The Hague Centre
for Strategic Studies

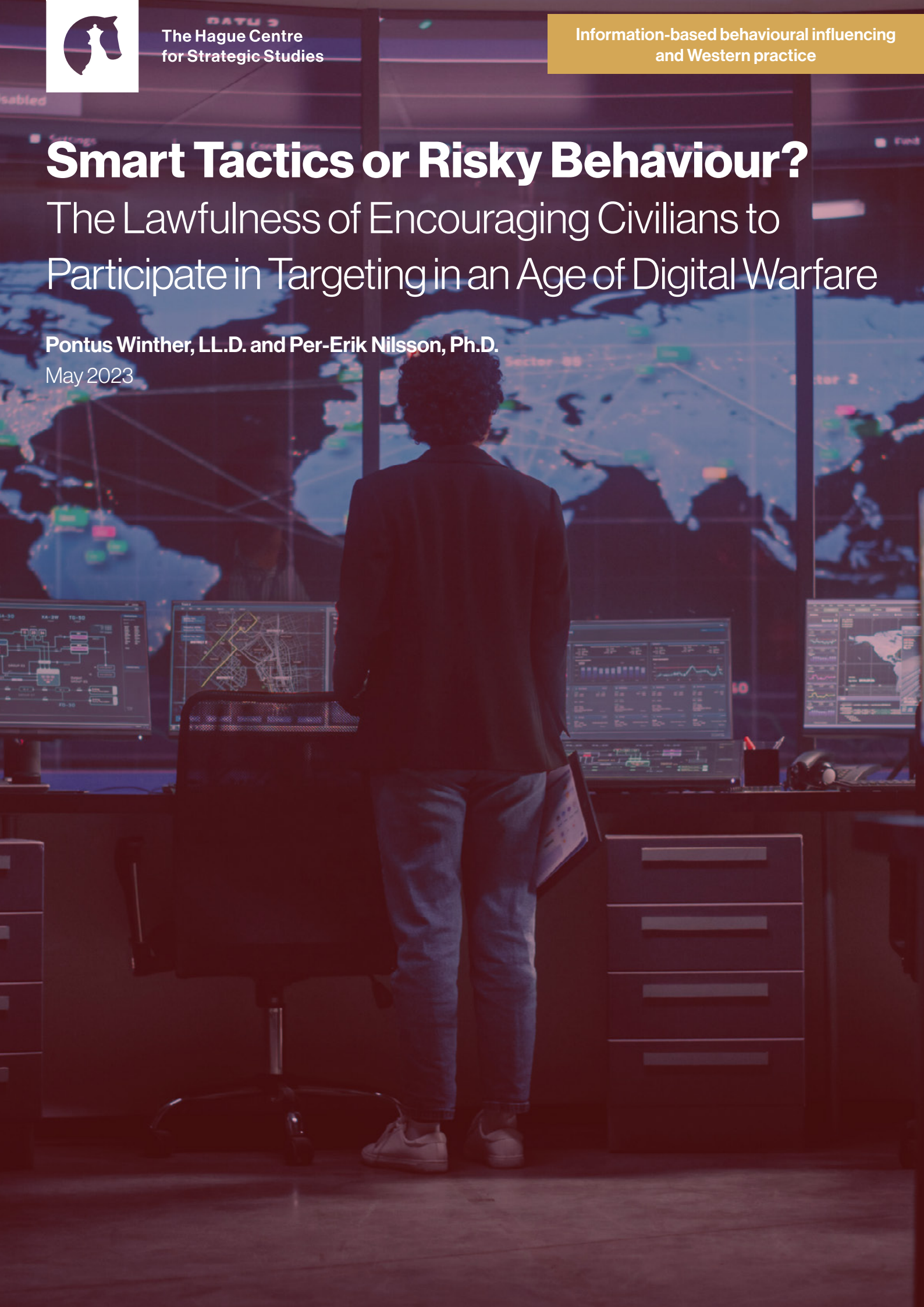
Information-based behavioural influencing
and Western practice

Smart Tactics or Risky Behaviour?

The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare

Pontus Winther, LL.D. and Per-Erik Nilsson, Ph.D.

May 2023



The Hague Centre
for Strategic Studies

Paper 2

Smart Tactics or Risky Behaviour?

