (July 8) (stating that the principles of distinction and proportionality are "to be observed by all States whether or not they have ratified the conventions that contain them, because they constitute intransgressible principles of international customary law"). The International Criminal Tribunal for the former Yugoslavia (ICTY) and the Rome Statute of the International Criminal Court (ICC) have reiterated the binding nature of the principle of distinction between combatants and civilians. *See* Prosecutor v. Galić, Case No. IT-98-29-T, Judgment, ¶ 62 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003); The United Nations Rome Statute of the International Criminal Court art. 8(2)(e)(i), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

combatants.[117] Deliberate targeting of civilians is expressly prohibited.[118] However, this protection is not absolute; civilians lose their protection from direct attack "for such time as they take a direct part in hostilities."[119] In other words, civilians who directly participate in hostilities, such as by taking up arms against the enemy, temporarily lose their protected status and can be lawfully targeted during the period of their participation.

The concept of DPH is crucial in determining when civilians lose their protection from direct attack. However, there is significant debate surrounding the precise definition, scope, and application of what constitutes DPH. Some activities are uncontroversially recognized as DPH, such as capturing enemy combatants or their equipment and sabotaging communication lines.[120] The same is true of planting and detonating an improvised explosive device (IED),[121] operating weapons systems (such as manning an anti-aircraft gun or launching a missile),[122] and gathering tactical intelligence (like acting as a spotter for artillery fire or providing real-time information on enemy troop movements for an immediate attack).[123]

However, many activities fall into a gray area where there is less consensus on whether they constitute DPH. These include transporting

---

117 *See* Additional Protocol I, *supra* note 8, art. 50(1). Notably, Additional Protocol I defines civilians by exclusion as all persons who are not combatants. *Id.*

118 *Id.* art. 51(2). These concepts are also reflected in the Rome Statute of the ICC, which provides that "[i]ntentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities" constitutes a war crime in international armed conflicts. *See* Rome Statute, *supra* note 116, art. 8(2)(b)(i).

119 Additional Protocol I, *supra* note 8, art. 51(3).

120 *See, e.g.*, U.K. Ministry of Def., The Joint Service Manual of the Law of Armed Conflict 54 (2004) [hereinafter U.K. Defence Manual] (listing some activities that are unambiguously classified as DPH); *see also* Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 1 N.Y.U. J. Int'l L. & Pol. 697, 710 (2010).

121 *See* Int'l Comm. Red Cross, Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law 54 (Nils Melzer ed., 2009) [hereinafter ICRC Interpretive Guidance], https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc-002-0990.pdf [https://perma.cc/F75T-6WMM].

122 *See* Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 Chi. J. Int'l L. 511, 544 (2005); *see also* U.K. Defence Manual, *supra* note 120, at 54.

123 *See* ICRC Interpretive Guidance, *supra* note 121, at 34–35 (categorizing individuals whose function is limited to the collection of intelligence other than of a tactical nature as not DPH, with the implication that those whose function is the collection of tactical intelligence can be DPH); Prosecutor v. Strugar, Case No. IT-01-42-A, Appeals Chamber Judgment, ¶¶ 176–79 (July 17, 2008) (listing "transmitting military information for the immediate use of a belligerent" and "serving as guards, intelligence agents, lookouts, or observers on behalf of military forces" as examples of DPH); HCJ 769/02 Pub. Comm. Against Torture in Israel v. Gov't of Israel, ¶ 35 (2005) (Isr.) [hereinafter *Targeted Killings*] (categorizing "a person who collects intelligence on the army" as DPH).

ammunition or combatants to the frontline,[124] assembling and storing IEDs,[125] providing logistical support (such as maintaining vehicles in a combat zone),[126] providing financial support to armed groups,[127] and engaging in recruiting and propaganda.[128] The application of the concept of DPH to these activities has been subject to considerable debate and varying interpretations.[129]

In an effort to provide clarity, in the years immediately following the 9/11 attacks and the start of the U.S. counterterrorism campaign, the International Committee of the Red Cross (ICRC) launched an informal expert process to develop guidance on the "notion of Direct Participation in Hostilities."[130] Although the ICRC initially aimed to produce a consensus document, this goal was abandoned when the convened experts failed to reach agreement.[131] The ICRC's resultant Interpretive Guidance concluded that direct participation in hostilities "refers to specific acts carried out by individuals as part of the conduct of hostilities between parties to an armed conflict."[132] To constitute DPH, a specific act must meet all three of the following elements:

1. Threshold of harm: "the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict

---

124 Schmitt, *supra* note 120, at 710–11.

125 ICRC Interpretive Guidance, *supra* note 121, at 53 n.123.

126 *Targeted Killings*, *supra* note 123, ¶ 35 (explaining that a civilian "who operates weapons which unlawful combatants use, or supervises their operation, or provides service to them, be the distance from the battlefield as it may" is DPH); Prosecutor v. Strugar, Case No. IT-01-42-A, Appeals Chamber Judgment, ¶¶ 176–79 (Int'l Crim. Trib. for the Former Yugoslavia July 17, 2008) (A civilian who "provid[es] specialist advice regarding the . . . correct maintenance of the weapons" is not DPH); U.K. Defence Manual, *supra* note 120, at 40 ("Armed forces increasingly rely on the technical and administrative support of civilians. Civilians who are authorized to accompany the armed forces in the field in such capacities remain non-combatants, . . . [t]hey may not be directly attacked").

127 *See* Ryan Goodman & Derek Jinks, *International Law, U.S. War Powers, and the Global War on Terrorism*, 118 Harv. L. Rev. 2653, 2658 nn.30 & 32 (2005) (explaining that the United States has previously designated individuals "involved in terrorist financing" and an individual who served as an "accountant and treasurer" as DPH (citations omitted)); *Targeted Killings*, *supra* note 123, ¶ 35 (explaining that providing "general support, including monetary aid" does not constitute DPH).

128 *See* Goodman & Jinks, *supra* note 127, at 2658 n.32 (describing a U.S. military commission charging an unlawful combatant for creating "several instructional and motivational recruiting video tapes" (citing al Bahlul v. United States, 840 F.3d 757 (D.C. Cir. 2016))).

129 *See* Schmitt, *supra* note 120, at 710.

130 Nils Melzer, Int'l Comm. of the Red Cross, International Humanitarian Law: A Comprehensive Introduction 89 (2016).

131 ICRC Interpretive Guidance, *supra* note 121, at 9–10; Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 Harv. Nat'l Sec. J. 5, 6 (2010).

132 ICRC Interpretive Guidance, *supra* note 121, at 43.

or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack";

2. Direct causation: "there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part"; and

3. Belligerent nexus: "the act 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."[133]

While the ICRC's three criteria provide a useful framework for understanding DPH, their interpretation and application remain contentious, leading to several critical areas of disagreement about when and whether civilians may be lawfully targeted.[134]

B. Critical Areas of Disagreement in International Armed Conflicts

As noted at the outset of this Part, there were significant differences among States and other actors, including the ICRC, over the proper interpretation of civilians directly participating in hostilities. While there is agreement that such civilians may be targeted, positions diverge on various factors. Here we outline four: (1) where in the causal chain the civilian is located; (2) the temporal scope of the civilian's targetability (that is, for how long the civilian is targetable); (3) whether civilians who repeatedly participate in hostilities remain targetable when not actively participating (and, if so, how much participation is enough to be "repeated"); (4) when and how a civilian who is directly participating in hostilities may cease participation and thus no longer be targetable. Here we discuss the different answers given to these questions by those adopting the narrow and broad interpretations. This sets the stage for our analysis in Part III, where we demonstrate the significant consequences of the answers to these questions for civilians participating in Crowdsourced War.

1. Where in the Causal Chain Is the Civilian Located?

One of the most significant areas of disagreement concerns the interpretation of "direct" participation and the extent of the causal chain that qualifies an act as DPH.[135] This debate centers on how closely

133 *Id.* at 16.
134 *See* Schmitt, *supra* note 120, at 710.
135 *See* Schmitt, *supra* note 131, at 29–30.

an act must be linked to a harmful act to qualify as DPH.[136] Under the narrow view, for an act to qualify as DPH, the resulting harm must occur within a single causal step.[137] This "one-causal-step" criterion limits DPH to acts that are reasonably expected to directly cause harm or form an integral part of a specific military operation which is reasonably expected to directly cause harm.[138] Under this view, activities such as the production and shipment of weapons and the provision of financial support to armed groups generally do not qualify as DPH because they are too far removed from the actual infliction of harm.[139]

In contrast, some international actors take a broader view of causation. For example, the U.S. Department of Defense Law of War Manual (DoD Manual) suggests that any "actions that are, by their nature and purpose, intended to cause actual harm to the enemy" could potentially fall under the DPH umbrella.[140] This interpretation extends

136 Recall that the ICRC defines a "harmful act" as one that is "likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack." ICRC Interpretive Guidance, *supra* note 121, at 47. Note that "[t]he qualification of an act as direct participation does not require the *materialization* of harm reaching the threshold but merely the objective *likelihood* that the act will result in such harm." *Id.* The U.S. Department of Defense does not have an explicit equivalent to the ICRC's "threshold of harm" requirement, but they similarly define what we call "harmful acts" as "acts that are an integral part of combat operations or that effectively and substantially contribute to an adversary's ability to conduct or sustain combat operations." U.S. Dep't of Def., Law of War Manual 237, § 5.8.3 (updated July 2023) [hereinafter Law of War Manual]. What exactly constitutes an adverse military effect sufficient to amount to direct participation is an inquiry that is analytically blurred with the broader issue of causation discussed in this Section.

137 *See* ICRC Interpretive Guidance, *supra* note 121, at 53.

138 *Id.* at 58 ("The requirement of direct causation is satisfied if either the specific act in question, or a concrete and coordinated military operation of which that act constitutes an integral part, may reasonably be expected to directly – in one causal step – cause harm that reaches the required threshold.").

139 *See id.* at 53 (listing examples of indirect participation, rather than direct participation); *see also* Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 § 1679 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter Commentary AP] ("[T]o restrict this concept [i.e. of 'direct participation in hostilities'] to combat and to active military operations would be too narrow, while extending it to the entire war effort would be too broad, as in modern warfare the whole population participates in the war effort to some extent . . . ."); Prosecutor v. Strugar, Case No. IT-01-42-A, Appeals Chamber Judgment, ¶¶ 176–79 (July 17, 2008) ("[D]irect participation in hostilities cannot be held to embrace all activities in support of one party's military operations or war effort."). It is worth noting that the ICRC itself deviates from the narrow view in one respect: It states in its Guidance that, production and transport of weapons "carried out as an integral part of the specific military operation designed to directly cause the required threshold of harm" may constitute direct participation, even though the production and transportation may be more than one causal step removed. *See* ICRC Interpretive Guidance, *supra* note 121, at 53.

140 Law of War Manual, *supra* note 136, at 236, § 5.8.3.

to activities such as training,[141] logistical support,[142] and providing safe houses and food to a combatant.[143] Under this broader view, individuals involved in the production of new kinds of weapons or the provision of logistical support might be considered targetable.[144]

The differing interpretations lead to varying assessments of specific activities. One area where this divergence is evident is intelligence gathering. Under the narrow view, only tactical intelligence directly linked to specific military operations would qualify as DPH.[145] For example, a civilian acting as a spotter for artillery fire would be considered to be directly participating in hostilities, but a civilian analyst working on long-term strategic intelligence would not. In contrast, the broad view might consider a wider range of intelligence activities as DPH.[146]

Weapons maintenance is another area where the narrow and broad interpretations differ. While a civilian operating a weapons system or a non-weapons system like a UAV used for target location clearly qualifies as DPH, the classification becomes more nuanced when considering various types of maintenance activities.[147] The

---

141 *Id.*

142 *Id.*

143 Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. Int'l L. & Pol. 641, 680–81 (2010).

144 Law of War Manual, *supra* note 136, §§ 5.8.3, 5.8.3.1; *see also id.* § 5.8.3 n.294 (asserting that the contributions of civilian personnel participating in the U.S. atomic weapons program Project Manhattan "was of such importance as to have made them liable to legitimate attack" and making a similar claim regarding "scientists involved in research and development at German rocket sites at Peenemunde in 1944" (quoting W. Hays Parks, Chief, Int'l L. Branch, Off. of the Judge Advoc. Gen., Dep't of the Army, *Memorandum of Law: Executive Order 12333 and Assassination*, Army Law., Dec. 1989, at 4, 6)); *cf. id.* § 5.8.3.2 (listing as an example of acts not considered taking a direct part in hostilities "working in a munitions factory or other factory that is not in geographic or temporal proximity to military operations but that is supplying weapons, materiel, and other goods useful to the armed forces of a State"); *id.* § 5.8.3.2 n.304 ("workers in defense plants or those engaged in distribution or storage of military supplies in rear areas . . . do not pose an immediate threat to the adversary and therefore would not be subject to deliberate individual attack" (quoting Michael Bothe, Karl Josef Partsch & Waldemar A. Solf, New Rules for Victims of Armed Conflicts 344 (2013))).

145 *See* ICRC Interpretive Guidance, *supra* note 121, at 35 (listing "the collection of intelligence other than of a tactical nature" as an example of indirect participation rather than DPH). The ICTY shares this view. *See* Prosecutor v. Strugar, Case No. IT-01-42-A, Appeals Chamber Judgment, ¶¶ 176–79 (July 17, 2008) (distinguishing between a person who is "gathering and transmitting military information" and a person who is serving as an "intelligence agent[], lookout[], or observer[] on behalf of military forces." The former would not be considered DPH, while the latter would be considered DPH).

