AEL 2024/16
Academy of European Law
European Society of International Law Paper

WORKING PAPER

Civilian non-violent defence against Russian Warfare – Eastern European strategies and the gap between civilians and combatants in Customary IHL

Saskia Millmann and Pia Hüsch

European University Institute

Academy of European Law

European Society of International Law
Research Forum, Tartu, April 2023

Civilian non-violent defence against Russian Warfare – Eastern European strategies and the gap between civilians and combatants in Customary IHL

Saskia Millmann and Pia Hüsch

ISSN 1831-4066

Published in July 2024 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu

With the support of the Erasmus+ Programme of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Academy of European Law

The Academy of European Law coordinates several important research projects and offers advanced-level courses, including the annual summer courses in human rights law and the law of the EU, resulting in an extensive publications programme. The Academy also hosts the Secretariat of the European Society of International Law (ESIL), and assists in the organization of ESIL events.
Papers presented at ESIL events in 2011-2019 can be downloaded from SSRN. As of 2022, the papers are available in the EUI CADMUS Research Repository.

More information about the Academy of European Law

European Society of International Law

The European Society of International Law (ESIL) is a dynamic network of researchers, scholars and practitioners in the field of international law. The Society's goals are to encourage the study of international law, to foster inquiry, discussion and innovation in international law, and to promote a greater understanding of the role of international law in the world today. The Secretariat of the Society has been based at the Academy of European Law since 2004 when the Society was set up.

More information about ESIL

ESIL Paper Series

The ESIL Paper Series features papers presented at ESIL events (Annual Conferences, Research Forums, and Interest Groups events). Publication in the ESIL Paper Series enables authors to disseminate their work widely and reach broader audiences without the usual delays involved in more traditional means of publication. It does not prevent the subsequent publication of papers in academic journals or edited collections.

More information about the ESIL Paper Series

2023 ESIL Research Forum, Tartu, 27-28 April 2023

The ESIL Research Forum is a scholarly conference that promotes engagement with research in progress by early-career researchers, who have the opportunity to present their works and receive comments from members of the ESIL Board and invited experts during the Forum. The 2023 ESIL Research Forum was hosted by the University of Tartu on 27-28 April 2023 and addressed the topic "Regional Developments of International Law in Eastern Europe and Post-Soviet Eurasia".

More information about the 2023 ESIL Research Forum

EUI ACADEMY OF EUROPEAN LAW

esil sedi EUROPEAN SOCIETY OF INTERNATIONAL LAW

Abstract

Russia's war against Ukraine and the widespread documentation of civilian participation therein sheds new light on the role of civilians in national defence. This paper examines historic and contemporary Baltic and Ukrainian defence strategies against Russian and previous Soviet aggression and how national policies envisage and perhaps encourage civilians to engage in resistance and potentially in defence.
The focus rests on the role of civilians who are not employed or subcontracted by the military but engage in acts ranging from singing national anthems to launching offensive cyber operations. The paper examines when such civilian participation amounts to direct participation in hostilities and the types of legal implications which follow from such activities. This paper takes a closer look at recent civilian participation in hostilities as seen in Ukraine, particularly focusing on intelligence gathering and cyber activities as conducted by the Ukrainian information technology (IT) army to illustrate the risks to which civilians expose themselves.
This paper concludes that while there are legitimate reasons for States to include civilians in their defence strategies, it is key that where civilians engage in direct participation in hostilities, they must do so on an informed basis, setting out the legal implications of their actions. Where a State (passively) encourages such activities, it has at least a moral, if not also a legal obligation, to inform civilians of the risks of their actions.

Keywords

civilian defence - DPH - cyber - total defence - Baltics - Ukraine

Author Information

Dr Saskia Millmann is a Research Affiliate and Lecturer at the University of Glasgow as well as a Project Manager in cUAS at ESG a Hensoldt Company. Her research focusses on IHL/LoAC, legal history, and international organisations. Saskia completed her PhD in Law at the University of Glasgow. She also holds an LLM in International Law from the University of Edinburgh and a BA and MA (with distinction) in History and Law from the University of Munich.

Dr Pia Hüsch is a Research Fellow in cyber, technology and national security at the Royal United Services Institute (RUSI). Her research focusses on the impact, societal risks and lawfulness of cyber operations and the geopolitical and national security implications of disruptive technologies, such as AI. Pia holds a PhD in International Law as well as an LLM in International Law Security (with distinction) from the University of Glasgow and an LLB in European Law from Maastricht University.

Table of Contents

1. Introduction

While Russia's latest aggression against Ukraine was not its first attempt to wage territorial warfare against Ukraine or indeed other Eastern European states, the 2022 invasion is receiving a lot more international attention.[1] However, in contrast to their Western neighbours, Eastern European states were not surprised by the attack on Ukrainian sovereignty and territorial integrity – rather they had prepared strategies and warned for such an event to occur. What is of particular interest to the authors is how civilians are addressed in these strategies and how (if at all) customary IHL addresses civilian defence in an international armed conflict (IAC).

[1] See e.g., 'Russia's Aggression against Ukraine: Press Statement by High Representative/Vice-President Josep Borrell, 24 February 2022, at: Https://Www.Eeas.Europa.Eu/Eeas/Russias-Aggression-against-Ukraine-Press-Statement-High-Representativevice-President-Josep_en (14 October 2022)'.

Civilians have played an important role in both the Baltics and Ukraine in strategies against Russian and previously Soviet aggression. The Baltic countries – Estonia, Latvia, and Lithuania - in particular have had a lot of experience with civilian defence as an alternative to military defence in times of occupation. More recently, all three Baltic countries included civilians in their respective defence strategies, primarily in response to Russian geopolitical and military objectives. Ukraine, similarly, explicitly addresses civilians in its current defence strategy and civilians are most prominently used in hybrid warfare against Russia. The first part of this paper analyses the national defence strategies of the Baltic countries and how IHL can be applied to them. The second part will focus on Ukraine's civilian defence strategy before and after the Russian aggression. The in-depth analysis and application of its civilian defence strategy to IHL is limited to the IT army.

While civilians often supplement a military force, either as contractors or as civilian employees, this paper focusses yet on a different phenomenon.[2] The authors are interested in the participation of civilians who are not employed or subcontracted by the military. Conversely, this could mean the general public or specific groups of civilians, like IT-experts, who are included in defence strategies outside of conscription or employment of any sort. The Baltic countries and Ukraine have demonstrated how vital the inclusion of civilians can be both in times of occupation and during an active armed conflict. We are therefore exploring what lessons are to be learnt for future (Western) defence strategies, and what possible implications for the application of IHL follow.

a. Civilian non-violent defence: A preliminary definition

Unlike traditional military defence, civilian defence relies on the participation of ordinary citizens to resist and undermine an aggressor's ability to exercise control. In the event of an on-going occupation, civilian defence strategies, at their core, aim to protect social values and social structure of the society.[3] Yet, it remains unclear how civilian defence can look like in the context of deterrence, or in an active IAC. Looking at Geneva Convention IV for guidance, one realises that Art. 63 also only applies to occupation and furthermore only addresses relief efforts of either relief societies following the Red Cross principles, or other special organisations of a non-military character whose aim is to ensure living conditions of the civilian population, the maintenance of essential public utilities and organising relief and rescues.[4]

While Chapter VI of AP I (Art. 61-67) defines and addresses civil defence in an active IAC, its scope is also limited to traditional relief and rescue efforts, not addressing actions to safeguard

[2] Novikovas et al. point out that e.g. the US government identify civilian contractors as part of the military's 'total force' whilst still classifying them as civilians. Andrejus Novikovas and others, 'THE PECULIARITIES OF MOTIVATION AND ORGANIZATION OF CIVIL DEFENCE SERVICE IN LITHUANIA AND UKRAINE' (2017) 7 Journal of Security and Sustainability Issues 371.

[3] Anika Binnendijk and Marta Kepe, *Civilian-Based Resistance in the Baltic States: Historical Precedents and Current Capabilities* (RAND 2021) xi–xii.

[4] Art. 63 Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287; Art. 61-67 also address traditional relief and rescue work 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, 1125 UNTS 3.

values, or inhibiting the aggressor through passive means.[5] What also remains out of scope of both the Geneva Convention and AP I are actions not undertaken by an organisation in the broadest sense. Individuals or groups of civilians who are not part of an organisational structure are therefore not included in this definition. Therefore, one needs to ask the question what activities conducted by civilians which are not mentioned in either the Geneva Convention or AP I still qualify as permissible civilian actions? Civil defence organisations are not, under any circumstances, allowed to conduct activities that are harmful to the enemy – they would lose their special protection under Art. 62.[6] Given that individuals or groups who are not part of such an organisation are not entitled to this special protection anyway, the only possible outcome could be, that they are either considered to engage in unlawful behaviour, or lose their status as civilian altogether.