The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare

Authors:
Pontus Winther, LL.D. and Per-Erik Nilsson, Ph.D.

This paper is part of the *Information-based behavioural influencing and Western practice* paper series.

May 2023

This paper is published as part of the project Platform Influencing Human Behaviour, commissioned by the Royal Netherlands Army. The aim of this platform is to build and share knowledge on information-based behavioural influencing in the military context. We bring together international experts and practitioners from both military and academic backgrounds to explore the military-strategic, ethical, legal, and societal issues and boundaries involved. Responsibility for the content rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Royal Netherlands Army.

Paper series: Information-based behavioural influencing and Western practice

The military application of information has a long history in influencing the outcome of war and conflict on the battlefield. Be it by deceiving the opponent, maintaining troop confidence, or shaping public opinion. These tactics are placed under the banner of influencing human behaviour. Behavioural influencing is the act of meaningfully trying to affect the behaviour of an individual by targeting people's knowledge, beliefs and emotions. Within the Dutch armed forces these tactics fall under title of Information Manoeuvre. With the ever-larger and more evasive employment of information-based capabilities to target human cognition, the boundaries of the physical and cognitive battlefield have begun to fade.

This paper is published as part of the project *Platform Influencing Human Behaviour*, commissioned by the Royal Netherlands Army. The aim of this platform is to build and share knowledge on information-based behavioural influencing in the military context. We bring together international experts and practitioners from both military and academic backgrounds to explore the military-strategic, ethical, legal, and societal issues and boundaries involved. Responsibility for the content rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Royal Netherlands Army.

For this paper series scholars, experts and policymakers submitted their papers on the employment of information-related capabilities to influence human behaviour in the military context. From the perspective of an individual European or NATO country's perspective. The Information-based behavioural influencing and Western practice paper series is edited by Arthur Laudrain, Laura Jasper and Michel Rademaker.

Seven papers will be published in this series. These are the following:

- **Deception as the Way of Warfare. Armed Forces, Influence Operations and the Cyberspace paradox.** By Colonel dr. Peter B.M.J. Pijpers, Netherlands Defence Academy and University if Amsterdam, and Brigadier-General prof. dr. Paul A.L. Ducheine, Netherlands Defence Academy and University of Amsterdam
- **Influencing security professionals: are they biased and by which source?** By Johan de Wit, TU Delft & Siemens Smart Infrastructure
- **A discursive analytical approach to understanding target audiences. How NATO can improve its actor-centric analysis.** By Yannick Smits, Research Master Middle Eastern studies Leiden University
- **The concept of Information Manoeuvre: Winning the Battle of Perceptions.** By Judith T. van de Kuijt (TNO), N. Keja (TNO), J.C. Slaager (TNO)
- **Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare.** By Pontus Winther, LL.D. Swedish Armed Forces, and Per-Erik Nilsson, Ph.D. Swedish Defence Research Agency and Associate Professor at Uppsala University
- **Cognitive Warfare as Part of Society: Never-Ending Battle for Minds.** By Robin Burda, Ph.D. candidate Security and Strategic Studies Masaryk University
- **Behavioural Influence Interventions in the Information Environment: Underlying Mechanisms and Technologies.** By dr. Hans Korteling (TNO), Beatrice Cadet (TNO), Tineke Hof (TNO)

Introduction

During the first year of the full-scale Russian invasion of Ukraine, the list of suspected war crimes committed by the Russian armed forces and its proxies will most likely continue to grow as more and more evidence is gathered. The perhaps most emblematic case so far are the mass-killing of civilians in Bucha. In a journalistic account a Russian defector, who was on the ground in Bucha, explained that his unit had been given a "'direct command to murder' anyone sharing information about the unit's position whether military or civilians."[1] More bluntly: "If someone had a phone – we were allowed to shoot them."[2]

A cynical reading of the soldier's story is that Russian authorities had planted the story to explain the unexplainable. In International Humanitarian Law (IHL), a civilian who is directly participating in hostilities (DPH) forfeits her or his protection against direct attack.[3] As a response to the Russian invasion, Ukrainian civil and military authorities have been ingenious in making use of the smartphone's potential to be an advanced sensor with military applications. For example, through quickly developed or tweaked applications and chatbots, ordinary citizens have been able to become rather advanced "spotters" of enemy movements.

Digital technology in contemporary war complicates the boundaries between combatants and civilians.