146 Dep't of the Navy & Dep't of Homeland Sec., The Commander's Handbook on the Law of Naval Operations 8–2 (2022) (listing "serving as a lookout, guarding a military objective, or gathering intelligence for enemy military forces" as an example of DPH); *Targeted Killings*, *supra* note 123, ¶ 35 (categorizing "a person who collects intelligence on the army, whether on issues regarding the hostilities, or beyond those issues" as DPH).

147 *See* Schmitt, *supra* note 122, at 544.

narrow view generally excludes weapons maintenance from DPH, considering it to be building up military capacity rather than directly causing harm.[148] However, broader interpretations might include maintenance activities that directly prepare equipment for immediate combat operations.[149] For instance, a civilian technician conducting last-minute checks on a fighter jet immediately before a combat mission might be considered DPH under the broad view. The broad view could also extend to scenarios such as civilian contractors repairing battle-damaged tanks near front lines, technicians loading missiles onto combat drones prior to launch, specialists calibrating artillery guidance systems before an offensive, engineers conducting emergency repairs on military communication systems during operations, or maintenance crews refueling and rearming attack helicopters between sorties.[150] The Judge Advocate General School of the Army takes a broad view on this matter, arguing that a contract technical advisor who works daily with armed forces to enhance weapon system effectiveness would be considered DPH.[151]

Similarly, the creation and dissemination of propaganda by civilians for armed groups, particularly when focused on recruitment, presents a gray area. The narrow view does not consider the general recruitment and training of personnel as DPH, as these activities do not directly cause harm.[152] Under the narrow view, a civilian engaging in training or recruitment activities for an armed group would only be considered DPH "where persons are specifically recruited and trained for the execution of a predetermined hostile act."[153] However, "broader interpretations, especially in the context of counter-terrorism operations in a non-international armed conflict, might view recruitment as . . . an integral part" of the hostile campaign.[154] Likewise, the broad view

148 *See* ICRC Interpretive Guidance, *supra* note 121, at 53.

149 *See, e.g.*, *Targeted Killings*, *supra* note 123, ¶ 35 (defining "a person who operates weapons which unlawful combatants use, or supervises their operation, or provides service to them, be the distance from the battlefield as it may" as DPH).

150 Schmitt, *supra* note 122, at 545.

151 Lisa L. Turner & Lynn G. Norton, *Civilians at the Tip of the Spear*, 51 A.F. L. Rev. 1, 31 (2001).

152 ICRC Interpretive Guidance, *supra* note 121, 53 ("[A]lthough the recruitment and training of personnel is crucial to the military capacity of a party to the conflict, the causal link with the harm inflicted on the adversary will generally remain indirect.").

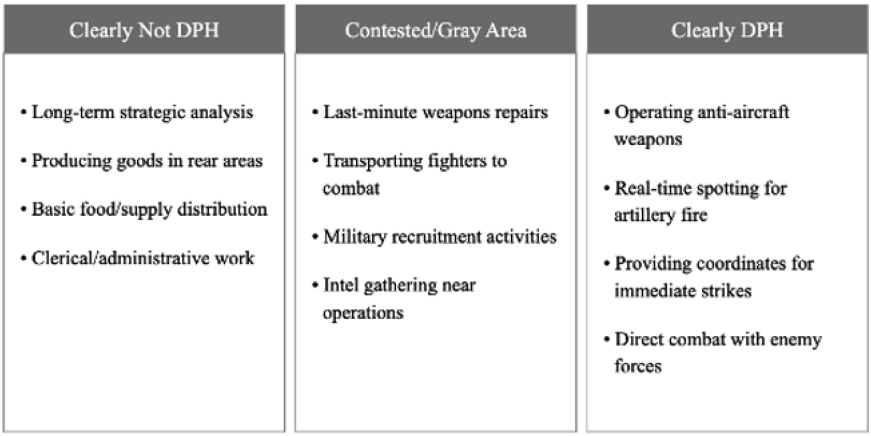
153 *Id*.

154 Law of War Manual, *supra* note 136, at § 5.8.3; *see also Targeted Killings*, *supra* note 123, ¶ 37 ("[T]he 'direct' character . . . should not be narrowed merely to the person committing the physical act of attack. Those who have sent him, as well, take 'a direct part.' The same goes for the person who decided upon the act, and the person who planned it." (citation omitted)). Notably, the DoD cites this passage from *Targeted Killings* for the proposition that "planning, authorizing, or implementing a combat operation against the opposing party, even if that person does not personally use weapons or otherwise employ

might sometimes view the dissemination of propaganda, including by the media, as DPH.[155]

Figure 1 summarizes the differences between the broad and narrow views by providing illustrative examples of actions they agree are not direct participation (clearly not DPH), those they agree are direct participation (clearly DPH), and those on which the broad approach considers DPH, but the narrow view does not (contested/gray area).

FIGURE 1: DIRECT PARTICIPATION IN HOSTILITIES CLASSIFICATION



2. *For How Long Can the Civilian Be Targeted?*

What is the precise time frame during which civilians forfeit their protected status due to their involvement in hostile acts?[156] Put more simply, how long is a civilian actually participating in hostilities and thus targetable? This is another question on which there are differing views.[157] These competing views turn on conflicting interpretations of

destructive force in connection with the operation" constitutes DPH. LAW OF WAR MANUAL, *supra* note 136, at 239, § 5.8.3.1.

155 *See, e.g.*, OFFICE OF THE PROSECUTOR, FINAL REPORT TO THE PROSECUTOR BY THE COMMITTEE ESTABLISHED TO REVIEW THE NATO BOMBING CAMPAIGN AGAINST THE FEDERAL REPUBLIC OF YUGOSLAVIA ¶ 47 (June 13, 2000) ("Whether the media constitutes a legitimate target group is a debatable issue. If the media is used to incite crimes, as in Rwanda, then it is a legitimate target.").

156 *See* Schmitt, *supra* note 131, at 36 (detailing the lack of consensus about the specific time at which civilians forfeit their protected status).

157 LAW OF WAR MANUAL, *supra* note 136, § 5.8.4 ("There has been a range of views about the duration for which civilians who have taken a direct part in hostilities forfeit protection from being made the object of attack."); NILS MELZER, BACKGROUND PAPER – DIRECT PARTICIPATION ON HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW – EXPERT MEETING OF OCT. 25–26, at 34 (2004) ("At one end of the spectrum were experts who . . . favoured strictly limiting loss of protection to the period where DPH is actually being carried out. At the

the "for such time" clause in Article 51(3) of Additional Protocol I: "Civilians shall enjoy the protection afforded by this Section, unless and *for such time* as they take a direct part in hostilities."[158] The temporal scope of DPH carries substantial implications for determining when a civilian becomes a legitimate target and when they regain their protected status.

The narrow view answers the question by concluding that deployment "begins only once the deploying individual undertakes a physical displacement with a view to carrying out a specific operation" and concludes "once the individual in question has physically separated from the operation."[159] The narrow view further defines preparatory measures to include only those "of a specifically military nature and so closely linked to the subsequent execution of a specific hostile act that they already constitute an integral part of that act."[160] This narrow interpretation aims to limit the window of vulnerability for civilians who engage in DPH. To illustrate how this approach works, consider a civilian who agrees to plant an IED. Under the narrow view, the civilian would only be considered to be DPH and therefore lawfully targetable from the moment they begin traveling to plant and detonate the device until they have returned from the operation.[161] The time spent planning the attack or acquiring the materials would not fall within the temporal scope of their participation.[162]

In contrast, others adopt a broad view, arguing that the period of participation extends as far before and after a hostile action as a causal connection exists.[163] Under this interpretation, the starting point of DPH is often pushed significantly earlier. It might include initial planning stages, gathering of intelligence, or acquisition of necessary materials for an attack. Furthermore, the period during which an individual could be considered a legitimate target might continue long after the hostile act itself, potentially extending to activities such as retreating from the area of operations or returning to civilian life. Under this broad view, the civilian planting an IED might be considered to be directly participating in hostilities from the moment they begin planning the attack, through the acquisition of materials, the planting of the device,

other end were experts who said that, once a person [began DPH, they lost protection until they] clearly [and] . . . definitively disengage[d]").

158 Additional Protocol I, *supra* note 8, art. 51(3) (emphasis added).

159 ICRC Interpretive Guidance, *supra* note 121, at 67.

160 *Id.* at 65–66.

161 *Id.* at 54.

162 *Id.*

163 Schmitt, *supra* note 131, at 36–37.

and potentially for some time after the operation as they evade capture or prepare for future operations.[164]

The consequences that flow from these divergent interpretations can be significant, especially when differences regarding both temporal scope and causal chain are factored into the DPH analysis. The interaction between causal chain and temporal scope creates a spectrum of interpretations that dramatically affects both *who* can be targeted and *for how long*. To illustrate how these interpretations interact, it is useful to first examine an uncontroversial example of DPH. Consider the civilian who plants an IED—an activity that both narrow and broad interpretations would consider direct participation in hostilities. Under the narrow view, this civilian would only be targetable during the actual operation—from departure to plant the device until return. However, even while keeping the causal chain narrow, the broad view would extend targetability to include the planning phase, acquisition of materials, and potentially a period after the operation during which the civilian might be preparing for future attacks.[165] In this way, temporal scope alone can significantly expand the window of vulnerability from hours to weeks.

The combined effect of differing interpretations is even more striking. Take the weapons maintenance technician example. Under the narrow view, routine maintenance would not qualify as DPH at all, making temporal scope irrelevant. However, if we apply the broad view that considers maintenance as DPH, the temporal question becomes critical. A narrow view of temporal scope would limit targetability to only when the technician is actively working on weapons systems. In contrast, combining a broad view of the causal chain with a broad view of the temporal scope would mean the technician might be considered targetable throughout their entire period of employment, potentially extending to months or years.

The spectrum of interpretations creates different outcomes in various scenarios. At the most restrictive end (narrow causal and temporal interpretations), consider a civilian providing intelligence tips about enemy force movements. Under this interpretation, they would only be targetable during the specific moments of transmitting the

---

164 *See* ICRC Interpretive Guidance, *supra* note 121, at 53 n.123 (noting the division amongst experts on whether the creation of IEDs should be considered direct participation in hostilities).

165 Indeed, the Law of War Manual views "everything from reconnaissance of the potential target . . . to the provision of a safe house and food, and the explosives-laden vehicle or suicide belt" as an activity that constitutes DPH. *See* Law of War Manual, *supra* note 136, § 5.8.3, n.292 (citing Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. Int'l L. & Pol. 641, 681 (2010)).

intelligence, since both the act itself might be considered too removed from direct harm and the temporal scope is limited to the actual conduct. This creates a very limited window of vulnerability.

At the most expansive end, the combination of broad interpretations of causation and temporal scope can dramatically expand both the pool of targetable civilians and the duration of their targetability. Consider a programmer who develops malware designed to disrupt enemy military communications. Taking broad views across both axes, not only would this software development be considered sufficiently close in the causal chain to constitute DPH, but the temporal scope would extend from initial planning through development, deployment, and post-deployment support. This could result in months of potential targetability. The combination of broad interpretations can exponentially increase both the types of activities that qualify as DPH and the duration of vulnerability, potentially transforming what might have been a few hours of targetability under the narrow interpretations into a semi-permanent status of targetability.

Figure 2 illustrates the key differences between the narrow and broad interpretations in their treatment of the temporal scope of DPH for a scenario involving the placement of an IED. It makes clear that the narrow and broad interpretations both include civilians participating in deployment, planting the device, and the return from the operation. The broader interpretation includes civilians involved in reconnaissance, planning, and materials acquisition. These preparatory activities often take longer, and involve far more people, than does the execution of the operation—meaning that more civilians will be swept into the DPH category and therefore considered targetable.

FIGURE 2: TEMPORAL SCOPE OF DPH FOR CIVILIANS INVOLVED IN THE PLACEMENT OF AN IED

3. *Is a Civilian That Repeatedly Participates Continuously Targetable?*

The issue of repeated participation in hostilities presents another challenge in interpreting DPH. The debate centers on whether civilians who repeatedly engage in hostile acts should continuously lose their

protected status or regain it between acts of participation.[166] This issue, while related to the temporal scope of DPH, presents its own unique challenges. The central question revolves around the interpretation of the phrase "for such time" in Article 51(3) of Additional Protocol I to the Geneva Conventions.[167] However, this debate extends beyond determining the temporal scope of targetability for a single act of DPH. Instead, it grapples with a more complex issue: Under what circumstances, if any, does a civilian who repeatedly participates in hostilities lose their protected status and become continuously targetable?

The narrow approach to DPH adopts what has been dubbed by its critics the "revolving door" approach.[168] According to this interpretation, civilians who participate in hostilities on a recurrent basis regain their protection from attack each time they disengage from hostile activities and return to civilian life.[169] However, they lose this protection again when they launch their next hostile act.[170] For example, under the narrow view, a farmer who occasionally acts as a lookout for an armed group would be targetable only when actually performing this function. Each time he returns to his farming activities, he regains his protected status as a civilian.