Further investigating the role of civilian defence in different scenarios is consequently vital to appropriately situate them in IHL. Recently, owing to the emergence of hybrid warfare, some civilian defence strategists propose "deterrence through both denial and offense" including civilians in these efforts short of using force.[7] Indeed, contemporary strategies are different to previous examples: they are intended to be used in an on-going IAC and arguably aim to achieve more than securing societal values. Therefore, one needs to investigate if such actions have the potential of becoming offensive in nature, crossing the threshold to DPH.

b. Goals/research question

The authors aim to take a closer look at the concept of civilian defence and how it is used both in a preparatory or perhaps deterrent way, as well as in an ongoing international armed conflict. In doing so, they first explore historical examples of civilian defence as well as current defence strategies in the Baltics on the one hand, and the current usage of civilian defence in Ukraine on the other.

What is of particular interest to the authors is how civilians are addressed in these strategies and how (if at all) customary IHL addresses civilian defence in an IAC. When do civilians cross the threshold of direct participation in hostilities (DPH)? Can this threshold be met through non-violent civilian action? How can cyber operations conducted by civilians during an IAC be assessed? Are Baltic and Ukrainian civilian defence strategies the next logical step in (hybrid) warfare?

2. Civil Defence Under IHL

While IHL does not prohibit civil defence – or even civilian direct participation – per se, civilians' actions may nevertheless carry consequences under humanitarian law. Civilians are normally protected from direct attack under the principle of distinction, which requires all parties to the

[5] 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, 1125 UNTS 3.
[6] Art. 65 (1) ibid.
[7] TX Hammes, 'Atlantic Council, "Baltic Porcupine: Harnessing the Fourth Industrial Revolution to Defend the Baltic States," Event Recap, July 11, 2019;' (16 April 2022) <https://www.atlanticcouncil.org/commentary/event-recap/baltic-porcupine-harnessing-the-fourth-industrial-revolution-to-defend-the-baltic-states/>.

conflict to always distinguish between combatants and civilians, and to only use direct attacks against combatants or military targets.[8] Except in the case of a *levée en masse*, individuals who do not belong to organised armed forces but engage in hostilities sporadically, spontaneously, or in an unorganised manner remain civilians under IHL.

The principle of distinction, however, temporarily ceases to apply to civilians for the time they are engaging in direct participation in hostilities (DPH) – a concept which is not defined in treaty law nor clearly defined in customary international law. AP I provides a starting point, stating that a civil defence organisation loses its protected status if it engages in activities that are harmful to the enemy.[9] The ICRC's guidance identifies that DPH is comprised of two elements, hostilities, and direct participation.[10]

For an act to qualify as DPH, it must meet three cumulative criteria: it must meet a threshold of harm, there must be a direct causal link between the act and such harm, and the act must be designed to support one party to the conflict to the detriment of the other (belligerent nexus).[11]

According to the ICRC's guidelines, the threshold of likely harm, generally must be similar to that of military force. While killing and wounding individuals or inflicting structural or functional damage to military objects is an obvious similarity to military force, one must also consider that even non-violent sabotage has the potential to adversely affect the enemy and cause harm. Examples thereof could be disturbing logistics and communications through cyber-attacks against the military computer network of the enemy.[12] Determining whether an act has 'adverse military effect' requires having enough information on the act itself and likely outcomes. Moreover, there must be a causal link between the (likely) outcome of the act and the harm. Acts merely building up capacity to cause such an effect, like engaging in propaganda, repairing roads, or even manufacturing and shipping weapons would not satisfy the causal link.[13] Lastly, the belligerent nexus and intent of the act must be 'specifically designed to do so in support of a party to an armed conflict and to the detriment of another'.[14]

---

[8] Art. 50 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, 1125 UNTS 3; Similarily, in Blaskic, the ICTY defined civilians as: 'persons who are not, or no longer, members of the armed forces' *Prosecutor v Tihomir Blaskic (Trial Judgement), IT-95-14-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 3 March 2000* 180.

[9] See Art. 65 (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, 1125 UNTS 3.

[10] Nils Melzer, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' 43 <https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf>.

[11] ibid 46.

[12] 'Third Expert Meeting on the Notion of Direct Participation in Hostilities, Geneva, 23 – 25 October 2005 (Summary Report)' 11, 29–31 <https://www.icrc.org/en/doc/assets/files/other/2005-09-report-dph-2005-icrc.pdf>.

[13] ibid 21, 27–34.

[14] *Prosecutor v Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic (Appeal Judgment), IT-96-23 & IT-96-23/1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 12 June 2002* 58; *Georges Anderson Nderubumwe Rutaganda v The Prosecutor (Appeal Judgement), ICTR-96-3-A, International Criminal Tribunal for Rwanda (ICTR), 26 May 2003* 570; Melzer (n 10) 59; 'Third Expert Meeting on the Notion of Direct Participation in Hostilities, Geneva, 23 – 25 October 2005 (Summary Report)' (n 12) 25.

If one agrees to accept the ICRC's three requirements and a civilian has indeed satisfied them, the civilian loses their protection from direct attack 'for such a time as they take a direct part in hostilities'.[15] Civilians engaging in DPH are not entitled to immunity from domestic prosecution,[16] but may be subject to criminal charges. As it is to this date the most established way to determine whether a civilian is partaking in DPH, this paper relies on the ICRC's interpretation to assess whether actions of civilian defence or resistance mean the individuals in question lose their protection from direct attack. Having said that, in practice it is often challenging to operationalise the application of such thresholds: it seems unlikely that a member of enemy armed forces would undertake an in-depth analysis of whether a civilian fulfils all of these criteria, particularly where the factual assessment is challenging to conduct at speed. Moreover, civilians engaging in these activitites need to take into account the possibility that the enemy power entirely disregards the *jus in bello* and targets civilians irrespective of whether they engage in DPH or not. We can see this behaviour, e.g. in the Russian armed forces and the Wagner group in Ukraine. However, the authors still feel it is important to identify what the law says and how it can be applied – not least because a violation of the law might constitute a war crime that can be prosecuted at the national or potentiall international level.

3. Using civilian defence as a strategy primarily against Russia – past and present approaches

To examine how states address civilians in their defence strategies, the authors focus on the Baltic States and Ukraine, which have a long history of being targeted by Russian attacks. Analysing their individual and collective defence strategies can provide valuable insights in how to use civilian defence against Russia's hegemonial threat, destabilisation attempts, and even aggression.

a. Estonia, Latvia and Lithuania – a long history of successfully using civil defence

The Baltic countries suffered Russian aggression and occupation from 1940 to 1941 and again from 1944-1991.[17] During the Soviet occupation and some would argue annexation,[18] the population of the Baltic countries were subjected to mass deportations, forced collectivisation, and other forms of oppression.[19] Despite these atrocities, non-violent resistance in the civilian population across all three Baltic countries prevailed, leading to ordinary citizens organising alternative election lists, tearing down Soviet symbols and flags, or displaying national symbols

[15] Art. 51 (3) 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, 1125 UNTS 3.

[16] Art. 43 (2). However, one should also note that IHL does not prohibit civilians to directly participate in hostilities. It merely removes their protection if they do, and also does not grant them imunity from domestic prosecution. ibid.

[17] Soviet occupation was only briefly interrupted by the occupation of Nazi-Germany from 1941-1944.

[18] Mälksoo offers a thorough and highly informative analysis on the illegal annexation of the Baltic republics and the necessary consequence of state continuity. Lauri Mälksoo, *Illegal Annexation and State Continuity: The Case of the Incorporation of the Baltic States by the USSR. Second Revised Edition* (Brill | Nijhoff 2022).