This is but one example of how digital technology in contemporary war complicates the boundaries between combatants and civilians. Drawing on earlier work in international law, media- and communications studies, and war studies,[4] this paper aims to discuss what the implications of this development are in relation to the rules of IHL.

Civilian Participation in Digital Armed Conflicts

Ideally, in an armed conflict, soldiers fight. Not civilians. Looking back at the history of armed conflict however, Roberts concludes that civilians are typically "both agents and victims; both co-players in the theatre of war and objects of propaganda; both participants in the war economy and protected persons in the laws of war."[5] Already in 1952 the US Supreme

1 Fred Pleitgen, Claudia Otto, and Ivana Kottasová, "'There Are Maniacs Who Enjoy Killing,' Russian Defector Says of His Former Unit Accused of War Crimes in Bucha," CNN, December 14, 2022, https://www.cnn.com/2022/12/13/europe/russian-defector-war-crimes-intl-cmd/index.html.

2 Pleitgen. Otto, and Kottasová, "'There Are Maniacs."

3 For the application of this rule in international armed conflicts, see Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977, 1125 UNTS 3 (AP I), Art. 51 (3). The rule is also widely held to be binding as customary international humanitarian law, see *e.g.* ICRC, International Humanitarian Law Database, Rule 6, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule6 (last visited 10 May 2023).

4 In particular: Michael N. Schmitt and William Casey Biggerstaff, "Ukraine Symposium – Are Civilians Reporting With Cell Phone Directly Participating in Hostilities," *Articles of War,* Lieber Institute, West Point, November 2, 2022, https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/; Michael N. Schmitt, "Ukraine Symposium – Using Cellphones to Gather and Transmit Military Information," *Articles of War*, Lieber Institute, West Point, November 4, 2022, https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/; Pontus Winther, "Military influence operations & IHL: Implications of new technologies", ICRC, Humanitarian Law and Policy Blog, October 27, 2017, https://blogs.icrc.org/law-and-policy/2017/10/27/military-influence-operations-ihl-implications-new-technologies/.

5 Roberts, Adam. "The Civilian in Modern War." In *The Changing Character of War*, edited by Hew Strachan and Sibylle Scheipers, 357-380, p. 361. (Oxford and New York: Oxford University Press, 2011). In this interdisciplinary paper, the term "armed conflict" used in international law and the term "war" used in political science are used alternately and interchangeably.

Court Justice Douglas asserted: "In these days of total war, manpower becomes critical, and everyone who can be placed in a productive position increases the strength of the enemy to wage war."[6]

If total war since long has contributed in rendering the role of civilians multifaceted and complex, the advent of the Digital Age have even further blurred the boundaries between combatant and civilian. Numerous scholars and analysts have pondered upon the changing nature of contemporary warfare in relation to digital technology.

William Merrin describes how digital technologies radically changed how war was mediated. In the 1990's, top-down military media management was at its peak. The US armed forces had developed a system for tight control of how war was narrated and showcased to a global audience. The web 2.0 and participative digital communication however meant "the USA's 1990s' dreams of achieving military, battlefield 'full spectrum dominance' were destroyed."[7] The result was a "new form of 'participative war' where anyone – including interested parties from around the globe – can share their experiences and images, comment, and promote their preferred cause."[8]

For anyone with an Internet connection, the theatre of war is merely a swipe away.

The rapidly expanding tech-sector democratised new forms of technologies and potential for connectivity and in a heartbeat civilian communications technology were outperforming military technology. In 2012, referring to wearable devices like the smartphone, a US Army specialist on digital technology stated" [n]o defense company in the world can beat the reliability and performance these small devices deliver."[9]

In particular, the smartphone has conflated military and civilian usages and actors. As Roman Horbyk puts it, "[t]he broad use of mobiles in the warzone disrupts the closed nature of the military as state institution... introducing new corporate actors beyond the traditional weapon manufacturers to the frontline concatenation, now embracing mobile phone producers, Big Tech, small local IT enterprises."[10]

Today, readily available off-the-shelf communication technology has the potential to place its user in the midst of an endless global information flow where every user is a potential producer of high-quality content with a global reach. For anyone with an Internet connection, the theatre of war is merely a swipe away. Travelling to the theatre of war through the digital information environment is however not only a matter of being a spectator of war. Digital technology has also created an unprecedented potential for wartime participatory media practices.