In contrast, the broad approach to DPH adopts a more continuous view of participation. Under this framework, civilians who engage in DPH forfeit their protected status—and are therefore targetable—until they "permanently cease" their participation.[171]

There also exists a middle-ground approach to continuous participation. This approach distinguishes between sporadic participants and those who engage in a continuous cycle of hostilities.[172] For sporadic

166 *See* Schmitt, *supra* note 131, at 36 (describing meetings where experts failed to agree on when direct participation starts and ends).

167 Additional Protocol I, *supra* note 8, art. 51(3).

168 *See* LAW OF WAR MANUAL, *supra* note 136, § 5.8.4.2, n.314 ("'[R]evolving door' evokes the idea of a . . . carnival shooting gallery, where soldiers must wait until an opponent pops out from behind a door to be shot at. [L]aw begins to be undermined by suggesting an opponent can repeatedly avail themselves of such protection." (citing Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641, 689 (2010))).

169 ICRC Interpretive Guidance, *supra* note 121, at 70.

170 *Id*.

171 LAW OF WAR MANUAL, *supra* note 136, § 5.8.4.2 ("[P]ersons who are assessed to be engaged in a pattern of taking a direct part in hostilities do not regain protection from being made the object of attack in the time period between instances of taking a direct part in hostilities."). For more on how civilians may cease participation under the broad approach, see *infra* Section II.B.4.

172 *See Targeted Killings*, *supra* note 123, ¶¶ 39–40 (holding that a civilian taking a direct part in hostilities "sporadically, who later detaches himself . . . is entitled to protection . . . . [A] civilian who . . . commits a chain of hostilities, with short periods of rest between them,

participants, the middle-ground adopts a view similar to the narrow approach: These individuals regain their protection from direct attack once they detach themselves from the hostile activity.[173] However, for individuals who commit a series of hostile acts with short periods of rest between them, the middle-ground approach considers the rest periods as merely preparation for the next hostile act, deeming these individuals to have lost their immunity from attack for the duration of this continuous cycle of activity.[174]

To illustrate the practical implications of these different approaches, consider two scenarios. First, envision a civilian taxi driver who occasionally transports fighters and weapons for an armed group. Under the narrow "revolving door" approach, this individual would only be targetable during the specific times they are transporting fighters or weapons. Once they return to regular civilian taxi driving, they would regain their protected status. Under the broad approach, however, this person might be considered to be continuously participating in hostilities until they take clear steps to disassociate from the armed group.

In another scenario, consider civilian computer experts who intermittently assist an armed group by hacking into enemy systems, but otherwise lead normal civilian lives. The narrow approach would limit their loss of protection to the specific periods of hacking activity directly related to the armed conflict. The broad view might consider their specialized skills and repeated involvement as justification for classifying them as continuous participants, and therefore targetable at all times unless and until they cease participation.

The significance of repeated participation takes on even greater importance when viewed through the lens of expanded causal and temporal interpretations. Under narrow interpretations of DPH that only include activities directly causing harm, the practical impact of the "revolving door" debate is limited to a small set of activities like planting IEDs or directly engaging in combat. However, when broad interpretations are applied—counting activities like weapons maintenance, strategic intelligence gathering, or malware development as DPH—the question of repeated participation becomes far more consequential. A broad interpretation of both causal chain and temporal scope, combined with a rejection of the "revolving door" approach, could transform large numbers of civilian technical specialists, logistics

loses his immunity from attack 'for such time' as he is committing the chain of acts" (internal citations omitted)).

173 *Id.*

174 *Id.*

workers, and support personnel into continuously targetable individuals based on their recurring support roles.

4. How Can a Civilian Cease Participation?

The question of when and how a civilian who has participated in hostilities can regain protected status is closely related to the issues of temporal scope and repeated participation. This area of disagreement focuses on what actions, if any, are required for a civilian to effectively "opt out" of hostilities.

The narrow approach suggests that protection is regained as soon as the specific act of DPH ends.[175] Under this view, no formal act of disengagement is required; the mere cessation of hostile acts is deemed sufficient for a civilian to recover protected status.[176]

In contrast, the broad approach requires "affirmative disengagement"—a definitive and observable action to terminate involvement in hostilities.[177] Such actions could include formally renouncing allegiance to an armed group or demonstrating through "concrete and verifiable facts or persuasive indicia" that they have returned to peaceful pursuits.[178] The challenge with this approach lies in defining what constitutes sufficient evidence of disengagement, particularly in complex conflict environments. There is the added challenge for participants of how to communicate their disengagement to the enemy. Even if they could do so, that communication may itself lead the person making the communication a target. Indeed, in practice, affirmative disengagement may be impossible to achieve.

Finally, the middle-ground approach suggests that the method of ceasing participation may depend on the individual's pattern of involvement.[179] For those engaged in isolated acts, simply stopping the specific activity may suffice to regain protection.[180] However, for individuals caught in a continuous cycle of hostilities, a more definitive break may be necessary to restore their protected status.[181]

---

175 *Id.*

176 *Id.*

177 Law of War Manual, *supra* note 136, 5.8.4.2, n.314 ("Repetitious participation can be considered in determining if such persons are in reality continuously engaged in hostilities. When such participation occurs, affirmative disengagement would be required in order to establish that such persons are no longer direct participants in hostilities." (quoting Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance*, 42 N.Y.U. J. Int'l L. & Pol. 641, 692–93 (2010))).

178 *Id.*

179 *Targeted Killings*, *supra* note 123, ¶¶ 39–40.

180 *Id.*

181 *Id.*

Real-world scenarios help to illustrate what is required to regain protected status under the competing interpretations of cessation. Consider a civilian who has been involved in making IEDs for an armed group who decides to stop. Under the narrow approach, the civilian would regain their protected status as soon as they ceased this activity. The broad approach requires them to take additional steps, such as turning themselves in to authorities or publicly renouncing their affiliation with the group.

Similarly, consider a hacker who has been conducting cyber-attacks on behalf of an organized armed group who decides to stop participating. The narrow view would likely consider the hacker's protection restored as soon as they cease hacking activities. The broader view might require the hacker to demonstrate that they have deleted any specialized software, cut ties with the group, and perhaps even assisted in counteracting their previous attacks.

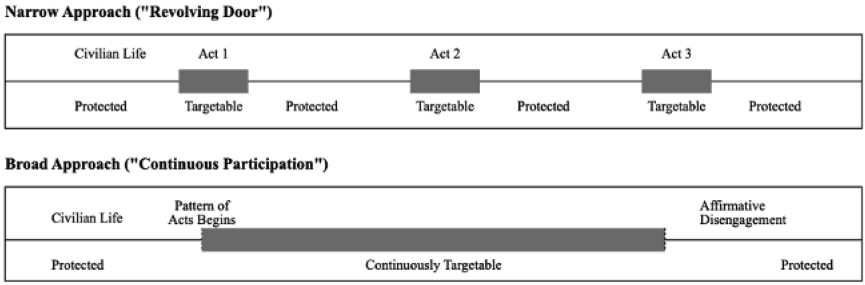
The complexity of this issue is further illustrated by the case of a civilian who has been acting as a lookout for an armed group in their village who wants to cease participation but fears reprisals if they openly renounce the group. The narrow approach would restore their protection when they stop acting as a lookout. The "affirmative disengagement" approach faces challenges here: What constitutes sufficient disengagement in a situation where open renunciation could be life-threatening?

Last, consider a civilian who has participated in multiple attacks and decides to stop after a close call with enemy forces. They return to their normal civilian life but do not take any overt actions to disassociate from the armed group. The narrow approach would likely restore their protected status after they cease hostile acts. The broad approach would hold that without clear disengagement, past patterns of behavior suggest they remain a potential threat and are therefore targetable. Here, as in all the prior hypotheticals, the civilians who have engaged in criminal acts remain subject to criminal prosecution under both the narrow and broad approach. To return to protected status simply means that they are protected from being intentionally targeted with lethal force, not that they are protected from legal consequences for their unlawful actions.

Figure 3 illustrates the difference between the two approaches. It makes clear that under the narrow approach, civilians are targetable only intermittently, whereas under the broad approach, they are continuously targetable from the moment the pattern of acts begins. While the figure illustrates a situation in which a civilian repeatedly participates, it is important to note that the decision to treat the civilian as continuously targetable takes place at the beginning of what may

or may not in fact be a pattern of participation. The figure also makes clear that the broad approach requires affirmative disengagement—though, as explained, how a civilian directly participating in hostilities can express that disengagement to an opposing State is far from clear.

FIGURE 3: REPEATED PARTICIPATION AND CEASING PARTICIPATION



C. Additional Challenges Posed by Non-International Armed Conflicts

As in international armed conflicts, civilians directly participating in hostilities during a non-international armed conflict may lose their protected status. Additional Protocol II, which applies to non-international armed conflicts, reflects the same language used in Additional Protocol I,[182] providing that civilians shall be protected "unless and for such time as they take a direct part in hostilities."[183] All of the same disagreements outlined above with regard to determining who is a civilian directly participating in hostilities and when they are targetable arise in the non-international armed conflict context, as well. Yet there are added challenges that arise in the non-international armed conflict context, namely: is membership in an organized armed group enough to render a person targetable, how to determine if someone is a member of an organized armed group, and how can members terminate that membership? We address each in turn.

1. Is Membership in an Organized Armed Group Enough?

Perhaps the most critical difference between the analysis of DPH in an international armed conflict and non-international armed conflict concerns whether affiliation with an organized armed group alone is sufficient to render someone targetable. This question does not arise in an international armed conflict, because all members of armed forces are,

182 *See* Additional Protocol I, *supra* note 8, art. 51(3).
183 Additional Protocol II, *supra* note 8, art. 13(3).

by definition, combatants.[184] They receive the privileges and immunities that come with membership, and, in return, they can be lawfully targeted.[185] In non-international armed conflict, however, determining who can be lawfully targeted becomes more complex because members of non-State organized armed groups lack the formal status of State armed forces. Unlike in international armed conflicts, where combatant status is clearly defined, the classification and targetability of organized armed group members has been subject to significant debate.[186]

Part of the debate stems from a disagreement about who can be properly defined as a member of an organized armed group. The broad view adopts a *status-based* approach to membership: Simply "being a part" of an organized armed group that is engaged in hostilities against a State makes a person targetable, regardless of what role they play.[187] In contrast, the narrow view adopts a *conduct-based* approach. Under this framework, an "organized armed group"[188] consists "exclusively [of] the armed or military wing of a non-State party" whose members perform a specific type of conduct known as a "continuous combat function" (CCF).[189] The narrow approach limits targetability: Only individuals with CCF are generally legitimate targets. Others—even those who identify as group members or serve political or administrative functions—are classified as civilians and cannot be targeted unless they directly participate in hostilities. Thus, targetability hinges on conduct in two ways: Individuals whose role inherently requires DPH are continuously targetable, while those in other roles (or who play no role) become targetable only when they actually engage in DPH, subject to the standard DPH doctrine.[190]

---

184 *See generally* Additional Protocol I, *supra* note 8, art. 43(2) (explaining how to determine membership in a State's armed forces).

185 *See id.* ("Members of the armed forces of a Party to a conflict . . . are combatants, that is to say, they have the right to participate directly in hostilities."); *id.* art. 52(2) (establishing that "[a]ttacks shall be limited strictly to military objectives"); Geneva Convention III, *supra* note 8 (establishing international legal protections for prisoners of war).

186 *See* ICRC Interpretive Guidance, *supra* note 121, at 27 (noting that "[w]hile it is generally recognized that members of state armed forces in non-international armed conflict do not qualify as civilians, treaty law, state practice, and international jurisprudence have not unequivocally settled whether the same applies to members of organized armed groups"). *Cf.* Law of War Manual, *supra* note 136, § 4.18.2 (noting that private persons who engage in hostilities are denied to distinct protections afforded to peaceful civilians).

187 Law of War Manual, *supra* note 136, § 4.18.4.1.

188 Note that the ICRC Guidance uses the term "organized armed group" rather than "non-state armed group" but those terms are interchangeable. ICRC Interpretive Guidance, *supra* note 121, at 30 ("For the purposes of this Interpretive Guidance . . . the armed forces of non-state parties [to a NIAC] are described as 'organized armed groups.'").

189 *Id*. at 32–33.

190 *Id*. at 34.

2. *Who is a Member of an Organized Armed Group?*

The implications of the different approaches to the targetability of members of organized armed groups is further compounded by the different approaches to defining membership. Unlike State armed forces, non-State-armed groups rarely use formal indicia of membership like uniforms or identity cards, and members may actively attempt to conceal their affiliations.[191] As a consequence, the "informal and clandestine structures of most organized armed groups and the elastic nature of membership render it particularly difficult to distinguish between a non-State party to the conflict and its armed forces."[192]

The narrow approach to membership defines an organized armed group as "armed forces of a non-State party to the conflict" that "consists only of individuals whose continuous function it is to take a direct part in hostilities ('continuous combat function')."[193] Significantly, under the narrow view, there are no civilians in an organized armed group, since only those who meet the CCF requirement are considered members.[194] The CCF requirement "distinguishes members of the organized fighting forces of a non-State party from civilians who directly participate in hostilities on a merely spontaneous, sporadic, or unorganized basis, or who assume exclusively political, administrative or other non-combat functions."[195] In contrast to a civilian directly participating in hostilities, an individual with a CCF has a "lasting integration" into the armed forces of a non-State party to a non-international armed conflict.[196] Therefore, it is only individuals whose *continuous* role "involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities" that are considered members of an organized armed group.[197]

The narrow approach to identifying members of an organized armed group recognizes the differing "degrees of affiliation" with organized armed groups "that do not necessarily amount to 'membership' within the meaning of IHL."[198] It expresses concern that while some

---

191 *Id.* at 33.