[19] See Alain Blum and Emilia Koustova, 'A Soviet Story: Mass Deportation, Isolation, Return', *Narratives of Exile and Identity* (Central European University Press 2018).

or signing national songs prohibited by the Soviets.[20] Thereby, the Baltic population preserved their own respective identities, keeping spirits high and making it as unpleasant and costly as possible for the occupying force, without using armed force.[21] All of these civilian efforts, growing in scale over time and using the economic and political crises in the USSR, mounted in a strong, public independence movement across all three countries. Lithuania ultimately declared independence on 11 March 1990, Latvia on 4 May 1990, and Estonia on 21 August 1991. Ultimately, the Soviet government recognised the independence of all three states on 6 September 1991.[22]

In the more recent history, Estonia, Latvia, and Lithuania have been subject to Russian strategic information operations and were met with Russian forces deploying close to their borders. Especially after the Russian annexation of the Ukrainian peninsula Crimea in 2014, many wondered if the Baltic countries would be next.[23]
Consequently, they have jointly – and separately – formulated strategies to deter Russian aggression and revisionist agenda.[24] Notably, these strategies explicitly include civilians. It is of particular interest to the authors how exactly civilians are addressed in particular in situations outside of foreign occupation, i.e., in defensive manoeuvres against an on-going aggressive attack from an enemy state. Based on the previously discussed history, and the permanent Russian threat, two defensive concepts that also include civilians have been integrated in the national defence strategies of the three countries: total defence and unconventional warfare.[25]

[20] Stephen Zunes, 'Estonia's Singing Revolution (1986-1991)' (*International Center on Nonviolent Conflict (ICNC)*) <https://www.nonviolent-conflict.org/estonias-singing-revolution-1986-1991/>; One particularly notable civilian effort was the Baltic Way which took place on 23 August 1989 where 2 million people joined their hands to form a human chain, connecting all three Baltic capitals. Baltic Defence College, 'Restoration of Independence in the Baltics' <https://www.baltdefcol.org/1243>.

[21] Binnendijk and Kepe (n 3) 36 Nevertheless, it should be mentioned that there also was violent resistance, both against the Soviet, as well as the German occupation. An example would be the Forest brothers.

[22] See for a more comprehensive appraisal: Grazina Miniotaite, 'Lithuania: From Non-Violent Liberation Towards Non-Violent Defence?' (1996) 28 Peace Research 19, 22; Baltic Defence College (n 20); Audrone Petrauskaite, 'Nonviolent Civil Resistance against Military Force: The Experience of Lithuania in 1991' (2021) 34 Security and Defence Quarterly 38; Maciej Bartkowski, 'Nonviolent Civilian Defense to Counter Russian Hybrid Warfare' [2015] John Hopkins University, Center for Advanced Governmental Studies 6, 13.

[23] Andres Kasekamp, 'Are the Baltic States next? Estonia, Latvia, and Lithuania' in Ann-Sofie Dahl (ed), *Strategic challenges in the Baltic Sea region: Russia, deterrence, and reassurance* (Georgetown University Press 2018) 62.

[24] Stephen J Flanagan, Jan Osburg and Marta Kepe, 'Deterring Russian Aggression in the Baltic States through Resilience and Resistance' Rand Corporation Research Report <https://apps.dtic.mil/sti/pdfs/AD1086498.pdf>.

[25] What total defence means in practice for each Baltic Republic will be discussed below. The concept of total defence has been included in Estonia's 2010 National Security Concept. It has also been used by Latvia and Lithuania in 2016 and 2017 respectively. Other nations that use total defence as part of their strategy are, e.g. Finland, Norway, and Sweden. 'National Security Concept of Estonia 2010 (Unofficial Translation)' <https://eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf>.

i) Estonia

Estonia's National Defence Concept between 1993 and 2010 focussed on total defence as well as territorial defence – prioritising a traditional military approach.[26] While Estonia had a history of civil disobedience which included asking its citizens to refuse any actions that would be breaking Estonian laws, strictly non-cooperate with the Soviets, and document any activities of the Soviet forces, civilian defence did not play a role after regaining independence.[27] However, there is the *Kaitseliit* (Defence League) which is a militarily organised voluntary defence organisation. Its roots go back to guerrilla groups who fought against the Nazis and Soviets.[28]

Having become a victim of massive hybrid attacks in 2007, the Estonians acknowledged that due to changing potential threats, especially such hybrid challenges, military means alone would not be enough to meet the new defence demands. This realisation was also reflected in the 2011 defence strategy which amended its previous total defence approach to an integrated defence and comprehensive security approach, listing civilian support to military defence as one of the six pillars of this new strategy.[29]

Estonia affirmed and updated its 2010 National Defence Strategy in 2017, branding it 'integrated defence and comprehensive security'.[30] This new approach consists of six pillars, one of which is civilian support to military defence, relying e.g., on the *Kaiseliit*.[31] In the event of an armed conflict, the Kaitseliit will split. The military wing will operate under the Estonian armed forces whilst the civilian wing will engage in non-violent defence. Whereas members of the military wing would be classified as ordinary combatants, members of the civil wing would remain civilians and would not be legitimate targets as long as they do not take part in DPH. Whether an enemy soldier would understand and recognise this distinction might, however, be a different question.

Estonia's 2017 defence concept vastly expanded a reference to civilian contribution to defence.[32] It acknowledges that networks of civilian volunteers play an important role,[33] and includes civilian contribution in psychological defence.[34] Such measures seem rather close to

---

[26] Flanagan, Osburg and Kepe (n 24) 7.

[27] Bartkowski (n 22) 14; This only shifted in 2014, which will be discussed in section 4. See for a detailed analysis on Estonian capabilities to include civilian defence at that time: Margus Kuul, 'Civil Resistance: An Essential Element of a Total Defense Strategy' (Naval Postgraduate School, Monterey California 2014) 101 et seq.

[28] Flanagan, Osburg and Kepe (n 24) 8.

[29] 'National Security Concept of Estonia 2010 (Unofficial Translation)' (n 25).

[30] ibid.

[31] 'National Security Concept of Estonia 2017' 3 <https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf>.

[32] In 2010 the only reference to civilians was the aim for civilian resilience and social cohesion. At 3.3: 'Social cohesion is enhanced and social risks prevented through higher employment rate and greater involvement in social life. The prevention of social risks is addressed in the national economic and social policy.' ibid 15.

[33] ibid 6.

[34] ibid 20.

previously successful Baltic attempts at civilian defence and would likely not cross the threshold to DPH as these are non-violent actions directed inwards.

ii) Latvia

Similarly, Latvia initially encouraged its citizens to non-violent resistance. Latvian total non-cooperation was part of the Latvian Popular Front strategy in 1990. They called on all citizens to 'to ignore the attackers' orders, not to participate in any elections or referendums, and to document all crimes perpetrated by the attackers'.[35] Civil defence was intended to be a constant supplement of military defence. Alas, civilian defence did not find its way into Latvia's defence strategy after regaining independence. The *Zemessardze* (National Guard) is a militarily organised unconventional defence group whose main task is to support the regular land forces units. While it is also responsible for civilian crisis management, the organisation cannot reasonably be considered part of non-violent civilian defence.[36]
Latvia's 2016 edition of its National Defence Concept outlines a duty for its civilian administrations (state, regional, and local) to coordinate 'the readiness and actions undertaken by individual and legal entities during times of peace, threats and war'[37] to support national defence, and to implement national defence measures. For the first time since regaining independence, the defence concept hints at the fact that civilians also could have a role during armed conflict: 'The state informs society on what actions should civilians undertake during a military conflict'.[38] While this is a rather vague statement, it would be reasonable to assume that the state would give similar advice to previous strategies, i.e. total non-cooperation, classical peaceful civilian defence methods. A recently published brochure titled 'what to do in case of crisis' gives citizens some suggestions how they could support national defence: join the National Forces, report any movement, actions, or marks and transmitters of the aggressor, offer practical support to National Forces and NATO, help build fortified structures, use deception (take off road signs), help salvage peace and help motivate your colleagues, family members and friends to support national defence, support your company's continuity planning, create a local Unit of National Guard.[39] While some of these suggestions are certainly below the threshold of DPH, some might, depending on circumstances, cross the line.

iii) Lithuania

As early as 1991, shortly after regaining independence, the Lithuanian Supreme Council adopted a resolution, reminding its citizens to continue to follow the principles of disobedience, non-violent resistance, and non-cooperation in their struggle for independence.[40] Having developed the concept further, Lithuania refers to civilians in its defence and security strategies

[35] As cited in: Bartkowski (n 22) 14.
[36] Flanagan, Osburg and Kepe (n 24) 10.
[37] See introduction para 3 Ministry of Defence Republic of Latvia, 'The National Defence Concept 2016' <https://www.mod.gov.lv/sites/mod/files/document/Valsts_aizsardzibas_koncepcija_EN.pdf>.
[38] 3.1.1 (29) ibid.
[39] Ministry of Defence Republic of Latvia, 'What to Do in Case of Crisis' 11 <https://www.sargs.lv/lv/brochure-what-to-do-in-case-of-crisis>.
[40] Bartkowski (n 22) 13–14.