Horbyk argues, the smartphone merges "private communications and entertainment" with functions such as "fire targeting, minefield mapping and combat communication" meaning that it becomes a "mediated extension of battlefield" that have come to "question the very definition of what constitutes weapon as tool of combat."[11]

6 U.S. Supreme Court, Kawakita v. United States, 343 U.S. 717 (1952), No. 570, Argued April 2–3, 1952, Decided June 2, 1952, 343 U.S. 717, https://supreme.justia.com/cases/federal/us/343/717/.

7 William Merrin, *Digital War: A Critical Introduction* (London and New York: Routledge, 2019), p. 3.

8 Ibid.

9 Jason Regnier in John Mchale, "Smartphones on the Battlefield," *Military Embedded Systems* (blog), December 5, 2012, https://militaryembedded.com/comms/communications/smartphones-the-battlefield.

10 Roman Horbyk, "'The War Phone': Mobile Communication on the Frontline in Eastern Ukraine," *Digital War* 3, no. 1 (2022): 9–24, p. 23. https://doi.org/10.1057/s42984-022-00049-2.

11 Horbyk, "'The War Phone'," p. 9.

For the civilians of our Digital Age,[12] this has led to a far-reaching potential to participate in warfare where old practices are amplified with civil digital technology, further blurring the boundaries between combatant and civilian. During the full-scale Russian invasion, this development manifests itself in several ways, not the least by civilian "spotters" (*i.e.* observers who detect and report enemy movements and positions) that moreover is encouraged by the Ukrainian state.[13]

As "spotters", civilians can use the chatbot eVorog (єВорог) to contribute to the Ukrainian armed forces' targeting process by reporting enemy movements, activities, and collaborators. The chatbot is based on the messaging platform Telegram, and with the chatbot users can send photos, videos, geolocations, and descriptions of suspected activities. Ukrainian authorities clearly encourage civilians to use it and frame it like a civilian public intelligence function: "We are grateful to everyone who joins the people's intelligence. Together we will drive the enemy out of the Ukrainian land! Together to victory!"[14] At the time of writing, approximately 400 000 Ukrainians have used the chatbot.

As "spotters", civilians can use the chatbot eVorog (єВорог) to contribute to the Ukrainian armed forces' targeting process by reporting enemy movements, activities, and collaborators.

Another "spotting" tool is the smartphone application "ePPO" that civilians can download and use to report air threats by simply pointing their phone to the threat and pressing a red button.[15] The purpose of the app appears to be defensive, in particular to signal the incoming Iranian Shaheed-136 drones that the Russian armed forces started to deploy *en masse* in October 2022.[16] When launching the app six months into the war, the Strategic Communications Department of the Office of the Commander-in-Chief of the Armed Forces of Ukraine declared "[n]ow every citizen of Ukraine can join the anti-missile and anti-aircraft defense of our skies."[17] Shortly after its launch, the app had been downloaded over 180 000 times.[18]

These two examples showcase that civilians with a simple computer or a smartphone can easily turn from being bystanders to participants and even "become part of the kill chain", as Ford puts it.[19] Moreover, as Ford points out, these practices are using civilian information technological infrastructure meaning that the users leave digital traces of their activities. This risks in itself turning protected civilian infrastructure into targetable military objectives.

While these initiatives are a testimony of Ukrainian morale and resilience, from the perspective of IHL they need extra consideration.

12 A case could be made that we are living in a post-digital age. Digital technology no longer is a disruptive technology but an integrated part of all aspects of life, including warfare. See: Ben. O'Loughlin, "Towards a Third Image of War: Post-Digital War," Digital War 1, no. 1 (2020): 123–30, https://doi.org/10.1057/s42984-020-00015-w.

13 There are numerous of initiatives for volunteers to support the war effort. See for example the Bee Safe initiative: "Bee Safe: About Us," Bee Safe, accessed March 10, 2023, https://beesafe.in.ua/?utm_source=a5o5_adwords&utm_medium=cpc&utm_campaign=cid_18143278285_search&utm_term=ukraine%20army; See also the Dream Ukraine initiative: "Dream UA: Home," Dream Ukraine, accessed March 10, 2023, https://www.dreamua.win/?gclid=EAIaIQobChMIop-4iIi9_QIVikFIAB2cgQASEAAYAiAAEgKNVfD_BwE.