192 *Id.*

193 *Id.* at 36.

194 *See, e.g.*, *id.* at 28 ("[C]ivilians, armed forces, and organized armed groups of the parties to the conflict are mutually exclusive categories also in non-international armed conflict."). The ICRC rebuffs a vision of organized armed groups which considers all members as civilians who are continuously directly participating in hostilities. *Id.*

195 *Id.* at 34.

196 *Id.*

197 *Id.* ("Individuals who continuously accompany or support an organized armed group, but whose function does not involve direct participation in hostilities, are not members of that group . . . . Instead, they remain civilians assuming support functions, similar to private contractors and civilian employees accompanying State armed forces.").

198 *Id.*

cases of affiliation may be truly voluntary, other instances result from "involuntary recruitment" or "more traditional notions of clan or family."[199] Therefore, the narrow approach does not consider "abstract affiliation, family ties, or other criteria prone to error, arbitrariness or abuse" as legitimate indicia of membership in an organized armed group. That said, the narrow view does take into account both formal and functional indicia of organized armed group membership. CCF "may be openly expressed through the carrying of uniforms, distinctive signs, or certain weapons" or "on the basis of conclusive behavior, for example, where a person has repeatedly directly participated in support of an organized armed group in circumstances indicating that such conduct constitutes a continuous function rather than a spontaneous, sporadic, or temporary role assumed for the duration of a particular operation."[200]

Like the narrow approach, the broad approach to determining membership considers formal indicia of membership such as "wearing a uniform or other clothing, adornments, or body markings that identify members of the group" or "documents issued or belonging to the group that identify the person as a member, such as membership lists, identity cards, or membership applications."[201] With regards to functional indicia of membership, both approaches rely on patterns of participation in hostilities—looking at the frequency, duration, and intensity of an individual's involvement.[202] However, the broad approach extends well beyond these shared criteria.

In instances where an organized armed group is not organized in a formal command structure, the broad approach relies on the concept of "functional membership" to determine if an individual is a member of an organized armed group. Under these circumstances, the broad approach considers individuals who are "integrated into the group such that the group's hostile intent may be imputed to him or her may be deemed to be functionally (i.e., constructively) part of the group" as members of an organized armed group.[203] Thus, if an individual is sufficiently "integrated" into the organized armed group, an inference is made that the "individual shares the group's intention to commit hostile acts" rather than being "merely sympathetic to the group's goals."[204] Indicia of functional membership are even broader than indicia of formal membership, such as "following directions issued by the group

199 *Id.*

200 *Id.* at 33, 35.

201 Law of War Manual, *supra* note 136, § 5.7.3.1.

202 *See id.* (listing different ways to determine an individual's involvement in non-State-organized armed groups).

203 *Id.* § 5.7.3.2.

204 *Id.*

or its leaders."[205] While determining this category of membership might rely on different indicia, the consequence of the determination remains the same: "individuals who are formally or functionally part of a non-State armed group that is engaged in hostilities may be made the object of attack because they likewise share in their group's hostile intent."[206]

The broad approach is once again exemplified in the DoD Law of War Manual, which authorizes the use of "circumstantial or functional information to assess whether a person is part of a non-State armed group."[207] For example, the broad approach considers "accessing facilities, such as safehouses, training camps, or bases used by the group that outsiders would not be permitted to access,"[208] "traveling along specific clandestine routes used by those groups,"[209] and "traveling with members of the group in remote locations or while the group conducts operations"[210] as indicia of membership in an organized armed group.[211]

---

205 *Id.*; *see also* Al-Adahi v. Obama, 613 F.3d 1102, 1109 (D.C. Cir. 2010) ("When the government shows that an individual received and executed orders from al-Qaida members in a training camp, that evidence is sufficient (but not necessary) to prove that the individual has affiliated himself with al-Qaida.").

206 Law of War Manual, *supra* note 136, § 5.7.3.

207 *Id.* § 4.18.4.1.

208 These citations are found in the Law of War Manual, *supra* note 136, § 5.7.3.1, n.261. Alsabri v. Obama, 684 F.3d 1298, 1306 (D.C. Cir. 2012) ("[I]t is difficult to believe that 'Taliban fighters would allow an individual to infiltrate their posts near a battle zone unless that person was understood to be a part of the Taliban.'" (quoting Alsabri v. Obama, 764 F.Supp.2d 60, 94 (D.D.C. 2011))); *see also* Uthman v. Obama, 637 F.3d 400, 406 (D.C. Cir. 2011) ("[S]taying at an al Qaeda guesthouse is 'powerful—indeed 'overwhelming'—evidence' that an individual is part of al Qaeda . . . . It is highly unlikely that a visitor to Afghanistan would end up at an al Qaeda guesthouse by mistake, either by the guest or by the host.").

209 Law of War Manual, *supra* note 136, § 5.7.3.1. *See* Suleiman v. Obama, 670 F.3d 1311, 1314 (D.C. Cir. 2012) ("There is no dispute that Suleiman's travel was initiated at the suggestion of and facilitated by a Taliban recruiter, and that he traveled a well-worn path to Afghanistan frequently used by Taliban recruits. . . . [s]uch travel may indicate that an individual traveled to Afghanistan to join the Taliban" (citing Al Odah v. United States, 611 F.3d 8, 14 (D.C. Cir. 2010))); *Uthman*, 637 F.3d at 405 ("[T]raveling to Afghanistan along a distinctive path used by al Qaeda members can be probative evidence that the traveler was part of al Qaeda"); *Al Odah*, 611 F.3d at 16 (finding it significant that "Al Odah traveled to Afghanistan on a series of one-way plane tickets purchased with cash in a manner consistent with travel patterns of those going to Afghanistan to join the Taliban and al Qaeda"). These citations are found in the Law of War Manual, *supra* note 136, § 5.7.3.1, n.262.

210 Law of War Manual, *supra* note 136, § 5.7.3.1; *see* Hussain v. Obama, 718 F.3d 964, 968–69 (D.C. Cir. 2013) ("Evidence that Hussain bore a weapon of war while living side-by-side with enemy forces on the front lines of a battlefield at least invites—and may very well compel—the conclusion that he was loyal to those forces. We have repeatedly affirmed the propriety of this common-sense inference."); *Uthman*, 637 F.3d at 405 (Uthman "[b]eing captured in the company of a Taliban fighter . . . in December 2001 . . . absent a credible alternative explanation, . . . strongly suggest[s] that he was part of al Qaeda"). These citations are found in the Law of War Manual, *supra* note 136, § 5.7.3.1, n.263.

211 *See* Law of War Manual, *supra* note 136, § 5.7.3.1 (listing different types of information that may indicate membership).

Under this view, a person can be considered a member of an organized armed group regardless of official affiliation.

Under the broad approach, *merely participating* in the activities of the organized armed group would be sufficient to establish "membership."[212] The DoD Law of War Manual states:

> Being part of a non-State armed group that is engaged in hostilities against a State is a form of engaging in hostilities that makes private persons liable to treatment in one or more respects as unprivileged belligerents by that State. Being part of a non-State armed group may involve formally joining the group or simply participating sufficiently in its activities to be deemed part of it.[213]

The divergent approaches to organized armed group membership profoundly shape how civilian support roles are evaluated in non-international armed conflicts. Under the broad approach that extends targetability based on group affiliation, individuals who regularly perform support functions—roles such as propagandists, financiers, or support crew—may be considered "constructively part of the group, even if they are, in fact, not formal members of the group."[214] This effectively creates a status-based category of targetable individuals analogous to members of the armed forces in an international armed conflict. The narrow approach, by contrast, maintains that such support personnel remain civilians unless they perform a continuous combat function, preserving a sharper distinction between civilian and military status:

> [R]ecruiters, trainers, financiers and propagandists may continuously contribute to the general war effort of a non-State party, but they are not members of an organized armed group belonging to that party unless their function additionally includes activities amounting to direct participation in hostilities. The same applies to individuals whose function is limited to the purchasing, smuggling, manufacturing and maintaining of weapons and other equipment outside specific military operations or to the collection of intelligence other than of a tactical nature. Although such persons may accompany organized armed groups and provide substantial support to a party to the conflict,

---

212 *See, e.g.*, *id.*

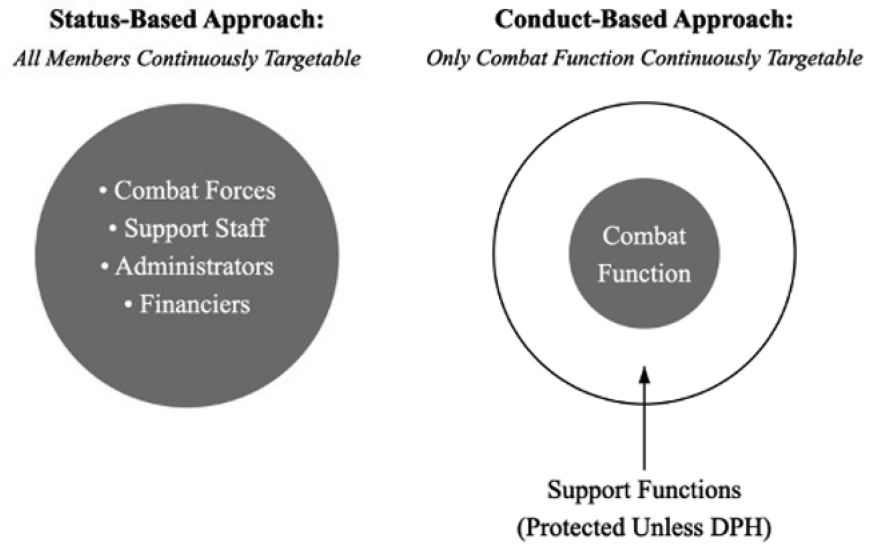
213 *Id.* § 4.18.4.1 (citation omitted).

214 *Id.*; *see id.* § 4.18.4.1, n.389 (arguing that the broad approach allows "civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services reponsible for the welfare of the armed forces" to be targetable) (quoting Reply Brief for Defendant-Appellant at 11–12, Hedges v. Obama, 724 F.3d 170 (2013) No. 12-3644 (internal citations omitted)).

> they do not assume continuous combat function and, for the purposes of the principle of distinction, cannot be regarded as members of an organized armed group.[215]

This fundamental difference in approaching membership becomes especially consequential when considering individuals who support an organized armed group without any formal affiliation. Consider civilians who provide financial support, operate drones from remote locations, or conduct open-source intelligence gathering about tactical movements. While both interpretive approaches will permit targeting such civilians if their activities qualify as DPH, they differ significantly in how they evaluate sustained support roles. The broad approach is more likely to view sustained support activities as creating a de facto membership status, while the narrow approach maintains a stricter distinction between membership and civilian support, evaluating each supportive act individually under DPH criteria. Finally, the broad approach considers members of the armed group targetable throughout the conflict, regardless of their direct role in combat activities, while the narrow approach will consider them targetable only if they have CCF or are actively participating in hostilities. Figure 4 illustrates the differences between the two approaches.

FIGURE 4: WHO IS TARGETABLE AS AN OAG MEMBER?



215 ICRC Interpretive Guidance, *supra* note 121, at 34–35.

Finally, the narrow approach emphasizes that there is a "presumption of protection in case of doubt" regarding the membership of an individual.[216] The broad approach does not emphasize such a presumption of protection. The DoD Law of War Manual, for example, contains no mention of the presumption of civilian status in cases of doubt in the section describing how to determine which individuals belong to an organized armed group.[217] The Manual, however, has made some steps toward adopting a presumption of civilian status. Whereas it previously stated that "no legal presumption of civilian status exists for persons or objects," it was revised in 2023 to state that, "[u]nder the principle of distinction, commanders and other decision-makers must presume that persons or objects are protected from being made the object of attack unless the information available at the time indicates that the persons or objects are military objectives."[218] This demonstrates that the DoD Law of War Manual, which in many cases exemplifies the broad approach, is capable of revision, particularly in instances, like this, where the approach is widely regarded as inconsistent with a correct reading of the law.

3. How Can a Civilian Cease Membership?

Under the broad approach, a determination of membership, once made, is particularly difficult to reverse. While the approach acknowledges that an individual can lose their targetable status by severing their association with an organized armed group, this requires "unambiguous" cessation of membership.[219] The standards for proving such dissociation are demanding. Merely ceasing participation in group activities or the passage of time alone are insufficient. Instead, the broad approach requires concrete evidence of dissociation, such as formal renunciation of membership, including filing relevant paperwork or explicitly rejecting allegiance to the group, verifiable return to peaceful civilian life, participation in official reconciliation programs, or sworn loyalty to the government.[220] Notably, the passage of time since an individual's last participation in group activities only becomes relevant when combined with other clear indicators of dissociation.[221] This high

---

216 *Id.* at 35.

217 *See* Law of War Manual, *supra* note 136, § 5.7.3 (containing no mention of the presumption of civilian status in cases of doubt in the section describing how to determine which individuals belong to an organized armed group).