since 1992.[41] Since this time, Lithuania relied on the participation of civilians in its defence strategy: 'State defence consists of military security, as well as civil resistance.'[42]

Lithuanian citizens are by law asked to engage in (not further defined) non-violent resistance, disobedience and non-collaboration, as well as armed resistance.[43] To help its citizens fulfil these duties, Lithuania has established a Civilian Resistance Training Centre at the Ministry of National Defence in 2000 – next to preparing civilians, its goal is also to act as a deterrent for any potential aggressor.[44] However, a further noteworthy shift in strategy occurred once Lithuania joined NATO in 2004. Now, protected under Art. 5 and geared towards collective security, civilian defence seemed to have been on the backburner for some time after.[45]

More recently, the Lithuanian Ministry of Defence updated its strategy regarding Russian hybrid warfare.[46] In May 2022 Minister of Defence, Arvydas Anušauskas, stated: "With the Strategy in place, we will begin a consistent and comprehensive education of the public on civil resistance. Such preparations will rest on three components: civil resilience, will to resist, and practical skills in both, armed and civil resistance. We aim to build on each of these. Another important aspect is that the preparation for civil resistance will cross over into the National Defence System area of expertise."[47]

Even more recently, in April 2023 a *Seimas* Committee started preparing to advise citizens how the strategy of civil resistance evolved since Russia's attack against Ukraine and how it should be implemented in the future. Lithuania plans for both unarmed and armed civil resistance, it educates school children and adults alike, and ultimately plans to raise the share to civilians willing to undertake non-armed violence to 70%.[48] Having briefly analysed Lithuania's updated approach, it becomes apparent that it has updated and upgraded its

---

[41] Gražina Miniotaitė, 'Civilian Resistance in the Security and Defense System of Lithuania: History and Prospects' (2004) 2 Lithuanian Annual Strategic Review 223, 234; LR Seimas (1996) Nacionalinio saugumo pagrindų įstatymas Nr. VIII-49 [The Law of National Security of the Republic of Lithuania. No VIII-49]. Available at: https://e-seimas.lrs.lt/portal (Accessed: 21 July 2020). For later inclusions see, e.g.:; Republic of Lithuania, 'National Security Strategy Lithuania 2002' <https://www.files.ethz.ch/isn/156885/LithuaniaNationalSecurity-2002.pdf>; Petrauskaite (n 22) As Petrauskaite points out, the strategy refers to non-military ways of resisting aggression.

[42] at 5.2.3.2 Republic of Lithuania (n 41); See also 34.8 'Seimas of the Republic of Lithuania Resolution Amending Resolution No IX-907 of the Seimas of the Republic of Lithuania of 28 May 2002 on the Approval of the National Security Strategy' <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3ec6a2027a9a11ecb2fe9975f8a9e52e?jfwid=rivwzvpvg>.

[43] 'Lietuvos respublikos nacionalinio saugumo pagrindu istatymas,' Valstybes zinios, 1997, No. 2, pp. 2-20 (Law on the Basics of National Security of Lithuania). As cited in: Miniotaitė (n 41) 234.

[44] Training at the Centre is not mandatory, it does therefore not cover the entirety of Lithuania's population. ibid 235.

[45] See Gražina Miniotaitė, 'Lithuania's Evolving Security and Defence Policy: Problems and Prospects' [2007] Lithuanian Annual Strategic Review 177.

[46] See Bartkowski (n 22).

[47] 'Seimas Approves Civil Resistance Readiness Strategy (Ministry of National Defence, Republic of Lithuania), 17 May 2022, at: Https://Kam.Lt/En/Seimas-Approves-Civil-Resistance-Readiness-Strategy/ (14 October 2022)'.

[48] Ministry of National Defence Republic of Lithuania, 'The Seimas Committee Will Explain How the Strategy of Civil Resistance Is Implemented (Ministry of National Defence, Republic of Lithuania), 12 April 2023' <https://kam.lt/en/seimas-approves-civil-resistance-readiness-strategy/>.

capacity for civilian defence. The choice whether to engage in armed or unarmed resistance would be up to citizens – however Lithuania's strategy does not necessarily demand a distinction and could therefore very likely mean that civilians will cross the threshold to DPH in some situations.

b. Impact of national strategies on IHL

After examining the national defence strategies of the Baltic countries, a fundamental question arises: do these strategies align with existing IHL, or do they represent a development of new, (possibly regional), customary international law? To address this, we must explore whether any of the acts outlined in the strategies of the Baltic states potentially violate IHL. As previously analysed in section 2, for any act to qualify as DPH, it must meet three cumulative criteria: it must meet a threshold of harm, there must be a direct causal link between the act and such harm, and the act must be designed to support one party to the conflict to the detriment of the other (belligerent nexus).[49] This threshold can only be met by violent actions – Estonian's duty to engage in psychological warfare, refusing to follow orders from enemy soldiers would not meet such a threshold. Likewise, engaging in other non-violent acts such as building fortifeit structures or removing road signs cannot be classified as DPH. Therefore, if it does not 'even' meet the threshold of DPH, how could it violate established IHL?

How would the law then be applicable to violent defensive action, particularly such action that does indeed qualify as DPH? As mentioned previously, civilians are not prohibited from using force or otherwise partaking in hostilities; rather, the legal consequence of such behaviour is losing the status of a civilian.[50] Hence, the principle of distinction no longer applies to them, and they become legitimate targets. Moreover, as they do not qualify for combatant privileges, they potentially could be prosecuted for any violations of domestic criminal law, e.g., murder or destruction of property. These consequences are clearly laid out in IHL; one could, therefore, not argue that they are a violation. Yet, it should be noted that the spirit of the Geneva Convention very much reflects a strict separation of civilians and combatants.[51] Civilians can only be protected if this separation is adhered to. Any gray-area situation might very well result in the targeting of the civilian in question. While a possible defense to that argument is a reference to the Lotus case and the long-standing principle that everything, in international law, that is not prohibited is allowed,[52] the authors would like to pose the question of whether it is necessary to encourage violent civilian defense, knowing the potential consequences. One would hope that states feel a higher moral obligation to safeguard their civilian citizens than to argue they are allowed to engage in such action because it is not prohibited. At the very least, states should take said responsibility seriously and inform their citizens of potential consequences which enables each and everyone to make an informed choice.

[49] Melzer (n 10) 46.
[50] See Art. 50 and 65 (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, 1125 UNTS 3.
[51] See preamble ibid.
[52] *SS 'Lotus' (France v Turkey)* (1927) Series A, no 10 (PCIJ).

To summarise, neither non-violent nor violent civilian defence constitutes a violation of IHL. While both forms can be read in conjunction with existing IHL, the authors argue that violent civilian defence certainly goes against the spirit and purpose of the Geneva Conventions.[53]

c. Ukraine's civil defence before and after Russia's attack(s)

Ukraine's defence strategy before the war was primarily regulated by the Law 'On fundamentals of National Security of Ukraine' which was passed in 2003. While this law does not address civil defence in the way the Baltic Republics have, it does mention the civil service and its role in Ukraine's defence. However, the role of civil servants in Ukraine's defence service was defined as supplemental to the military service. This means, civilians were used, e.g., on a fixed-term contract basis in a specialist function. Their role was to fill positions and provide expertise that the military itself did not have, or to free up the military's capacity to focus on their original duty: combat and defence.[54]

Since Russia's invasion on 24 February 2022, the Ukrainian population had to endure unspeakable things: mass destruction of cities, atrocities, even including the abduction of children. Not to speak of the experiences of Ukrainian soldiers who are subject to atrocity crimes. However, for the purpose of this paper, the authors would like to take a closer look at civilians. How does the civilian population engage in defensive actions – be it a defence of democratic values and the protection of Ukrainian identity, or actions more geared towards restoring territorial integrity. Understandably, as this is still an on-going conflict, information is hard to come by. No one on the ground has, for good reason, shared anything that could potentially be of use to the Russians, hence whatever we can analyse here will remain on the surface.[55] The following sections will, nevertheless, attempt to situate different examples of known Ukrainian civilian defence actions in IHL (if applicable).

i) Conventional means of Civilian resistance

Particularly in the beginning of the Russian invasion of Ukraine 2022, media coverage was astonished by the bravery of resistance of Ukrainian civilians facing their occupiers. Videos and photos of unarmed civilians in Ukraine emerged and were shared widely, documenting how inhabitants of attacked villages and towns greeted their invaders: with protests, by singing

[53] Kellenberger pointed out that the increasingly blurred lines between civilians and combatants lead to more civilians being killed: both mistakenly and arbitrarily. 'Sixty Years of the Geneva Conventions: Learning from the Past to Better Face the Future. Ceremony to Celebrate the 60th Anniversary of the Geneva Conventions. Address by Jakob Kellenberger, President of the ICRC, Geneva, 12 August 2009.' <https://www.icrc.org/en/doc/resources/documents/statement/geneva-conventions-statement-president-120809.htm> accessed 29 September 2023.