14 Committee on Digital Transformation, "Закликаємо повідомляти про окупантів чи колаборантів у чатбот єВорог [We urge you to report occupiers or collaborators to the chatbot eVorog, - Committee on Digital Transformation]," Verkhovna Rada, accessed March 10, 2022, https://www.rada.gov.ua/news/news_kom/229367.html.

15 For instructions on how to use the app, see: "The ePPO Application Has Started Working in Ukraine: How to Notify the Armed Forces of Ukraine about a Missile or a Drone," Visit Ukraine, accessed March 10, 2023, 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.

16 See: Schmitt and Biggerstaff, "Ukraine Symposium."

17 Jerusalem Post Staff, "New App Lets Civilians Help Shoot Down Drones and Missiles in Ukraine," *Jerusalem Post*, October 17, 2022, https://www.jpost.com/international/article-719836.

18 Dan Sabbagh, "Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks," *The Guardian*, October 29, 2022, https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo.

19 Matthew Ford, "Download. Geolocate. Fire and Forget: The Smartphone at War," Manuscript, March 11, 2022, p. 6.

Civilians' Direct Participation in Hostilities

In any armed conflict, the parties to the conflict must abide to applicable rules of IHL. The rules of IHL are, with the words of the International Committee of the Red Cross (ICRC), "those rules of international law which establish minimum standards of humanity that must be respected in any situation of armed conflict".[20] One of the core principles of IHL is the principle of distinction. It means, as far as individuals are concerned, that parties to an international armed conflict must distinguish between combatants and civilians. Combatants are described in Article 43 (2) AP I – broadly speaking and with certain exceptions – as members of the armed forces of a party to an international armed conflict, except medical personnel and chaplains.[21] Article 50 (1) AP I explains that any person who is not a combatant is a civilian. While combatants have a right to directly participate in hostilities according to Article 43 (1) AP I, civilians have no such right in IHL. The main rule in armed conflict is therefore that civilians shall not be the object of attack, Article 51 (2) AP I. However, this rule comes with one important exception. According to Article 51 (3) AP I, civilians are only entitled to this protection "unless and for such time as they take a direct part in hostilities".[22]

Direct participation in hostilities does not alter the legal status of civilians.

The rule in Article 51 (3) AP I thus constitutes the pivoting point of the principle of distinction as far as individuals are concerned. It means that civilians lose the protection against the effects of hostilities otherwise afforded to them if and when they take a direct part in the hostilities. Therefore, when the act that constitutes direct participation in hostilities ceases, civilians regain their full protection against the effects of hostilities provided by IHL. This is sometimes referred to as the "revolving door" mechanism. It is also important to note that even though – as stated above – IHL does not provide any *right* for civilians to take direct part in hostilities, there is no *prohibition* in IHL to do so either. It is another question that a party to an armed conflict may have *domestic* laws that provide for the arrest, investigation and prosecution of civilians for directly participating in hostilities. Moreover, direct participation in hostilities does not alter the legal status of civilians. In particular, they do not acquire the formal status of combatants solely by taking a direct part in hostilities. Lastly, the rule on DPH does not contain any exception for certain groups of civilians, not even for those who are bestowed with additional legal protection, such as children or civilian medical personnel.

It is against this legal background that the practice of targeting Ukrainian civilians with cell phones must be viewed. It is a breach of IHL, and may indeed even be a war crime,[23] to attack civilians with cell phones unless, and then only for such time as, they take a direct part in the hostilities. The question that thus has to be answered is: does the act of civilians "spotting" Russian forces with the help of cell phone apps or chatbots, as illustrated above, qualify as DPH, and if so, under which circumstances?

ICRC suggests the following three cumulative elements for an act to amount to DPH.[24] They are used as an analytical framework to answer the question posed above.

20 Nils Melzer, "International Humanitarian Law – A Comprehensive Introduction", (Geneva: ICRC, 2016), p. 17.

21 AP I, Art. 43 (2). Both Ukraine and Russia have ratified AP I, https://ihl-databases.icrc.org/public/refdocs/IHL_and_other_related_Treaties.pdf.