218 *See* Michael W. Meier, *2023 DoD Manual Revision—A Welcome Change to the Presumption of Civilian Status*, Articles of War (July 31, 2023), https://lieber.westpoint.edu/welcome-change-presumption-civilian-status [https://perma.cc/MA8W-MD96].

219 *See* Law of War Manual, *supra* note 136, § 5.7.3.3.

220 *Id.*

221 *Id.*

bar for reversing membership status stands in stark contrast to the relatively expansive criteria for establishing membership in the first place, creating an asymmetric framework where membership is easier to establish than to terminate.

III
The Stakes: The Vulnerability of Civilians in Crowdsourced War

We now return to the examples of Crowdsourced War examined at the outset of this Article. Here, we examine how the different interpretations of direct participation in hostilities dramatically affect civilian vulnerability on the modern battlefield. We show that while some forms of digital participation clearly constitute direct participation in hostilities under both narrow and broad interpretations, others fall into a gray area. Under broad interpretations, vast numbers of civilians could be deemed lawful military targets, whereas narrower interpretations would classify them as protected civilians. Moreover, we show that the continuous nature of many digital activities—from maintaining apps on phones to operating cloud infrastructure—also challenges traditional temporal frameworks for determining when participation begins and ends. In short, this Part demonstrates the real-world life-and-death stakes of what may appear to be arcane legal distinctions.

A. e-Enemy and ePPO

Civilians using the e-Enemy and ePPO apps are the modern analogs of civilians in previous wars who provided tactical intelligence about the enemy or who served as artillery spotters. Through these apps, Ukrainian civilians can instantly relay the location and trajectory of Russian military assets to Ukrainian forces for immediate targeting.[222] While civilians have long served intelligence-gathering functions in warfare, digital technologies now enable them to perform these tasks with unprecedented accuracy, efficiency, and scale.[223]

Civilians who provide tactical information about the enemy are paradigmatic examples of DPH under both the narrow and the broad approaches to DPH.[224] The ICRC's Interpretive Guidance, which is

[222] *See* Tiahnyriadno, *supra* note 1; Bergengruen, *supra* note 11.

[223] *See* Tiahnyriadno, *supra* note 1 (describing how the smartphone app ePPO is used in the defense of Ukraine); Bergengruen, *supra* note 11 (describing how government apps are used to collect evidence of Russian war crimes).

[224] *See* ICRC Interpretive Guidance, *supra* note 121, at 34–35 (categorizing individuals whose function is limited to the collection intelligence other than of a tactical nature as not

generally representative of the narrow approach, explicitly provides that a civilian engaged in "transmitting tactical targeting information for an attack" is direct participation.[225] Other relevant examples of direct participation provided by the ICRC's Interpretive Guidance include: "a civilian woman who repeatedly peeked into a building where troops had taken cover in order to indicate their position to the attacking enemy forces"[226] and "an unarmed civilian sitting in a restaurant using a radio or mobile phone to transmit tactical targeting intelligence to an attacking air force."[227]

Similarly, the U.S. Department of Defense Law of War Manual, which is generally representative of the broad approach, sets forth several examples of acts that qualify as DPH, and among these is "providing or relaying information of immediate use in combat operations, such as acting as a . . . spotter or member of a ground observer corps or otherwise relaying information to be used to direct an [attack]."[228] Therefore, a civilian using e-Enemy and ePPO plainly meets the requirements to be considered DPH under both the narrow and broad approaches, at a minimum for the moment or two it takes to open and use the app.[229]

While these examples suggest that use of surveillance apps like e-Enemy and ePPO would be considered to be DPH regardless of the interpretation adopted, there remain critical differences between the broad and narrow approaches regarding when civilians using these apps can be targeted and for how long. These differences dramatically affect the scope of vulnerability for civilians.

DPH, with the implication that those whose function is the collection of tactical intelligence can be DPH); Prosecutor v. Strugar, Case No. IT-01-42-A, Appeals Chamber Judgment, 176–79 (July 17, 2008) (listing "transmitting military information for the immediate use of a belligerent" and "serving as guards, intelligence agents, lookouts, or observers on behalf of military forces" as examples of DPH); *Targeted Killings*, *supra* note 123, ¶ 35 (categorizing "a person who collects intelligence on the army" as DPH).

225 ICRC Interpretive Guidance, *supra* note 121, at 48 n.103.

226 *See id.*

227 *Id.* at 81.

228 Law of War Manual, *supra* note 136, § 5.8.3.1. Citing "lessons learned" from combat operations in Afghanistan and Iraq, the DOD Law of War Manual subsequently provides an example of a specific factual scenario of a civilian directly participating in hostilities as follows: "Your unit comes under fire, you notice a young civilian woman who appears to be pointing to the location where friendly troops are concealed, based on her actions, those locations are then targeted. Response: Shoot to eliminate the threat . . . ." *Id.* n.300 (citing 101st Airborne ROE Card, Iraq (2003), reprinted in Center for Law and Military Operations, The Judge Advocate General's Legal Center & School, U.S. Army, 1 Legal Lessons Learned from Afghanistan and Iraq: Major Combat Operations (11 September 2001 – 1 May 2003) 315, 316 (2004)).

229 *See id.* § 5.8.3.1.

1. How Long Are App Users Targetable?

The approaches diverge significantly on the temporal scope of targeting—that is, precisely how long civilians using e-Enemy or ePPO forfeit their protected status. This question turns on different interpretations of the "for such time" requirement in Article 51(3) of Additional Protocol I,[230] and takes on particular urgency given that these apps reside on the Diia platform, which is already installed on approximately nineteen million Ukrainian smartphones used by about seventy percent of the population.[231] Specifically, does the duration of DPH last from the time the app is downloaded through when it is deleted, or only while the app is open and actively being used?[232]

Under the narrow approach, a civilian's loss of protection begins only when they undertake a specific hostile act and ends once they have physically separated from that operation.[233] The duration of DPH may include preparatory measures if such measures aim to carry out a specific hostile act but not if they merely aim to "establish the *general capacity* to carry out unspecified hostile acts."[234] In other words, under the narrow approach, preparatory measures are included within the temporal scope of DPH only if they are "of a specifically military nature and so closely linked to the subsequent execution of a specific hostile act that they already constitute an integral part of that act."[235] The act of downloading an app for future use is more akin to establishing a "general capacity" for future acts. Therefore, under the narrow view, civilian users of e-Enemy and ePPO are engaging in DPH from the time they open the app for the purpose of reporting until they complete their transmission.[236] The time spent downloading the app or maintaining it on their phone would not be included in the temporal scope of participation.

By contrast, the broad approach extends the period of targetability to include any activities causally connected to the hostile act, both before and after its execution.[237] Under this view, the temporal scope could begin when civilians first download the apps in preparation for future reporting and extend through periods between uses when they maintain the apps ready for deployment. Just as this approach would consider an IED planter targetable from initial planning through post-operation

---

230 Additional Protocol I, *supra* note 8, art. 51(3).
231 *See* O'Carroll, *supra* note 11.
232 *See* Schmitt & Biggerstaff, *supra* note 1, at 5.
233 *See supra* Section II.B.2.
234 ICRC Interpretive Guidance, *supra* note 121, at 66 (emphasis in original).
235 *Id.* at 65–66.
236 *See id.* at 54.
237 Schmitt, *supra* note 131, at 37.

activities,[238] it might view e-Enemy and ePPO users as targetable throughout the period they maintain the capability to provide targeting data to Ukrainian forces. This interpretation is particularly concerning given that e-Enemy and ePPO are integrated into Diia, Ukraine's primary platform for government services that most Ukrainian civilians use for everyday activities like applying for government benefits, filing tax returns, and renewing passports.[239] The broad approach could therefore transform a vast portion of Ukraine's civilian population into continuously targetable individuals simply because they maintain apps on their phones that could be used for military purposes.

2. *Are Civilians Who Use the App Several Times Continuously Targetable?*

Critical differences between the broad and narrow approaches emerge with respect to the civilians who repeatedly engage in DPH, and also with respect to whether civilians need to take affirmative steps to demonstrate that they have ceased their participation in hostilities. While temporal scope addresses how long a civilian forfeits protection for a single use of e-Enemy or ePPO, repeated participation asks whether civilians who regularly use these apps should regain their protected status between acts of participation. This takes on particular significance given that Ukrainian civilians are actively encouraged to use these apps whenever they spot Russian military assets.

Under the narrow approach, civilians who use e-Enemy or ePPO on a recurrent basis regain their protection from attack "in parallel with the intervals of their engagement in direct participation in hostilities (so-called 'revolving door' of civilian protection)," that is, each time they disengage from the hostile activity and return to civilian life.[240] A civilian who regularly reports Russian military movements would be targetable only during the specific moments of reporting, then regain protection upon completing each transmission.[241] Thus, the narrow approach protects civilians who may feel compelled to participate intermittently in Ukraine's defense while maintaining their primary civilian roles. Civilians who use the e-Enemy and ePPO apps on a regular basis will lose their civilian protection only for the short period of time when they are directly participating, i.e., from the time they open the app for the purpose of reporting until they complete sending the data via the app;

238 ICRC Interpretive Guidance, *supra* note 121, at 53 n.123.

239 *See supra* notes 11–17 and accompanying text (describing Diia's widespread civilian uses).

240 ICRC Interpretive Guidance, *supra* note 121, at 70.

241 *See supra* Section II.B.2.

once this is completed, they will regain their civilian protection, up until the next time they use the apps.

The broad approach, however, views repeated app use as establishing a pattern of hostile participation that forfeits protected status indefinitely.[242] Specifically, "persons who are assessed to be engaged in a pattern of taking a direct part in hostilities do not regain protection from being made the object of attack in the time period between instances of taking a direct part in hostilities."[243] For the millions of Ukrainian civilians with these apps on their phones, this could mean that reporting Russian military movements even a few times could make them continuously targetable until they take clear steps to disassociate from these activities. Even more troubling is that there is no agreed-upon set of actions which constitute cessation.[244]

Such vagueness has profound consequences for civilians. Under the broad approach, once a civilian has engaged in "a pattern" of DPH by using the e-Enemy or ePPO apps with some unspecified degree of regularity, they are deemed to be targetable up until the time that they "permanently cease[]"[245] doing so, but this raises several questions that remain unanswered. What constitutes a pattern of using cell phone apps—is once enough, or are two or more uses needed to establish a pattern, and does the frequency of these acts matter (for instance, is it a "pattern" if two instances of use are separated in time by a year)? A civilian user who willingly used the app on one occasion is presumably willing to do so again, and whether or not they actually have a chance to do so depends more on the presence of enemy forces in the vicinity and not on the civilian. Also, how does one permanently cease using the cell phone apps—is it sufficient simply to not use them anymore, or must the apps be uninstalled from the phone, and is a civilian required to undertake any additional action to demonstrate that they intend to permanently cease using the apps? How could an enemy be made aware of this?

The implications become particularly stark when considering how these interpretations interact.[246] Under the narrow approach, both temporal scope and repeated participation are limited—a civilian is only targetable while actually using the apps, regardless of how often they do so. But under the broad approach, not only does each use of the apps create an extended period of targetability, but repeated use could

242 *See* LAW OF WAR MANUAL, *supra* note 136, § 5.8.4.2.
243 *Id*.
244 *See supra* Section II.B.4.
245 *See* LAW OF WAR MANUAL, *supra* note 136, § 5.8.4.1.
246 *See supra* Sections II.B.3–4.

transform civilians into continuous targets, regardless of their primary civilian roles. Given that these apps are integrated into a platform used by most Ukrainian civilians for basic government services, this broad interpretation could effectively militarize a substantial portion of Ukraine's civilian population.

B. IT Army

The IT Army of Ukraine represents another way digital technologies have transformed civilian participation in warfare. This volunteer cyber force enables civilians worldwide to conduct coordinated attacks on Russian infrastructure and websites.[247] Unlike traditional civilian participation in warfare, the IT Army allows civilians to engage in hostile acts from anywhere in the world, coordinating through cloud services and tools hosted on platforms like GitHub.

The broad and narrow approaches to DPH diverge significantly on which IT Army activities constitute direct participation in hostilities. This question is particularly complex given the range of activities involved, from DDoS attacks on government websites to more sophisticated operations targeting critical infrastructure like the successful attack that shut down power to the Leningrad region through Loesk's systems.[248]

Under the narrow approach, only cyber operations that directly cause military harm in one causal step would constitute direct participation.[249] For example, hacking that disrupts military communications or directly interferes with weapons systems would qualify.[250] However, participating in DDoS attacks against civilian websites, even government ones, would likely not meet this threshold as these actions are too far removed from military operations.[251] Similarly, developing cyber tools or maintaining IT Army infrastructure would be considered indirect support rather than direct participation—analogous to how the narrow approach excludes weapons maintenance and general logistical support from DPH in traditional warfare.[252]

---

247 *See supra* Section I.B.

248 *See* Coble, *supra* note 54; Technology.org, *supra* note 55.

249 *See* ICRC Interpretive Guidance, *supra* note 121, at 51. Notably, the ICRC recently expressed concern that civilian volunteers participating in cyber operations may be DPH. *See* Munich Cyber Security Conference, *MCSC 2023: Vantage Point by Mauro Vignati*, YouTube (Mar. 6, 2023), https://www.youtube.com/watch?v=FZEwvaVSXT4 [https://perma.cc/3PML-UEZU].

250 *See supra* Section II.A.2.