[54] Novikovas and others (n 2) 376 et seq See also: Law of Ukraine "On the Fundamentals of National Security of Ukraine", 2003. Bulletin of the Verkhovna Rada of Ukraine, № 39, as cited in Novikovas, p. 376.

[55] Juurvee points this out and underlines that he and his team deliberately did not include certain information. This includes information that would have opened Ukrainian civilians to potential conflicts with law enforcement. Ivo Juurvee, 'Civil Defence in Ukraine. Preliminary Lessons from the First Months of War, November 2022' 1 <https://icds.ee/wp-content/uploads/dlm_uploads/2022/11/ICDS_Analysis_Civil_Defence_During_the_War_in_Ukraine_Ivo_Juurvee_November_2022.pdf>.

the Ukrainian national anthem, with road blockades, by stopping moving vehicles from further progressing.[56]

For example, in the city of Berdyansk, civilians protested against Russian soldiers occupying the city.[57] Civilians have also blocked the road access to Zaporizhzhia, the Ukrainian nuclear powerplant now in control of Russian forces.[58] Other video material shows how civilians actively stopped moving vehicles from progressing en route.[59] The bravery of unarmed civilians facing their occupiers is exemplary, but do their activities meet relevant thresholds to alter their status of protection under international humanitarian law?

Civil resistance, e.g. in form of protests or singing the national anthem, do not amount to DPH. Clearly, these activities do not fulfil the necessary harm threshold. Nor is this the case where civilians merely refuse to collaborate with invading or occupying forces.[60] Where civilians join war-sustaining efforts, e.g. by producing camouflage nets or even making Molotov cocktails, they also do not fulfil the requirements of DPH, as these wider activities lack the direct causation to the hostilities.[61] Constructing road blockades only constitutes DPH where these blockades result in an adverse impact on the military operations or military capacity of a party to the conflict: where no such effect is given and the activity in question is also not likely to cause death, injury, or destruction, building a road blockade would not meet the necessary harm threshold to speak of DPH.[62] Civilians thus have a range of options to take up activities that support the defence of their state and that constitute war-sustaining efforts without losing their civilian protection from direct attack.

Is this still the case though where civilian resort to more drastic measures? How about inhabitants who pick up arms and use force and violence to defend themselves against their occupiers? Their exact status depends on the circumstances under which they resort to the use of force. Firstly, where civilians engage in violent civil unrest against occupying forces, such activities would likely not amount to DPH as they are missing the belligerent nexus that is necessary for such activity to qualify as DPH.[63] Instead, they would fall under the regular

[56] Deutsche Welle News, ‚Russia's military faces various forms of civilian resistance in Ukraine', 1 March 2022, https://www.youtube.com/watch?v=_RiaCgwAh04; Deutsche Welle News, 'Footage shows how citizens try to stall Russian forces all over Ukraine', 4 March 2022 https://www.youtube.com/watch?v=UZhl9UnTXSc; Guardian News, 'Ukrainian protesters unmoved as Russian forces fire bullets and stun grenades overhead', 27 March 2022, https://www.youtube.com/watch?v=hX2BLtETyGE.

[57] Shaun Walker and Isobel Koshiw, ''We're living a nightmare': life in Russian occupied Ukraine', 14 March 2022, *The Guardian*, https://www.theguardian.com/world/2022/mar/14/were-living-a-nightmare-life-in-russian-occupied-southern-ukraine.

[58] Sarah Cahlan, 'Drone footage shows citizens block Russian troops in Enerhodar, home to Zaporizhzhia nuclear plant', 3 March 2022, *The Washington Post*, https://www.washingtonpost.com/world/2022/03/03/zaporizhzhia-nuclear-plant-blockade-drone-video/.

[59] GuardianNews,'Unarmed Ukrainian try to push back Russian troops', 1 March 2022, https://www.youtube.com/watch?v=ev0x9pqYqvs.

[60] Melzer (43), p. 49.

[61] Nils Melzer, 'Civilian Participation in Armed Conflict', *Max Planck Encyclopedia of Public International Law*, 2010, §16.

[62] Melzer (43), p. 50.

[63] Melzer (77), §9.

law enforcement paradigm.[64] Where civilians, in an unoccupied territory, spontaneously use force to resist invading forces, carry their arms openly, adhere to IHL and wear a distinctive emblem, they might qualify as participants in a *levée en masse*. As a result, they enjoy combatant privilege and prisoner of war status.[65] However, this requires a level of spontaneity that is not always given.

Shortly before the Russian invasion, Ukraine had passed new legislation in January 2022 that legitimises *ad hoc* resistance, e.g. when civilians join the territorial defence forces (TDF), and which incorporates these groups into its military command structure.[66] They have been distributed weapons and they wear a distinctive emblem, a yellow taped band around their arm.[67] In these instances, those who are fighting would be part of a command structure and likely wear a distinctive emblem. If they also carry their weapons openly and conduct their operations in line with IHL, they could qualify as a volunteer group which is part of armed forces and therefore enjoys prisoner of war status when captured.[68] However, with this level of organisation, they would no longer be qualify as participating in a *levée en masse*.

Civilians who do not join organised volunteer groups and individuals who are not members of a *levée en masse* but are also directly participating in hostilities, lose their civilian protection for the duration of their activities when such activities are likely to inflict death, injury or destruction or their activities are integral to a military operation (see section 2). Examples here would include acts of sabotage or using delayed or remote weapons, including booby traps, missiles or mines but also drones.[69]

While these examples of activities potentially amounting to DPH are not new – after all, these are examples of civilians reacting to or participating in conventional warfare – and established rules of IHL apply to them, the wide availability of video and photographic footage recording these activities bring them closer to those outside the war zone. One still relatively new way in which civilians can participate in hostilities is through cyber means, which will be examined more closely in section 4.

ii) Intelligence gathering by civilians

In any armed conflict, information is key: information about road conditions, the enemy's location, the equipment used or the enemy's morale are only few of the examples a party may want to collect data on. To do so, it needs information or intelligence, typically obtained through a number of sources, including professional intelligence agencies but also informants in the civilian population.

---

[64] *ibid*.
[65] Art. 4(a)(6) GC III.
[66] Interfax Ukraine, ‚Law on foundations of national resistance enters info force in Ukraine', 1 January 2022, https://en.interfax.com.ua/news/general/789443.html; Kim Bubello and Chad de Guzman, ''We are fighting for Survival.' The Ukrainian Vitizens Volunteering to Defend their Country from Russian Troops', 3 March 2022, *Time*, https://time.com/6154068/ukrainian-citizens-fight-russian-troops/.
[67] Bubello and Guzman.
[68] Art. 4(a)(2) GC III.
[69] Melzer (77), §17.

In Ukraine, for example, civilians have been sending intelligence information, especially via telegram chats or via the Ukrainian government app Diia that allows users to "report the movements of Russian troops, sending location-tagged videos directly to Ukrainian intelligence", reportedly receiving tens of thousands submissions a day.[70] The intelligence gathering effort benefits from a wide availability of smart phones that can record sound and photographic material that can be passed on quickly. A Ukrainian intelligence official confirmed in news reports that the local population is "supportive" but did not want to expand on the details of the activities conducted by civilians.[71] Relying on public reporting makes the following examples of information gathering by individuals anecdotal reference rather than confirmed activities, but they raise a range of interesting questions about civilians gathering intelligence in support of Ukrainian forces: Who organises this? Where do civilians report to? What is the information used for? Do civilians know what their information is used for? And finally, does intelligence gathering by civilians amount to DPH?