22 Art. 51 (3) AP I.

23 See e.g. Rome Statute of the International Criminal Court, 17th July 1998 (2187 UNTS 3), Art. 8 (b)(i).

24 Nils Melzer, "Direct Participation in Hostilities under International Humanitarian Law", (Geneva: ICRC, 2009), p. 46.

1. The act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm),
2. 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 (direct causation), and
3. 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 (belligerent nexus).

The period of direct participation should commence when a civilian makes concrete preparations for reporting, or with other words, from the period in time where the civilian actively starts looking for Russian forces.

When it comes to the first element, the threshold of harm, it appears clear that the use of a chatbot like "eVorog" or the app "ePPO" is at least *likely* to adversely affect Russian military operations or capacity. This is so because of the general likelihood that the information provided via those "spotting-channels" results in attacks on, or other effects for, the Russian forces. Indeed, the ICRC guidance specifically mentions transmitting tactical targeting information for an attack as one example of an act that meets this requirement.[25]

The second element, direct causation, may or may not be met in the case of civilian "spotting" Russian forces. It depends on how information is transmitted. In the situation in Ukraine, at least the chatbot eVorog appears to be designed to *directly* convey relevant information to the Ukrainian armed forces for targeting purposes. Even if the act of conveying information about the character and position of Russian armed forces with eVorog does not *in itself* result in the requisite harm, such an act should arguably be considered "an integral part of a concrete and coordinated tactical operation that directly causes such harm",[26] and therefore meet the requirement of direct causation.

Lastly, concerning the third element, belligerent nexus, it seems that at least the act of reporting through the eVorog chatbot normally is done in support of Ukraine's war efforts and to the detriment of Russia's. In contrast, the use of an air-raid alert app to warn fellow civilians in order to be able to take shelter would arguably not reach the threshold of belligerent nexus, even though it may affect the Russian operations negatively. Thus, if the ePPO app is used to warn the civilian population, such acts would not be specifically designed to reach the threshold of harm required. Neither would, incidentally, an app by which civilians can report suspected war crimes to Ukrainian authorities reach that threshold.

It thus appears that if a civilian uses at least the eVorog chatbot in the way it is intended to be used, that use may amount to direct participation in hostilities. It consequently entails the loss of legal protection against direct attack normally awarded to civilians. A more complicated question is, however, when that loss of protection begins and ends. As noted above, civilians loose their protection only "for such time as" the direct participation in hostilities lasts. Schmitt and Biggerstaff have suggested that the period of direct participation should commence when a civilian makes concrete preparations for reporting, or with other words, from the period in time where the civilian actively starts looking for Russian forces. The direct participation continues over the time where the actual reporting is being made, and does not cease until the reporting has been completed and the civilian has stopped to actively look for Russian forces.[27]

25 Melzer, "Direct Participation in Hostilities under International Humanitarian Law", p. 48.

26 Melzer, "Direct Participation in Hostilities under International Humanitarian Law", p. 54-55.

27 Michael Schmitt and William Biggerstaff, "Ukraine Symposium – Are Civilians Reporting With Cell Phone Directly Participating in Hostilities".

Naturally, this temporal extent of loss of protection poses considerable practical difficulties.[28] For one, it is far from always possible to establish with certainty whether a civilian is "actively looking" for opposing forces or not. For this case, Article 50 (1) AP I specifically promulgates that in case of doubt whether a person is a civilian, that person shall be considered to be a civilian. Moreover, the determination of DPH must be made on a case-by-case basis. Therefore, attacks on civilians by Russian armed forces based on a general presumption that *any* civilian with a cell phone is a person that takes a direct part in hostilities constitute a misinterpretation and a violation of the DPH rule, and may, as was previously noted, also amount to a war crime.[29]

Encouraging Civilian Participation in the Targeting Process

To encourage Ukrainian civilians to report Russian forces may effectively be to encourage them to take a direct part in hostilities.