251 *See* ICRC Interpretive Guidance, *supra* note 121, at 52–54 (describing the direct and indirect causation).

252 *Id.*

The broad approach, however, extends direct participation to include activities further along the causal chain that contribute to military operations.[253] Just as the broad approach considers weapons maintenance, strategic intelligence gathering, and logistical support as DPH in traditional warfare, it would likely encompass many IT Army support functions in addition to direct cyberattacks.[254] For instance, developing malware for future deployment could be analogous to assembling IEDs.[255] Maintaining the IT Army's communication infrastructure could be viewed like maintaining physical military communications systems.[256] Even participating in IT Army channels to share intelligence about potential targets or vulnerabilities could constitute DPH under this broader view of causation.[257]

This broad interpretation is particularly significant in the cyber context because it could make civilians who never personally conduct attacks targetable. For example, civilian programmers who create tools that enable others to conduct cyber operations might be viewed as directly participating in hostilities even if they do not deploy the tools themselves—similar to how the broad approach sometimes considers weapons manufacturers as legitimate targets when their work is sufficiently connected to specific military operations.[258] For an operation like the Loesk power system hack, everyone in the operational chain—from those who identified the vulnerability, to those who developed the exploit, to those who executed the attack—might be considered to be directly participating in hostilities.

The gap between broad and narrow views of causation widens when considering how long and how often civilians can be targeted. Under the narrow approach, even when IT Army activities qualify as direct participation, civilians would only be targetable during their active involvement in specific cyber operations.[259] A civilian who occasionally participates in DDoS attacks would regain protection

253 *See supra* Section II.B.2 (discussing the causal inquiry under the broad approach).

254 *See* LAW OF WAR MANUAL, *supra* note 136, § 5.8.3 (describing direct participation in combat as including "certain acts that . . . effectively and substantially contribute to an adversary's ability to conduct or sustain combat operations").

255 *See id.* § 5.8.3.1 (including "supplying weapons and ammunition, whether to conventional armed forces of non-state armed groups, or assembling weapons (such as improvised explosive devices) in close geographic or temporal proximity to their use" as an example of direct participation in hostilities).

256 *See* Turner & Norton, *supra* note 151, at 31 (describing the U.S. Army's view that civilian technical advisors who are fully integrated into the armed forces are taking an active role in hostilities).

257 *Targeted Killings*, *supra* note 123, ¶ 35.

258 LAW OF WAR MANUAL, *supra* note 136, § 5.8.3 n.294.

259 *See* ICRC Interpretive Guidance, *supra* note 121, at 68.

between operations, just as e-Enemy users regain protection between reports.[260] The broad approach, however, could extend vulnerability far beyond active participation. Just as maintaining e-Enemy on a phone could create extended periods of targetability, maintaining cyber tools or IT Army communication channels could make civilians continuously targetable.[261] Moreover, under the broad view that rejects the "revolving door" of protection, repeated participation in IT Army operations could make civilians targetable until they "permanently cease[]" participation—requiring them to take clear, verifiable steps to disassociate from cyber operations.[262]

Apparently alarmed by the fact that civilians in the IT Army are targetable, as well as seeking to formalize its own cyber defense force, the Ukrainian government has been debating a law to designate IT Army volunteers as members of the country's reserve forces.[263] As members of the reserve forces, these volunteers would still be targetable, but they would be afforded combatants' privileges consistent with international humanitarian law in the event they were captured. For example, combatants cannot be prosecuted for killing enemy troops or for destroying lawful military objectives.[264] But if members of the IT Army are characterized as members of Ukraine's military reserve forces, presumably they will need to be subject to the military's command structure and disciplinary proceedings, and it is unclear how this could be achieved logistically with respect to volunteers who are not located in Ukraine or are not Ukrainian citizens.[265] Subsuming the IT Army into the military command structure would also require that the Ukrainian government take steps to ensure that members of the IT Army comply with international humanitarian law. Thus, it could no longer attack civilian targets. As of mid-2025, it appears that this proposed law has not been enacted.

C. Social Media Recruiting & Crowdfunding

Social media enables both States and non-State actors to recruit fighters and raise funds for military operations. As described in Part I,

---

260 *See id.* at 70.

261 *See supra* Section II.B.2.

262 Law of War Manual, *supra* note 136, § 5.8.4.1.

263 Shaun Waterman, *Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army*, Newsweek (Mar. 14, 2023), https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814 [https://perma.cc/FPZ3-NPH6].

264 *Id.*

265 *Id.* By way of comparison, Estonia is considered to be a leader in cyber operations and has a volunteer cyber defense force which is under the command of the country's military. *See* Shaun Waterman, *Ukraine's Volunteer Cyber Army Could be Blueprint for the World: Experts*, Newsweek (Feb. 21, 2023), https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970 [https://perma.cc/TX9T-UM28].

platforms like GoFundMe, Reddit, Telegram, and Bluesky have become tools for military recruitment and procurement.[266] For example, in the international armed conflict context, Ukraine's International Legion recruits through online channels, while social media enables foreign volunteer units to source everything from basic medical equipment to tactical gear and armaments.[267] Likewise, in the non-international armed conflict context, organized armed groups have leveraged social media platforms for recruitment and fundraising.[268]

The legal implications of these activities vary significantly depending on the nature of the conflict. In international armed conflicts, the central question is whether social media recruiting and crowdfunding constitute direct participation in hostilities.[269] Under the narrow approach, recruitment and financial support are explicitly excluded from the scope of DPH.[270] Even when social media campaigns directly enable military operations—like Ukraine's United24 platform raising funds for military drones or Bluesky users organizing equipment purchases for specific units[271]—civilians would merely be building military capacity rather than directly causing harm.[272]

The broad approach to international armed conflicts, however, takes a markedly different view of these activities. Under this interpretation, coordinated campaigns to recruit fighters or raise funds for specific military operations might constitute DPH.[273] For instance, a civilian using Bluesky to raise funds for night vision equipment needed for an imminent operation might be considered to be directly participating in hostilities. Moreover, regular crowdfunding organizers or social media recruiters might be considered to be engaged in a pattern of hostile acts, making them targetable until they take clear steps to permanently cease participation.[274]

---

266 *See supra* Section I.C.

267 *See International Legion of Defense*, *supra* note 84; *see also supra* Section I.C.2. (describing ways in which States rely on social media to recruit and crowdfund).

268 Kenyon & Birenbaum, *supra* note 9; *see also supra* Section I.C.1 (describing ways in which organized armed groups rely on social media to recruit and crowdfund).

269 *See supra* Section II.C (distinguishing between the DPH analysis in the IAC and NIAC context).

270 ICRC Interpretive Guidance, *supra* note 121, at 53; *see also* Commentary AP, *supra* note 139, § 1679 (critiquing the broad approach on the grounds that "in modern warfare the whole population participates in the war effort to some extent, albeit indirectly").

271 *See supra* Section I.C.2.

272 *See* ICRC Interpretive Guidance, *supra* note 121, at 53 ("[I]ndividual conduct that merely builds up or maintains the capacity of a party to harm its adversary, or which otherwise only indirectly causes harm, is excluded from the concept of direct participation in hostilities.").

273 *See* Law of War Manual, *supra* note 136, § 5.8.3; *Targeted Killings*, *supra* note 123, ¶ 37.

274 *See supra* Section II.B.3.

The analysis shifts significantly when examining these same activities in non-international armed conflicts, where the broad and narrow approaches diverge dramatically. Under the narrow approach, civilians engaging in social media recruiting or crowdfunding would generally maintain their protected status.[275] "[R]ecruiters, trainers, financiers, and propagandists" are not considered to be members of an organized armed group unless they also engage in an additional continuous combat function.[276] Therefore, a civilian using social media to recruit or raise funds for an organized armed group would remain subject to the standard DPH analysis, which would conclude they are not DPH.[277]

The broad approach, by contrast, assesses membership through activities like "following directions issued by the group" or "participating sufficiently in its activities."[278] Under this broad view, civilians who regularly engage in social media recruiting or crowdfunding for an organized armed group might be considered functional members of the group, making them continuously targetable.[279] Moreover, the broad approach requires unambiguous evidence of dissociation to terminate membership—a standard that could be difficult to meet in the context of social media activity or fundraising.[280]

D. Open-Source Intelligence Reporting

The majority of civilians engaged in conducting open-source investigations are not DPH under either the broad or narrow view since they are sufficiently removed in terms of temporality and causation from any resulting hostilities.[281] These investigations, which are often conducted in a "crowdsourced" fashion by individuals or coordinated groups of volunteers all over the world, typically focus on documentation and evidence preservation of prior events. Results of these investigations are generally not publicized in real time, and may not be publicized at all, particularly if the objective is to preserve the evidence for later prosecutions. In short, because such investigations are not tactical in nature, they cannot constitute DPH under either the narrow or broad approaches.

---

275 *See* ICRC Interpretive Guidance, *supra* note 121, at 34.

276 *Id.*

277 *See supra* Section II.B.1.

278 Law of War Manual, *supra* note 136, §§ 5.7.3.2, 4.18.4.1.

279 *See supra* Section II.C.2 (discussing the ways in which participation in activities of organized armed groups can establish membership).

280 Law of War Manual, *supra* note 136, § 5.7.3.3.

281 *See supra* Sections II.B.1–2.

However, the Ukrainian private open-source intelligence company Molfar presents an interesting case study because it occupies the extreme end of the OSINT spectrum. The information Molfar has provided to the Ukrainian military has been of a tactical nature and therefore its investigators could be considered targetable under either the narrow or broad views of DPH.[282] The fact that some time elapsed between Molfar's reporting the data to the Ukrainian government and the Ukrainian military's response (two days in the case of the Russian soldier's unit location being struck, and a few weeks with respect to the attack on the Pyatnashka Brigade),[283] suggests that the military needed some time to plan their responsive attacks, which appear to have been larger in scale than a single missile strike. In situations where there is a lengthy intervening period, it could be argued that the temporal and causal connection between the OSINT and the resulting attack becomes more tenuous. Nevertheless, this argument is harder to sustain when a military response happens within a day or two of receiving the information.

Another concern arises because Molfar seems to be engaged in a regular pattern of providing actionable OSINT to the Ukrainian military, thus potentially rendering their researchers continuously targetable under the broad view. As the OSINT industry grows, civilian OSINT researchers whose jobs will involve providing real-time tactical intelligence about an enemy—essentially the same function performed by a State's own intelligence service or military contractors—will increasingly risk losing their civilian protections and becoming targetable for DPH. This risk is compounded, particularly under the broad view of DPH, for civilians whose jobs require that they regularly perform these functions, rendering them continuously targetable.[284]

E. Starlink

Though less intuitively obvious than other examples of Crowdsourced War, Starlink demonstrates how civilian technological infrastructure and private sector capabilities can be mobilized in response to a nation's call for assistance during armed conflict.[285] When Ukraine requested assistance maintaining internet connectivity in the face of Russian attacks, SpaceX responded by activating Starlink service, mobilizing its civilian workforce to implement and maintain the

282 *See supra* Section II.A.
283 *See supra* notes 102–06 and accompanying text.
284 *See supra* Section II.B.3.
285 *See supra* Section I.E.

system, and creating mechanisms for individual civilians worldwide to contribute through terminal donations.[286]

The approaches diverge significantly on whether civilian SpaceX employees operating Starlink constitute direct participation in hostilities. A particularly complex question involves Elon Musk's personal role. As Starlink's CEO with distinctive unilateral control over the company, Musk has made direct decisions about the system's availability in combat zones—including activating the service in Ukraine upon request and later reportedly restricting its use in certain areas to prevent its application in potential attacks on Crimea.[287]

Under the narrow approach, most Starlink operations, including Musk's high-level decisions about service availability, would fall outside direct participation as they involve providing and maintaining general communications infrastructure rather than directly causing harm to the Russian military.[288] Even when this infrastructure enables specific Ukrainian military operations—like the naval drone attacks on Russia's Sevastopol base—civilian satellite operators and executives would likely maintain their protected status because their contributions are viewed as enabling military communications and coordination rather than causing direct harm.[289]

The broad approach presents a more complex picture. While maintaining general privately available satellite infrastructure would likely fall outside direct participation in hostilities, Starlink's direct integration into Ukrainian combat operations raises more difficult questions.[290] When civilian SpaceX employees maintain connections that enable real-time drone targeting or adjust coverage to support specific military operations, their actions might be viewed as sufficiently enabling military operations to constitute direct participation under the

---

286 *See supra* note 113 and accompanying text; *see also* Kan, *supra* note 115.

287 *Elon Musk Says He Denied Ukraine's Satellite Request to Avoid Complicity in "Major Act of War" vs. Russia*, CBS News (Sept. 8, 2023), https://www.cbsnews.com/news/elon-musk-ukraine-russia-war-starlink-satellite-denied-major-act-of-war [https://perma.cc/T5Z9-HVEJ].

288 Svenja Berrang, *Does the Dual-Use of Space Objects Necessitate a New Geneva Convention?*, 57 Case W. Rsrv. J. Int'l L. 315, 329 (2025), https://scholarlycommons.law.case.edu/jil/vol57/iss1/22 [https://perma.cc/5EDS-PU68] ("Because the activities of many civilian operators are too remote to constitute a direct causation or belligerent nexus, the great majority of civilian space operators cannot be considered as taking direct part in hostilities."); ICRC Interpretive Guidance, *supra* note 121, at 53 (differentiating between building military capacity and directly causing harm for purposes of DPH analysis).