Intelligence gathering would amount to DPH and meet the relevant harm threshold and meets the direct causal link criterion if it forms an integral part of a military operation to the adverse affect of a party to the conflict, e.g. because it is considered a preparatory act for a specific hostile act.[72] For example, it has been reported that one informant passed on information obtained by a farmer who had identified the position of a Russian missile launcher – which was replaced by a hole in the ground the next day.[73] While difficult to confirm, it would seem that the relevant information here was used to provide targeting coordinates and therefore was an integral part of a specific military operation. Similarly, Ukrainian informant "Dollar", a civilian who had been providing targeting coordinates and other information on Russian operations, provided information on a hotel hosting Russian officers to his handler at the Security Service of Ukraine, with the hotel later being bombed.[74] A further example of civilian involvement stems from U.S. officials who noted that an underground of intelligence informants helped lead to Russia's withdrawal from Kherson – providing little insight on information structure and in how far information was used for distinct military operations. In contrast, Reuters reports on an interview with a former policeman who has been gathering intelligence on collaborators, leading to criminal investigations.[75] Such general information gathering, or the reporting of information on potential war crimes,[76] would not be considered DPH given that there is no direct causal link, the belligerent nexus is missing and the intelligence obtained does not form integral part of a military operation.

[70] Drew Harwell, 'Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War', 24 March 2022, The Washington Post, https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/.
[71] Jonathan Landay and Tom Balmforth, 'How a band of Ukraine ciivilians helped seal Russia's biggest defeat', Reuters, 9 February 2023, https://www.reuters.com/world/europe/how-band-ukraine-civilians-helped-seal-russias-biggest-defeat-2023-02-09/.
[72] Melzer (43), p. 180.
[73] Landay and Balmforth.
[74] Jonathan Landay and Tom Balmforth, 'How a band of Ukraine ciivilians helped seal Russia's biggest defeat', Reuters, 9 February 2023, https://www.reuters.com/world/europe/how-band-ukraine-civilians-helped-seal-russias-biggest-defeat-2023-02-09/.
[75] Landay and Balmforth.
[76] This can be done via this government website: https://warcrimes.gov.ua.

The value of civilian intelligence gathering is clear: a wide net of undercover informants, who with the help of smart phones can quickly communicate essential information, is critical to the war effort. The Ukrainian Defence Minister has reportedly even awarded decorations to civilian informants for cooperation with the armed forces.[77] However, again it must be noted that it is pivotal that civilians understand the risks and consequences of their activities, including under international humanitarian law, and can therefore come to an informed decision about their activities. This is especially key given that enemy soldiers may not be able to distinguish between regular use of a phone and intelligence gathering amounting to DPH in the fog of war, and while any party must adhere to the principle of distinction and when in doubt consider civilians to be protected, such legal rule may not in practice always be adhered to. It is thus key that civilians gathering intelligence are aware of such risks and implications.

4. Hybrid Warfare, the Ukrainian IT Army and Civilian Cyber Defence

On 26 February, 2022, Kykhaylo Fedorov, Ukraine's Deputy Prime Minister and Minister for Digital Transformation announced the launch of an IT Army on Twitter and called upon "digital talents" to join a Telegram channel "to continue the fight on the cyber front", promising "tasks for everyone".[78] While many of the details about their activities are unknown or at least not confirmed by official sources, some suggest that over 400.000 people have joined the Ukrainian IT army, many of which from outside Ukraine. Although repeated statements that there is no coordination between the Ukrainian government and the cyber IT army,[79] a list of targets, including a number of Russian and Belarussian businesses, banks as well as governmental departments, was initially published in the telegram chat in which administrators continue to post targets.[80]

So far, knowledge of the IT army's activities remains limited, especially from official sources. Initially, it has been reported that members have conducted a number of distributed denial of service (DDoS) attacks against Russian and Belarussian targets, including against the Kremlin, the Foreign Ministry and the Ministry of Defence as well as the Moscow Stock exchange.[81] Furthermore, members of the IT army have been said to patch vulnerabilities and thereby defend Ukrainian networks from Russian attacks. Other reported activities include gathering intelligence through espionage operations.[82] However, some reports find that the IT Army is "purely offensive in nature" and conducts offensive cyber operations against a number

[77] Landay and Balmforth.
[78] Tweet by Mykhailo Fedorov, 26 February 2022, available via https://twitter.com/FedorovMykhailo/status/1497642156076511233.
[79] Joe Tidy, 'Meet the hacker armies on Ukraine's cyber frontline', 15 April 2023, *BBC,* https://www.bbc.co.uk/news/technology-65250356; Jason Healey and Olivia Grinberg, ''Patriotic Hacking' is no Exception', 27 September 2022, *Lawfare*, https://www.lawfareblog.com/patriotic-hacking-no-exception.
[80] Matt Burgesm 'Ukraine's Volunteer 'IT Army' is hacking in Uncharted Territory', 27 February 2022, Wired, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.
[81] Healey and Grinberg.
[82] Independent via AP NewsWire, 'Ukraine cyber official: We only attack military targets', 4 March 2022, https://www.independent.co.uk/news/ukraine-russia-kremlin-boston-hackers-b2028853.html.

of targets, including Russian civilian infrastructure or online pharmacies.[83] As there is little authoritative information on the IT army's activities, these activities must be assessed with caution but even if they are hypothetical, tney raise key questions for the application of IHL.

In light of the considerations raised in Section 3 on the question what considers direct participation in hostilities by civilians, this IT army raises new questions for the concept and its application to hybrid warfare and especially to civilians who participate in conducting cyber operations in the wider context of armed conflicts. Against this backdrop, this section considers whether members of the cyber IT army constitute civilians that are directly participating in hostilities (a), whether they form a *levée en masse* (b) or whether they indeed must be considered combatants under new reform proposals (c).

a. Are the members of the IT army civilians directly participating in hostilities?

The Ukrainian IT army is also sometimes referred to as cyber volunteers or civilian volunteer hackers.[84] Such names carry a different connotation than describing the group as an IT army. What is in the name then and are the participants of this group actually civilians? According to Art. 5 of the ICRC customary international humanitarian law study, civilians are negatively defined as those who are not combatants.[85] Combatants, in turn, are members of the regular armed forces of one of the parties to the armed conflict. For the purpose of this section, the IT army is not incorporated into the regular structures under the Ukrainian armed forces (on reform plans see section 4c). However, some distinguish between the core team of the IT army which may have different, governmental support and assumes a coordinating function, than the wider membership of the IT army.[86] While such distinction could have implications, particularly as to the status of the core group under IHL, this paper does not have further information to analyse the separate status of the "core group" of the IT army but in line with the paper's main theme focuses on the implications of individual civilian participation. This paper also assumes that the Ukrainian IT army does not constitute a separate organised armed group fighting against the Russian armed forces and thereby engaging in a separate non-international armed conflict. To do so, the group in question would have to be sufficiently organised, able to implement IHL norms and also be "capable of engaging in sufficiently intense violence with their adversary".[87] Even where the organisational requirement is interpreted loosely, the IT army does not identify itself as distinguished group, but instead, members have indicated in interviews that they see themselves as part of the Ukrainian army[88]

[83] Stefan Soesanto, ‚The IT Army of Ukraine – Structure, Tasking, and Eco-System', ETH Zurich, June 2022, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/552293/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf?sequence=2, p. 4ff.

[84] Independent via AP NewsWire, 'Ukraine cyber official: We only attack military targets', 4 March 2022, https://www.independent.co.uk/news/ukraine-russia-kremlin-boston-hackers-b2028853.html.

[85] ICRC, International Humanitarian Law Database, Customary international humanitarian law, rule 5, available via https://ihl-databases.icrc.org/en/customary-ihl/v1/rule5.

[86] Soesanto, p. 7-8.

1. [87] Tilman Rodenhäuser, Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law, Oxford University Press 2018, p. 63.

[88] Janosch Delcker, ‚Inside Ukraine's Cyber Guerilla army', Deutsche Welle, 24 March 2022, https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527, Tidy.

and they do not fulfil the necessary threshold of violence or intensity of protracted armed violence as set out in the *Tadic* judgment.[89] The analysis is thus based on the assumption that the individuals of the IT army are civilians in an international armed conflict.

If the members of the IT army are not combatants but indeed civilians, do their activities nevertheless carry consequences for the application of IHL? If participants of the IT army are not combatants but civilians, they can nevertheless lose their civilian protection if they are directly participating in hostilities. As explained above, DPH requires three elements, i.e. a threshold of harm, direct causation and belligerent nexus.[90]

Assessing whether activities of the IT army meet the harm threshold requires a case-by-case analysis. Reported activities of the IT army so far included DDoS attacks and fixing vulnerabilities, both activities that arguably do not meet the threshold of harm, as they do not lead to death, injury or destruction and arguably, depending on the exact target, do not adversely affect Russian military operations or military capacity. However, this does not mean that cyber operations cannot principally reach such threshold given that cyber operations that do successfully interrupt the ability of Russian armed forces to communicate or conduct logistics would adversely affect Russian military operations. Soesanto's examples of offensive cyber operations against Russian (civilian) infrastructure mentioned previously would seemingly reach such threshold and potentially even violate the principle of distinction. Likewise, intelligence collection has in the past been considered to amount as DPH in specific circumstances.[91] Such collection could also be conducted via cyber means. It thus seem that irrespective of geographical location of the members of the IT army, some of these (potential) activities arguably may still meet the relevant harm threshold to constitute DPH. This has also been confirmed by the ICRC's guide on DPH that finds that "Electronic interference with military computer networks could also suffice" to meet the threshold of harm.[92] The authors of this paper find that it is unlikely that general defensive activities, such as patching vulnerabilities of Ukrainian networks to protect them from Russian cyber-attacks, would meet the harm threshold, but that certain offensive cyber operations e.g. to interrupt Russian military communications would indeed meet such threshold..