Important and difficult as it is, the question regarding DPH is only one side of the legal coin in this situation. The other side of that coin is the question concerning whether, and if so to what extent, IHL prohibits a party to an armed conflict, in this case Ukraine, to encourage or otherwise influence civilians to act as "spotters". As follows from the above, to encourage Ukrainian civilians to report Russian forces may effectively be to encourage them to take a direct part in hostilities, with loss of protection for the duration of that participation as a direct legal consequence. It is evident that the Ukrainian authorities are conscious about the fact that "spotting" may cause serious danger for civilians. For example, in their instructions to the chatbot eVorog, the Ukrainian Ministry of Defence instructs users to "[r]emove carefully and clean your phone after using the chatbot. It is necessary to delete the personnel of the occupiers or equipment and correspondence with the chatbot. It can save your life."[30]

The risks for civilians notwithstanding, there exists no explicit prohibition in IHL on encouraging civilians to take a direct part in hostilities. However, there are provisions that may *restrict* certain activities to this effect.

The first and most obvious of these restrictive provisions is the obligation to ensure that children do not take a direct part in hostilities. Article 77 (2) of AP I provides that "[t]he Parties to the conflict shall take all feasible measures in order that children who have not attained the age of fifteen years do not take a direct part in hostilities". This provision is not merely a prohibition of encouraging children under the age of fifteen to take a direct part in hostilities. It is also an obligation to take *active measures* in order to ensure that those children do not take a direct part in hostilities. Consequently, both the direct encouragement of children to use chatbots such as the eVorog and the failure to take measures to ensure that children do not use it would be contrary to this provision. It is therefore incumbent on Ukrainian authorities to take all feasible measures so that children under the age of fifteen do not use such tools, for example by imposing an age limit on the use of them.

28 See in particular the discussion in Schmitt/Biggerstaff on the revolving door dilemma and the discussion by ICRC about continuous combat function in Nils Melzer, "Direct Participation in Hostilities under International Humanitarian Law", p 44-45.

29 See at fn. 23 above.

30 Ministry of Defence Ukraine, "Побачили С400, С300, Буратіно/Солнцепьок чи Іскандер? Повідомте в чатбот єВорог [Have you seen C400, C300, Pinocchio/Colnetsepok or Iskander? Report to chatbot eVorog]," Facebook, February 9, 2023, https://www.facebook.com/MinistryofDefence.UA/posts/pfbid-083DWJBJUkD4oVwMZwK92Vb58PJNKLiAqt6uRZwPrKy3UxVZ22Mfcaf59DifQGzRPl.

A second provision of relevance in this case is enshrined in Article 51 (1) AP I. It provides that "[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations". A similarly phrased obligation is expressed in article 57 (1) AP I. It holds that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects". These obligations apply to the act of Ukrainian authorities' encouraging civilian "spotting", since such activities are integral parts of the Ukrainian armed forces targeting process. The question is what the notions "general protection" and "constant care" mean in this context. From the wording of the provisions, it seems that they do not simply entail a duty to abstain from military operations that entail risks for civilians. They rather seem to express a duty to conduct operations in a manner where operational requirements and risks for civilians are balanced in a sensible way. This is also the way in which the ICRC Commentary to AP I understands them: "[t]here is no doubt that armed conflicts entail dangers arising from military operations, but these should be reduced to a minimum".[31] It is therefore suggested here that the duties includes taking measures such as constantly evaluating the risks for civilians associated with "spotting", as well as providing instructions on how and by whom such "spotting" may and may not be done, and how to avoid the risks associated with it.

It is therefore suggested here that the duties includes taking measures such as constantly evaluating the risks for civilians associated with "spotting", as well as providing instructions on how and by whom such "spotting" may and may not be done, and how to avoid the risks associated with it.

Conclusions

In conclusion, civilians participating in the Ukrainian armed forces targeting process by "spotting" Russian forces, for example via the chatbot eVorog, run a risk of losing their legal protection from direct attack during that participation. While it is true that IHL does not prohibit civilians to take a direct part in hostilities, it is equally true that IHL does not prohibit attacking them while that participation is ongoing. This has certain consequences from a legal perspective. First and most obvious, Ukrainian civilians risk being lawfully killed or injured by Russian armed forces without any corresponding legal right for Ukrainian civilians to use force against Russian armed forces. Such right follows only with the status as a combatant. Second, since direct participation in hostilities is not a *right* for civilians similar to that for combatants, if detained by Russian forces Ukrainian civilians run the risk of being put before trial by Russia for their direct participation in a manner that Russian domestic law dictates instead of being provided legal protection as prisoners of war. Third, a widespread civilian participation in the targeting process can make it more difficult to prove Russian breaches of IHL and thus make it more difficult to prosecute members of the Russian armed forces for the war crime of intentionally directing attacks against civilians.