289 *See* ICRC Interpretive Guidance, *supra* note 121, at 53.

290 *See, e.g.*, Turner & Norton, *supra* note 151, at 31 (describing the view of the Judge Advocate General School of the Army that civilian technicians who "make a weapon more effective" could be considered actively hostile).

broadest interpretations.[291] Musk's role becomes particularly interesting under this view—his personal decisions about where and when Starlink can be used for military operations might be seen as more directly connected to the military use of the satellites than the routine maintenance work of other SpaceX employees.[292] As a result, it is possible that he would be regarded as directly participating by virtue of his role in directing and enabling the deployment of a communications network that is essential to Ukrainian military operations. While it is unlikely that the Russian military will use lethal force to target Musk or Starlink employees,[293] if any Starlink employee were to travel to Russia, they may be at risk for detention by Russians claiming that they are unprivileged combatants in the conflict with Ukraine by virtue of their civilian participation in hostilities.

IV
New Rules for Crowdsourced War

This Article has aimed to demonstrate that interpretations of the law of armed conflict that evolved over the course of several decades largely in response to one challenge—the threat of terrorism by organized armed groups in the Middle East—now have unanticipated consequences for civilians participating in what we have called "Crowdsourced War." Crowdsourced War often enlists the services of large numbers of civilians in war—subjecting them to substantial risks as a result, often without their full knowledge of their new vulnerability. Here we examine the problems created by the rise of Crowdsourced War. We then offer recommendations for reforms. We urge the United States and other States that have adopted broad interpretations of direct civilian participation in hostilities and civilian membership in organized armed groups to reassess their positions. We also offer recommendations for revising international humanitarian law to better protect civilians in an era of Crowdsourced War.

---

[291] *See Targeted Killings*, *supra* note 123, ¶ 35 (including civilians who "collect[] information about the armed forces" as direct participants in hostilities).

[292] *See* Brad Dress, *How Elon Musk Became a Power Player in the Ukraine War*, The Hill (Sept. 13, 2023), https://thehill.com/policy/defense/4200944-how-elon-musk-become-a-power-player-in-the-ukraine-war [https://perma.cc/EV2Q-34XH] (describing Musk's influential role in determining Ukraine's access to Starlink); Ronan Farrow, *Elon Musk's Shadow Rule*, New Yorker (Aug. 21, 2023), https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule [https://perma.cc/U3M3-79MF] (same); Walter Isaacson, '*How Am I in this War?': The Untold Story of Elon Musk's Support for Ukraine*, Wash. Post, (Sept. 7, 2023), https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion [https://perma.cc/D2VQ-SR4B] (same).

[293] The nearest Starlink office is located in London. Starlink Internet Services UK Limited, Company Number 12794964, Companies House, https://find-and-update.company-information.service.gov.uk/company/12794964 [https://perma.cc/Q2Z5-VREX].

A. The Problem with Crowdsourced War

Crowdsourcing war through new technologies, such as through apps, cyber armies, and private satellites, allows those outmatched in the conventional warfighting arena to draw on popular support for their cause and thus do battle with far more powerful foes. But the rise of Crowdsourced War carries significant risk for the civilians who participate. If such civilians are identified by enemy forces, they may be targeted, consistent with international humanitarian law. Moreover, under the broad view of DPH as articulated in the U.S. Department of Defense Law of War Manual, citizens who engage in a "pattern" of DPH may be targetable far beyond when they are actively participating.

Consider the first example in Part III: ePPO and e-Enemy. Both the narrow and broad interpretive approaches agree that use of these apps by civilians can constitute direct participation in hostilities, though they differ on the duration of their DPH status. This means that users of these apps may forfeit their protected status simply by using the app. The broad approach to direct participation in hostilities magnifies this vulnerability to an alarming degree: Those using such apps may be targetable for the *entire time* the apps are installed on their phones. While the narrow approach would at least limit targeting to moments of active app use—for example, when taking a picture of Russian forces and uploading that picture to the app. As a result, the broad approach's expansive view of temporal scope and repeated participation could transform Ukraine's digital infrastructure into a mechanism for converting millions of civilians into military targets. And because it remains unclear how civilians can conclusively indicate to the enemy that they have ceased participation under the broad approach, given that the apps, even after deleted, can be easily redownloaded, they may lose that protection forever.

Under the broad approach to DPH, the millions of civilians who maintain these apps on their phones could potentially be regarded as lawful military targets. The dangers confronting civilians in such circumstances are very real. Russia[294] has targeted civilians merely for

---

294 Russia purported to withdraw from Additional Protocol I in 2019, but it remains bound both by the four Geneva Conventions and by customary international law. *See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, Int'l Humanitarian L. Databases, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/state-parties [https://perma.cc/7A26-5V2Y] (listing state parties and signatories to Additional Protocol 1); *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Russian Federation*, Int'l Humanitarian L. Databases, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/state-parties/ru?activeTab= [https://perma.cc/BL3D-HC27] (indicating Russia's purported withdrawal from Additional Protocol I).

possessing phones with photos of Russian military assets[295] and used drones to hunt civilian participants in Ukraine's defense efforts.[296] Russia has also vowed to retaliate against members of the IT Army.[297] There are numerous ways that the identities of civilian users of the apps might be revealed. They could be photographed in the act by Russian drones, the app may be detected in a personal search (a particular vulnerability for those located in occupied parts of Ukraine), or their names could be exposed through a cyberattack, which could also expose information about everyone in their contact list. Their identities may be revealed in other ways. For instance, the IT Army uses leaderboards to acknowledge its most active volunteers,[298] but this could lead to dangerous situations if the system is hacked and their true identities are revealed. Indeed, the Diia platform has already experienced security breaches exposing user data.[299]

The dangers to civilians participating in Crowdsourced War are not limited to civilians located in the countries in conflict. Because Crowdsourced War can often involve civilians from around the world, it can bring the possibility of retaliation against civilians participating in the war from outside the war zone—possibly involving other States in the conflict in the process.

Furthermore, civilians deemed to have engaged in DPH lose certain protections under the laws of war. Enemy forces do not have to consider them civilians when assessing whether a contemplated attack is indiscriminate, nor do they factor into proportionality calculations or the requirement to take precautions to avoid harming civilians when attacking military objectives or other lawful targets.[300] This risk exposes

---

295 *See* Olejnik, *supra* note 11, at 5; Judah, *supra* note 10.

296 Yogita Limaye, *Russian Drones Hunt Civilians, Evidence Suggests*, BBC News (Oct. 31, 2024), https://www.bbc.com/news/articles/c207gz7key6o [https://perma.cc/D8SY-GN7Z].

297 *See Foreign Ministry Statement on Continued Cyberattack by the "Collective West,"* Russian Ministry of Foreign Aff. (March 29, 2022), https://mid.ru/ru/foreign_policy/news/1806906 [https://perma.cc/Y7RJ-EAS3] (stating that "the cyber aggression unleashed against Russia will lead to serious consequences for its instigators and perpetrators. The sources of the attacks will be identified, and the perpetrators will inevitably be held accountable for their actions in accordance with the requirements of the law") (English language translation).

298 Pascal Geenens, *The Democratization of DDoS Attacks: Insights from the IT Army of Ukraine's Cyber Campaign*, Radware (Feb. 21, 2024), https://www.radware.com/blog/ddos-protection/the-democratization-of-ddos-attacks-insights-from-the-it-army-of-ukraines-cyber-campaign [https://perma.cc/3YNC-53UZ].

299 In 2022, there was a leak of personal information from Ukraine's driving license database on Diia. If similar identifying information for users of the open-source apps were discovered by Russian intelligence services, it could be "a death sentence" for informants. *See* The Economist, *supra* note 11.

300 *See* Additional Protocol I, *supra* note 8, arts. 48, 51(5)(b), 57(1)–(2); Schmitt & Biggerstaff, *supra* note 1, at 3.

not only the civilian who participated in the DPH attack, but it also increases the risk to other civilians and civilian objects in the area. In addition, the phones, computers, and other digital infrastructure used by civilians engaging in DPH are at risk of being treated as military objectives, which in turn raises the likelihood that these objects will be attacked and that nearby civilians and civilian objects will be harmed.

Civilians participating in Crowdsourced War also face risks of being detained or captured. Unlike lawful combatants who are considered prisoners of war when captured and afforded certain privileges, the so-called "combatant's privilege" does not apply to protect irregular or unlawful combatants like civilians who have directly participated in the hostilities.[301] If captured, these civilians would therefore lack the protections and immunities afforded to members of the armed forces of a State party to the Geneva Conventions—for example, they do not receive the protections accorded to prisoners of war.[302] Captured civilian participants in Crowdsourced War could be tried and sentenced for their war-related activities.

Finally, in a Crowdsourced War, civilian participants in hostilities often put the *enemy's* civilians at risk, contrary to the principles of international humanitarian law. For example, the majority of the IT Army's targets have been civilian in nature, including banks, companies, pharmacies, hospitals, railway networks, and civilian government services.[303] Moreover, these attacks tend to not be very sophisticated, often failing to materially advance a military objective since the target is able to recover quickly. That attack might nonetheless significantly inconvenience or harm civilians who rely on the civilian target. The decentralized nature of hacker armies makes them especially challenging to control, reform, or discipline because the members are not accountable to any central authority.

B. The Way Forward

As Crowdsourced War grows more prevalent, the law of armed conflict must keep pace with modern combat to remain effective at protecting civilians. Here we propose several responses that States and the broader international community can take to protect civilians in light of this fundamental change in the nature of war fighting.

---

301 *See* Olejnik, *supra* note 11, at 4.

302 *See id.*

303 Tilman Rodenhäuser & Mauro Vignati, *8 Rules for "Civilian Hackers" During War, and 4 Obligations for States to Restrain Them*, Humanitarian L. & Pol. (Oct. 4, 2023), https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them [https://perma.cc/27D9-2LAV].

1. Revisiting the Broad Approach

As Part II demonstrates, there are multiple approaches to determining whether civilians are directly participating in hostilities and whether they are members of organized armed groups. We have identified "narrow" and "broad" approaches; the broad approach renders a vastly larger number of civilians vulnerable to military force than does the narrow approach.

Under both approaches, civilians lose protection from attacks while engaging in actions that harm a party's military operations or capacity (threshold of harm), have a direct causal link to that harm (direct causation), and are conducted to the detriment of a party to the conflict (belligerent nexus). But the broader approach sweeps in far more civilians—sometimes including those far removed from any violent act. As we noted above, the broad interpretation of causation and temporal scope—individually and especially in combination—dramatically expands the pool of targetable civilians and the duration they may be targeted. Because Crowdsourced War makes it possible for more civilians to participate in a conflict in an indirect and distant manner, far more civilians are vulnerable to targeting and detention as a result. Moreover, their potential targetability creates vulnerability for those around them.

Similarly, under both the narrow and broad approaches, persons who serve a combat function in an organized armed group are targetable. But under the broad approach, those who provide support functions are also targetable—including those who serve as support staff, administrators, and financiers. Moreover, anyone that participates in the activities of an organized armed group can be considered to be a member, and thus targetable, regardless of formal affiliation. Last, under the broad approach, terminating membership is extremely difficult. As we have shown, all of these interpretations have significant implications for participants in Crowdsourced War in the context of non-international armed conflicts. Is an American who clicks on the YouTube contribution button for an organized armed group now a "member" who can be targeted or detained as a result?

Private contractors are also at increasing risk. Consider Palantir, Mandiant, Raytheon, and a host of other private companies that develop and service essential intelligence and cybersecurity capabilities for militaries—functions that armed forces may lack in-house.[304] Under

304 For example, Palantir has provided the Israeli Defense Forces with artificial intelligence infrastructure and services that have been essential to their operational capabilities in Gaza. *See* James Bamford, *How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza*, The Nation (Apr. 12, 2024), https://www.thenation.com/article/world/

the broadest interpretations of DPH, civilian employees at these companies who routinely service essential targeting and intelligence capabilities could be considered legitimate targets due to their work's military value.[305] While this growing reliance on private sector expertise represents a different phenomenon from Crowdsourced War—these contractor relationships involve formal contracts rather than open calls for civilian participation—they raise some of the same concerns regarding civilian vulnerability.

One answer to this problem is for those States that have adopted the broad approach to defining civilians DPH and organized armed groups to revisit those definitions. The United States could lead the way by revising the U.S. Department of State Law of War Manual to more closely reflect the narrow approach exemplified by the ICRC's guidelines. As noted earlier, the U.S. DoD Law of War Manual has adopted an interpretation of direct participation in hostilities that extends beyond actions that cause direct harm to the enemy—including training, logistical support, and providing safe house and food to a combatant.[306] The DoD definition can include "combat support" and "combat service support functions."[307] As a result, it could arguably include any civilian that uses the ePPO app to upload a photo or any civilian participating in the IT Army—not only while they are using the app or participating in a cyber operation but perhaps even while they are having dinner with their families afterwards. It could even extend

nsa-palantir-israel-gaza-ai [https://perma.cc/A8VB-H3VP]. Israel is not an outlier: "Palantir's software, which uses AI to analyze satellite imagery, open-source data, drone footage, and reports from the ground to present commanders with military options, is 'responsible for most of the targeting in Ukraine.'" Vera Bergengruen, *How Tech Giants Turned Ukraine into an AI War Lab*, Time Mag. (Feb. 8, 2024), https://time.com/6691662/ai-ukraine-war-palantir [https://perma.cc/95AA-6RAN]. And Palantir is not alone: other tech giants like Microsoft, Amazon, Google, and Starlink have also become prolific defense contractors. *See id.*; Yuval Abraham, *'Order from Amazon': How Tech Giants Are Storing Mass Data for Israel's War*, +972 Magazine (Aug. 4, 2024), https://www.972mag.com/cloud [https://perma.cc/RB8J-5J2H]; Nico Grant, *Google Worried Israeli Contract Could Enable Human Rights Violations*, N.Y. Times (Dec. 3, 2024), https://www.nytimes.com/2024/12/03/technology/google-israel-contract-project-nimbus.html [https://perma.cc/FDL5-J8NL]. For more on the way in which the government "deputizes" the private sector to take on national security roles, see Jon D. Michaels, *Deputizing Homeland Security*, 88 Tex. L. Rev. 1435, 1435 (2010).

305 *See supra* Section III.E (explaining how civilian employees working at Starlink might become targetable under the broad interpretation of DPH). The concern that civilian tech workers might be considered direct participants in hostilities is amplified by views like those of W. Hays Parks, cited in the DoD Law of War Manual, who asserts that civilian scientists working on the Manhattan Project during World War II were "liable to legitimate attack." *See supra* note 144. Though representing an extreme position, and one that the DoD Manual seemingly rejects, *see id.*, the DoD Manual's citation of this view is concerning for the countless civilian employees working in tech companies across the United States.

306 *See supra* notes 137–41.

307 Law of War Manual, *supra* note 136, § 5.8.3.

to Americans who respond to pleas on Bluesky to help fund protective gear, night vision goggles, and drones for Ukrainian soldiers. The same is true of its expansive interpretation of membership in organized armed groups.

The Law of War Manual was adopted at a time when the imagined paradigmatic conflict was a conflict between the United States and al Qaeda and its affiliates and successors. The imagined target was a person who built IEDs to be deployed against U.S. soldiers in Iraq or Afghanistan. The authors of the Manual almost certainly did not consider that the rules they were developing would apply in the near future to people taking pictures of invading Russian soldiers from their own homes or Americans responding to GoFundMe requests. But the world has shifted, and the rules developed in one context are now applying to a vast array of new situations. In the process, States who take the broad approach currently reflected in the Law of War Manual are putting more civilians—including Americans and citizens of allied countries—at greater risk than ever before. By revisiting these rules, the United States and other States that have adopted the broad interpretation of civilians DPH and organized armed groups could limit the vulnerability of civilians in wartime.

There is a strong argument that revisiting the broad approach is not just good policy but legally obligatory. Only a small number of states have openly adopted the broad approach that we outline here. Their interpretation is at odds with the narrow approach advocated by the ICRC and adopted by the many States that share the ICRC's views. Given the small number of States that have adopted the broad approach, it is clear that the broad position does not reflect customary international law. In the face of uncertainty, moreover, the legal obligation to take "constant care . . . to spare the civilian population, civilians and civilian objects"[308] and to take all feasible precautions[309] requires States to adopt the more protective approach.

---

308 Additional Protocol I, *supra* note 8, art. 57(1).

309 *Id.* art. 57(2)(a)(i) (providing that prior to any attack, all feasible precautions must be taken "to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them"). While Additional Protocol I only pertains to international armed conflicts, because the precautionary principle is deemed to reflect customary international law, it is presumed to apply in non-international armed conflicts as well. *See* Emma J. Breeze, *Duty to Act on Knowledge: Precautions, Intelligence and the Law of Armed Conflict*, 29 J. Conflict & Sec. L. 311, 315–16 (2024).

2. *State Responsibility for Civilians Participating in Crowdsourced War*

In many of the examples of Crowdsourced War described in this Article, civilians directly participating in conflict are doing so at the behest of States. When States actively encourage their citizens to participate in conflict, they may be failing in their duty to protect their own civilians from harm.

The obligation of a State to take "necessary precautions" to protect the civilian population from harm "to the maximum extent feasible" is expressly stated in Additional Protocol I to the Geneva Conventions and is widely recognized as customary international law.[310] Applied to the State's own population, the obligation to take precautions has been interpreted to prohibit States from, for example, situating military objectives within densely populated civilian areas and to require States to evacuate civilians from areas likely to be targeted.[311] Yet States' obligations to their civilians are not limited to these circumstances. The obligations to take precautions and exercise constant care to spare the civilian population may also be understood to require that a State not encourage its civilians to engage in actions that could subject them to lawful targeting by the enemy.[312] At a minimum, State action that encourages civilians to take actions that may be interpreted by the enemy as direct participation in hostilities is best understood to trigger an affirmative duty for the State to warn its civilians of the risk to which they will be subject as a result.[313]

Many States that have encouraged civilians to participate in Crowdsourced War do not appear to have provided those civilians with adequate notice of their vulnerability as a direct result of their participation. It is troubling, for example, that the Ukrainian government does not seem to have warned its citizens of the risks they may be exposed to through use of ePPO and e-Enemy. Rather, Ukrainian officials are actively encouraging citizens to use these apps to report Russian war activity. Instructing users to simply delete images and messages from their phones after uploading them may not be an

---

310 Additional Protocol I, *supra* note 8, art. 58; Breeze, *supra* note 309.

311 *See* Law of War Manual, *supra* note 136, at 280–81 §§ 5.14.1–5.14.2; *id.* at 280 § 5.14 ("Outside the context of conducting attacks (such as when conducting defense planning or other military operations), parties to a conflict should also take feasible precautions to reduce the risk of harm to protected persons and objects from the effects of enemy attacks.").

312 Dan Maurer, *A State's Legal Duty to Warn its Own Civilians on Consequences of Direct Participation in Hostilities*, Lieber Inst. (Feb. 21, 2023), https://lieber.westpoint.edu/states-legal-duty-warn-civilians-consequences-direct-participation-hostilities [https://perma.cc/EC6N-KQQT].

313 *Id.* (suggesting that the ePPO app should contain a simple, blunt legal disclaimer the user must read before downloading the app).

adequate safety precaution if a hack or cyberattack reveals information about the users of the app.[314] Moreover, the widespread dissemination of an app to the civilian population for these purposes may have the effect of making any civilian a suspect of collecting intelligence for the Ukrainian military. Although this would not justify Russia's targeting of civilians, Ukraine must be aware that its decision to appeal to the entire civilian population in this way could have this dangerous impact.

It is true that even if informed of the risk, civilians may choose to use the apps because they perceive the benefits to outweigh the risks. The apps have had a concrete impact in helping Ukraine's military defense. And the digitalization of war enables individuals who may feel helpless to get involved.[315] Still, the implications for States who encourage their citizens to engage in Crowdsourced War need to be considered, particularly to the extent that such participation may violate international humanitarian law.

There are a number of domestic legal reforms that could help. The ICRC, for example, has recently encouraged States to adopt and enforce national laws that regulate civilian hacking.[316] While acknowledging that international humanitarian law does not outright prohibit civilians from conducting cyber operations against military assets, the ICRC has proposed "8 Rules for Civilian Hackers."[317] These rules prohibit cyberattacks against civilian objects, prohibit the use of malware that may attack military and civilian objects indiscriminately, and reiterate international humanitarian law concepts of proportionality and how these should apply when civilians use digital technologies to assist in armed conflict.[318] The ICRC also recently released the report of its global advisory board, which contains similar guidance for States, belligerents, tech companies, and humanitarian organizations.[319] In response to these rules, the IT Army has purportedly agreed to de-escalate its attacks and to comply with the new rules of engagement.[320]

---

314 *See supra* notes 294–99 and accompanying text.

315 *See* Kateryna Zarembo, Michèle Knodt & Jannis Kachel, *Smartphone Resilience: ICT in Ukrainian Civic Response to the Russian Full-Scale Invasion*, Media, War & Conflict, March 18, 2024, at 4.

316 *See* Rodenhäuser & Vignati, *supra* note 303.

317 *Id.*

318 *Id.*

319 ICRC Glob. Advisory Board on Digit. Threats During Armed Conflicts, Protecting Civilians Against Digit. Threats During Armed Conflict: Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations (Sept. 2023) [hereinafter ICRC Glob. Advisory Board].

320 *See* Joe Tidy, *Ukraine Cyber-Conflict: Hacking Gangs Vow to De-escalate*, BBC (Oct. 6, 2023), https://www.bbc.com/news/technology-67029296 [https://perma.cc/E8U9-9AG9].

These recommendations are critically important, and States that invite citizen hackers to support their war effort should adopt them. Indeed, these recommendations should not be limited to civilian participation in cyber operations. Where States are encouraging civilians to participate in a war effort through any form of Crowdsourced War, similar legal obligations apply: States must instruct civilians working on their behalf of their obligation to comply with international humanitarian law. If these civilians fail to do so, the State must investigate and prosecute violations.

The aforementioned ICRC rules for "civilian hackers" are a step in the right direction, but they do not address a critical concern raised in this Article—the vulnerability of the civilians participating in Crowdsourced War to violence by participants in the conflict. The ICRC acknowledged that "civilian hackers risk exposing themselves, and people close to them, to military operations," and that "the computers and digital infrastructure they use risk becoming military objectives" and thus risk being attacked, but it offered no specific guidance to address these concerns.[321]

We recommend, at a minimum, that States inform civilians before encouraging them to participate in Crowdsourced War activities that could potentially turn them—and their property—into military objectives that could be targeted by the opposing military forces. It should warn them, as well, that their participation in armed conflict as a civilian does not immunize them from ordinary criminal law and that they may be subject to law of war detention if identified as participants in armed conflict by enemy armed forces.

3. International Humanitarian Law Reform

Crowdsourced War has profound ramifications for international humanitarian law itself. As more civilians engage in Crowdsourced War, they not only place themselves and other civilians at risk, but also erode the principle of distinction between civilian and combatant.

As noted above, the ICRC has become increasingly concerned about the risks that Crowdsourced War presents to civilians as well as the erosion of the international humanitarian law principle of distinction. Its "8 Rules for Civilian Hackers"[322] and global advisory board report[323] both point to the need to develop the rules that apply to some aspects of Crowdsourced War—civilians participating in cyber operations in

321 Rodenhäuser & Vignati, *supra* note 303; ICRC Glob. Advisory Board, *supra* note 319.
322 Rodenhäuser & Vignati, *supra* note 303.
323 ICRC Glob. Advisory Board, *supra* note 319.

the case of the "8 Rules" and broader issues of digital threats during armed conflict in the case of the advisory board report.

Neither of these documents, however, gets to the key problem raised in this Article: the new and growing threat to civilians in a world of Crowdsourced War. Several of the global advisory board report's recommendations aim to distinguish between military and civilian uses of technology infrastructure.[324] For example, the report recommends that tech companies should, "to the maximum extent feasible, segment data and communications infrastructure they provide for military purposes from civilian ones."[325] But the phenomenon of Crowdsourced War is arguably at odds with this recommendation and others in the report, as it harnesses what would otherwise be civilian property and resources for military purposes. Segregating civilian and military infrastructure is protective only if the civilians are not themselves participating in military operations.

The ICRC issued its Interpretive Guidance a decade-and-a-half ago.[326] With more than two decades of experience in the post-9/11 era behind us, the full range of consequences of the interpretive issues addressed in that effort have become even more clear. The rise of Crowdsourced War makes it even more pressing for States to rally behind a cohesive interpretation of when civilians directly participating in hostilities and members of organized armed groups are targetable. It is time, then, for a new effort to strengthen the protections that international humanitarian law offers to civilians. To close the gap created by Crowdsourced War, the ICRC, together with States that are committed to the rule of law, should renew efforts to tighten standards for targeting civilians.

Conclusion

The horrors visited on civilians in two world wars in the first half of the twentieth century—in which tens of millions of civilians lost their lives—led to a shared global conviction that it was essential to create rules that would insulate civilians from violence during war. In 1949, States came together to rewrite the rules that would govern the conduct of war. The Four Geneva Conventions and their Additional Protocols established a new principle of distinction—a principle that requires civilians and combatants to be distinguished from one another. This principle served as the foundation for what was meant to be a more

---

324 *See id.* at 4.
325 *Id.* at 4.
326 ICRC Interpretive Guidance, *supra* note 121, at 8.

humane era of warfare. Though war might not be prevented, it was hoped that civilians would be spared.

Crowdsourced War threatens to upset that achievement. By allowing civilians to participate in war more easily, it opens the door to involving larger numbers of civilians in conflict. The dangers of Crowdsourced War are amplified by the expansive interpretations of international humanitarian law adopted after the attacks on the United States on September 11, 2001. Facing threats from non-State actor groups, the United States led the way in interpreting the law to define civilians with limited connections to armed conflict as civilians directly participating in hostilities or as members of organized armed groups. The United States and other States that adopted the broad interpretation of DPH expanded the aperture of civilians that were targetable. In an era of Crowdsourced War, that broad interpretation has unanticipated effects—threatening to place large numbers of civilians squarely in the crosshairs and making those around them acutely vulnerable. The risk extends beyond those in conflict zones to civilians worldwide who contribute to crowdfunding sites or engage in coordinated cyber operations against belligerents. It is time to revisit the rules of war once again, to ensure that the era of Crowdsourced War does not become the era in which the distinction between civilian and combatant evaporates.