Even where they do, these activities would also still have to fulfil the other two requirements of DPH, i.e. have direct causation and belligerent nexus. To establish a direct causal link, the activity in question must result or be likely to result in harm or be an integral part of a coordinated military operation causing such harm. Currently, little is known how the activities of the IT army link to other military operations or their direct impact on Russian capabilities. It is thus not always evident that there is a direct causal link between some of these activities

---

[89] *Tadic, IT-94-1-T*, para 562.

[90] Melzer (43), p. 46.

[91] ICTY, The Prosecutor v. Pavle Strugar, Case No. IT- 01-42-A, Appeal Judgement, 17 July 2008, para. 177.

[92] Melzer (43), p. 48.

and the harm caused, especially where they contribute to the wider defence of Ukrainian networks or general intelligence efforts. In light of Ukrainian claims that the IT army does not coordinate with the Ukrainian military, it also not confirmed that these activities form an integral part of coordinated military operations. However, depending on the activities and the context of each of these, it is generally feasible that activities conducted by members of the IT army could fulfil the direct causation requirement.

Finally, the activities in question must be committed to directly cause the required threshold of harm in support to a party to the conflict and the detriment of the other (belligerent nexus). It seems likely that activities by a hacktivist or a civilian joining the IT army out of support for the Ukrainian state fighting against the Russian enemy would meet this requirement. However, little is publicly known about the exact involvement of the participants or their link to the hostilities. One news report states that participants "have different motives, and they use different cyber weapons, from simple tools for online vandalism to sophisticated cyber operations. But they are united in their goal: to support besieged Ukraine".[93] In that sense, it seems likely that belligerent nexus can be established for specific activitites. However, the question arises how loosely such requirement can be interpreted. While some might argue *any* cyber security measure taken by one party has in turn a negative impact on the enemy's military capacity, such interpretation would go too far in the eyes of the authors of this paper who consider that generic cyber security measures such as fixing vulnerabilities therefore do not have a sufficient belligerent nexus.

Overall, it is thus possible that where members of the IT army conduct cyber operations that have an adverse affect on the military operations of capacity of the enemy, have a direct causal link with the hostilities and have a belligerent nexus, they qualify as civilians directly participating in hostilities. However, where this is not the case and the activities in question do not meet the relevant criteria, as is the case for passive defences protecting Ukraine's networks or limiting the impact of Russia disinformation campaigns, Väljataga concludes that such activities would merely constitute indirect participation in hostilities.[94] Indirect participation in hostilities, e.g. in form of activities that are part of the general war effort or war-sustaining, however, does not mean that a civilian loses their protection from direct attack.[95]

It follows that civilians participating in the IT army that stay below the relevant threshold of harm and do not meet the three requirements of DPH do not lose their civilian protection. Nevertheless, they may be violating domestic law and could be criminally charged for their activities. However, where the relevant three requirements are met and the individual in question is directly participating in the hostilities, they could be directly targeted under IHL provisions for the time they are DPHing, even if such direct targeting could violate other norms of public international law where such civilian is located in a state that is not party to the conflict. Although the publicly available information on the IT army's activities is limited, it is likely that adversarial forces may hold different information, influencing their judgment on whether or not civilians who have joined the IT army are indeed directly participating in hostilities.

[93] Delcker.
[94] Ann Väljataga, ‚Cyber Vigilantism in support of Ukraine: a legal analysis', March 2022, CCDCOE, https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-pub.pdf, p. 3.
[95] Melzer (43), p. 51.

Furthermore, Russia has in the past advanced broad interpretations of what support of Ukrainian forces would amount to direct participation in hostilities and thus, who could be directly targeted.[96] Nevertheless, all parties must be reminded that where doubt as to their legal status exists, individuals must be treated as civilians.[97]

Finally, the authors of this paper would like to stress that civilians who are supporting Ukraine's cyber efforts are not principally acting in violation of IHL but need to be able to do so on an informed basis. As such, they must be aware about the legal and practical consequences of their actions. However, where "a growing number of (…) volunteers with little experience in cybersecurity who run hacker programs without fully understanding how they work" are joining these efforts, it is highly questionable whether they are sufficiently informed about the consequences their activities may carry. Arguably, it is up to them to inform themselves before joining such group and conducting these cyber operations, but it is at least questionable whether a state that directly benefits from their activities if not at least passively supports their activities has at the very least a moral – if not a legal – obligation to provide information that helps participants to make a conscious decision as to their levels of participation and possible consequences thereof. After all, all High Contracting Parties to the Geneva Conventions are obliged to ensure respect for the Geneva Conventions under all circumstances.[98]

b. Are the members of the IT army participants in a Levée en Masse?

While this paper has so far argued that the members of the IT army do not form part of the regular armed forces or a separate organised armed group, it could also be considered whether they are participants in a *levée en masse*. Participants in a *levée en masse* are "inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war".[99] Where participants of the IT army are indeed also participants in a *levée en masse*, they enjoy prisoner of war status and combatant immunity. However, the application of these requirements to the Ukrainian IT army is unclear, especially given the lack of detailed information on its operations.

Firstly, it is unclear in how far participants of the IT army are "inhabitants" of Ukraine. Whereas some members may certainly be, it is suspected that a number of individuals who hail from across the globe, i.e. non-inhabitants of Ukraine, have also joined the IT army, or at least have joined the respective Telegram channel.[100] However, those non-inhabitants of Ukraine – whether they are Ukrainian or not – cannot form part of a *levée en masse*. This first requirement is thus likely only fulfilled in part. Even where non-inhabitants of Ukraine use Ukrainian

[96] Väljataga, p. 3.
[97] ICRC, International Humanitarian Law Database, Customary international humanitarian law, rule 1, available via https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1.
[98] Common Article 1 GC I-IV.
[99] Art. 4(a)(6) GC III.
[100] Matt Burgess. However, whether this is sufficient to establish membership is debatable.

infrastructure to conduct the cyber operations, such limited involvement is not permanent enough to consider them inhabitants of Ukraine.[101]

Secondly, participants of the *levée en masse* must act within an unoccupied territory and to resist the invading forces. In this context, it is clear that activities in question must be conducted against Russian armed forces. However, what constitutes occupied territory may be less clear, as the situation continues to develop dynamically. The factual uncertainties aside, where it can be established that the Russian armed forces hold effective control and occupy a certain area,[102] inhabitants in such territories could not be participants of a *levée en masse*.

As a third requirement, spontaneity is key. Whereas little is known about the actual level of organisation and planning within the IT army, Buchan and Tsagourias elaborate that in their view, "the critical question is whether the group has been *organised* by the invaded government".[103] They conclude that the mere invitation or encouragement by government to join such group does not amount to commanding or organising the relevant participants.[104] Rena Uphoff also finds that the IT army "stood up in an ad-hoc manner without a clear structure and proven plan".[105] This is in line with Ukrainian officials who have repeatedly claimed that there is no coordination between government and the cyber IT army,[106] which they see as a volunteer group with multiple leaders.[107] However, some have describe the IT army as "government-led"[108] and others consider that "its level of organisation and subordination to the Ukrainian government seems a degree too high for it to be viewed as a *levée en masse*".[109] The level of coordination and organisation between the IT army and the Ukrainian government and therefore the degree of spontaneity thus remains subject to speculation.

Finally, it is unclear whether the members of the Ukrainian IT army carry their arms openly – or what this requirement even constitutes in cyberspace – and whether they adhere to IHL. Given that the ICJ held in the *Nuclear Weapons a*dvisory opinion that a weapon can be any instrument that causes harmful effects,[110] this means that the necessary hardware and software used by the members of the IT army could constitute such weapons. However, carrying them openly is also needed. Buchan and Tsagourias argue that for the *levée en*

---

[101] Russel Buchan and Nicholas Tsagourias, ‚Ukrainian ‚IT Army': A cyber Levée en Masse or Civilians Directly Participating in Hostilities?', 9 March 2022, *EJIL:Talk!,* https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/.

[102] RULAC/Geneva Academy, 'Military occupation of Ukraine by Russia', available via https://www.rulac.org/browse/conflicts/military-occupation-of-ukraine#collapse2accord.

[103] Buchan and Tsagourias.

[104] *Ibid.*

[105] Rena Uphoff, ‚The IT Army of Ukraine', 22 June 2022, https://css.ethz.ch/en/center/CSS-news/2022/06/the-it-army-of-ukraine.html.

[106] Healey and Grinberg, referencing Victor Zhora, senior cyber official in Ukraine, saying there is no coordination.

[107] Sam Schechner, ‚Ukraine's ‚IT Army' has hundreds of thousands of hackers, Kyiv says', Wall Street Journal, 4 March 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX.

[108] Burgess.

[109] Väljataga, p. 4.

[110] § 39 *Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory opinion), 8 July 1996, ICJ Rep 66* [1996].

masse this means visibly in line with the 1960 Commentary.[111] However, visibility with respect to "cyber weapons" is of course of limited practicality. While a laptop or computer may very well be visible, it is arguably invisible components such as malware that are decisive, especially given that any civilian would nowadays also be likely to carry around a phone or laptop, thus being indistinguishable from members of the IT army.[112]

Given the limited information available, it is also not clear whether the members of the IT army currently comply with the IHL rules. Victor Zhora, a senior Ukrainian cyber official, stressed that the IT army only targets military targets,[113] but some have questioned these assessments, e.g. by pointing out that the Moscow Stock Exchange is a civilian target.[114] Similarly, Soesanto finds that civilian infrastructure has been targeted by the Ukraine IT army.[115] While formerly civilian objects may under certain conditions constitute legitimate military targets, it is nevertheless uncertain to what extent the members of the IT army adhere to IHL rules.

To conclude, the participants of the Ukrainian IT army are – at least given the limited information available – unlikely to meet the requirements necessary to constitute a *levée en masse*. This is especially in light of the continued operations throughout the armed conflict and the level of coordination and therefore lacking spontaneity that must be assumed. It follows that they do not enjoy combatant privilege nor are they entitled to prisoner of war status.

c. Will the IT army be integrated in Ukrainian armed forces?

New developments indicate that Ukraine wants to incorporate its IT army in its regular armed forces.[116] While an established cyber command section within Ukrainian armed forces is not a surprise, the proposal seeks to continue to involve volunteer hackers. Such structure is also implemented by the Estonian Cyber Defence Unit on which the Ukrainian plans are modelled after, seeking to build a cyber reserve after training personnel as part of their mandatory service.[117]

While there are currently no further updates on the restructuring of the IT army, should active members of the IT army assume a role within the Ukrainian armed forces this could change their legal status under IHL. If their plans are indeed based on the Estonian Cyber Defence Unit, it is likely that the Ukrainian model would also constitute a volunteer corps that is, however, part of the armed forces as it also falls under army command structures in armed conflict.[118] As such, active members would then qualify as combatants in line with Article 4(a)(2) GCIII assuming that they fulfil the respective requirements. Where this is the case,

---

[111] Buchan and Tsagourias
[112] *Ibid.*
[113] Independent via AP news wire (n 98).
[114] Healey and Grinberg.
[115] Soesanto, 4.
[116] Shaun Waterman, 'Ukraine Scrambles to Draft Cyber Law, Legalizing its Volunteer Hacker Army', 14 March 2023, NewsWeek, https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.
[117] *Ibid.*
[118] Kadri Kaska et al, ,The Cyber Defence Unit of the Estoniann Defence League – Legal, Policy and Organisational Analysis', 2013, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf.

members of the IT army would gain combatant privilege, meaning they can lawfully participate in the ongoing armed conflict against Russia, but they would therefore also lose their civilian protection and could be directly targeted, both by cyber and conventional means.

The details of this plan, however, are currently unclear. For example, it is not evident how the Ukrainian army would treat foreigners located outside Ukrainian territory that have so far informally joined the IT army. Nevertheless, further steps taken by the Ukrainian government will likely clarify this. Until then, their participation in Ukrainian cyber operations or in support thereof must be assessed with caution. While volunteers provide effective support for Ukraine's defence against an unlawful intervention and brutal invasion from Russia, their activities can carry severe consequences – not all of which may be clear to those who are civilians and have not been educated and informed about their status and its legal implications under IHL.

5. Concluding thoughts

Estonia, Latvia, and Lithuania offer valuable insights into how civilian populations can be effectively incorporated into national defence strategies, drawing from their extensive experience in successful non-violent civilian defence. While civilian defence was initially regarded primarily as a non-violent means of maintaining social cohesion and upholding national values, this perception has evolved over time. Our analysis of the Baltic Republics' defence strategies reveals that civilians are not only encouraged to engage in typical non-violent civilian defence work but also to participate in activities that may potentially meet the threshold for DPH. Non-violent defencive actions cannot cross the threshold to DPH. On the other hand, engaging in violent civilian defence can potentially lead to civilians engaging in DPH. However, such strategies are not per se in violation of IHL due to a lacking prohibition of such acts.

Over time, and in response to the increasing threat from Russia, civilian defence has morphed into a more blended approach, combining non-violence and violence. A civilian secretary is likely aware that picking up a rifle to join in their country's defence (irrespective if it is a case of *levée en masse* or not) will mean they are participating in hostilities and therefore a legitimate target. However, a student who is skilled in IT and participates in certain cyber-attacks, might not be aware that they are crossing the threshold to DPH and can become a target for lethal force.

Baltic countries have shown examples of how civilians can be included in resisting foreign aggression. While it might not be a necessity to allow or encourage civilians to engage in violent acts and such civilianisation of conflict comes with considerable risks, it certainly is necessary to at the very least address civilian *resilience* against hybrid threats. Consequently, NATO and Western states should urgently consider the Baltics' example.

Indeed, the 2022 invasion of Ukraine by Russia further underlines the crucial element civilians play in national defence. Whether in the form of civilian protest, keeping up morale and Ukrainian identity or by war-sustaining efforts on or offline – examples of how civilian Ukrainians contribute to their defence are manifold. Yet the war in Ukraine also underlines that whereas civilian contributions may continue to take place in traditional forms like making

camouflage covers or Molotov cocktails, civilian defence contributions in the 21st century may also entail a cyber element.

The war in Ukraine also exposes the challenge of determining the legal consequences of civilians' actions, especially assessing when civilian activities qualify as DPH, particularly in the absence of adequate factual information. Civilians often have limited access to comprehensive information, both due to their relative lack of resources and the complex nature of conflict information. Consequently, assessing the extent to which their contributions are integral to military operations and potentially amount to DPH becomes difficult. This means that both based on the limited information that civilians may hold but also a likely lack of information and understanding about the legal consequences their activities may carry, it will be difficult for civilians to assess in how far their contributions are, for example, integral to military operation, and, as a result, amount to DPH which would mean that they lose their protection from direct attack.

Therefore, informing civilians about implications of their actions is key.[119] While the necessity for the Ukrainian government recruiting digital skills for their cyber defence or civilians supplying information is evident and understandable when defending themselves in an armed conflict that seeks to eliminate a sovereign state, this does not mean that the Ukrainian government does not hold at least a moral if not also a legal responsibility to inform its civilians about the consequences of their involvement under international humanitarian law. The same applies to any other state seeking to develop defence strategies that include civilian participation of violent and non-violent kind. Of course, the two researchers writing this paper have limited access to information that confirm in how far information sharing on such matters already occurs, for example through warning notifications when using relevant apps or cyber tools. Therefore, this section is written with caution, merely confirming the central importance of educating all participants – civilian or not – of an armed conflict about their rights and obligations but also of the legal consequences of their involvement.

The last question the authors sought to address in this paper was whether Baltic and Ukrainian civilian defence strategies are the next logical step in (hybrid) warfare? While such an inclusion is compatible with excisting IHL, the authors hope that states refrain from encouraging their civilian population to engage in acts that cross the threshold to DPH. Otherwise, the principle of distinction could lose its bite and dramatically increase civilian deaths and suffering - the very thing the Geneva Conventions sought to minimise.

[119] See also Kubo Macak, 'Will the centre hold? Countering the erosion of the principle of distinction on the legal battlefield#, Internaiotnal Review of the Red Cross, https://international-review.icrc.org/articles/will-the-centre-hold-923, setting out legal implications under domestic and international law.