If Ukraine encourages the use of cell-phone "spotting tools" in a way that may amount to direct participation in hostilities, it is essential that such encouragement be accompanied by instructions on precautionary measures so that civilians have a possibility to avoid the dangers associated with the use of these tools. These measures should at least include ensuring that children under the age of fifteen years do not take a direct part in the hostilities, as well as instructions so that civilians fully understand the legal risks of participating directly in hostilities.

31 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), "Commentary on the Additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949" (Geneva: ICRC, 1987), para. 1875.

References

"The ePPO Application Has Started Working in Ukraine: How to Notify the Armed Forces of Ukraine about a Missile or a Drone." Visit Ukraine, accessed March 10, 2023. 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.

Committee on Digital Transformation. "Закликаємо повідомляти про окупантів чи колаборантів у чатбот єВорог [We urge you to report occupiers or collaborators to the chatbot eVorog, - Committee on Digital Transformation]." Verkhovna Rada, accessed March 10, 2022. https://www.rada.gov.ua/news/news_kom/229367.html.

Ford, Matthew. "The Smartphone as Weapon. Part 3: Participative War, the Laws of Armed Conflict, and Genocide by Smartphone." Manuscript, April 20, 2022.

Horbyk, Roman. "'The War Phone': Mobile Communication on the Frontline in Eastern Ukraine." *Digital War* 3, no. 1 (2022): 9–24, https://doi.org/10.1057/s42984-022-00049-2.

Jerusalem Post Staff. "New App Lets Civilians Help Shoot Down Drones and Missiles in Ukraine." *Jerusalem Post*, October 17, 2022. https://www.jpost.com/international/article-719836.

Mchale, John. "Smartphones on the Battlefield." *Military Embedded Systems* (blog), December 5, 2012. https://militaryembedded.com/comms/communications/smartphones-the-battlefield.

Melzer, Nils, *Direct Participation in Hostilities under International Humanitarian Law*. Geneva: ICRC, 2009.

Merrin, William. *Digital War: A Critical Introduction*. London and New York: Routledge, 2019.

O'Loughlin, Ben. "Towards a Third Image of War: Post-Digital War." Digital War 1, no. 1 (2020): 123–30. https://doi.org/10.1057/s42984-020-00015-w.

Pleitgen, Fred Claudia Otto, and Ivana Kottasová. "'There Are Maniacs Who Enjoy Killing,' Russian Defector Says of His Former Unit Accused of War Crimes in Bucha." CNN, December 14, 2022. https://www.cnn.com/2022/12/13/europe/russian-defector-war-crimes-intl-cmd/index.html.

Roberts, Adam. "The Civilian in Modern War." In *The Changing Character of War*, edited by Hew Strachan and Sibylle Scheipers, 357-380. Oxford and New York: Oxford University Press, 2011.

Sabbagh, Dan. "Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks." *The Guardian*, October 29, 2022. https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo.

Sandoz, Yves, Swinarski, Christophe and Zimmermann, Bruno (eds), *Commentary on the Additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.* Geneva: ICRC, 1987.

Schmitt, Michael N. "Ukraine Symposium – Using Cellphones to Gather and Transmit Military Information." *Articles of War*, Lieber Institute, West Point, November 4, 2022. https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-post-script/.

Schmitt, Michael N. and William Casey Biggerstaff. "Ukraine Symposium – Are Civilians Reporting With Cell Phone Directly Participating in Hostilities." *Articles of War,* Lieber Institute, West Point, November 2, 2022. https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/.

U.S. Supreme Court. Kawakita v. United States, 343 U.S. 717 (1952). No. 570, Argued April 2-3, 1952, Decided June 2, 1952, 343 U.S. 717. https://supreme.justia.com/cases/federal/us/343/717/.

Pontus Winther is a doctor of international law and a reservist legal adviser to the Swedish Armed Forces. He wrote his doctoral thesis on the protection of civilians from unlawful communication influence activities during armed conflict. He does research on various legal aspects of cognitive warfare in grey zone and armed conflict.

Per-Erik Nilsson holds degrees in political science and sociology of religion. He works as a senior researcher at the Swedish Defence Research Agency and is Associate Professor at Uppsala University. His current works focuses on strategic communications, information warfare, and methodological development in social data theory.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl