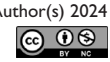
Article

Media, War & Conflict

Media, War & Conflict
2025, Vol. 18(3) 305–324



DOI: 10.1177/17506352241236449
journals.sagepub.com/home/mwc


Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion

Kateryna Zarembo[1,2], Michèle Knodt[1] and Jannis Kachel[1]

Abstract

In modern warfare, digitalization has blurred the line where civilian ends and military begins. Embedded in the participative warfare theoretical paradigm, this article looks into how the information and communication technologies (ICT) enable civic resilience under the conditions of the foreign armed aggression. Specifically, the authors explore how smartphones and smartphone applications empowered the Ukrainian civil society in the aftermath of the Russian full-scale invasion of 2022. Based on an online survey and semi-structured interviews, the article highlights how the device and its features not only allowed civilians to adapt to living in conditions of a constant threat, but also to respond and support the defence from the rear. The authors conclude that, while the smartphone becomes an 'online resilience hub', acquiring many new functions like a mobile office, an online volunteer (frontline logistics and procurement) hub, an air-threat warner, a first-hand news source and so on, its security provision functions are not unconditional and may turn to the opposite, depending on the physical circumstances on the ground as well as the virtual information battlefield.

Keywords

civil society, participatory warfare, resilience, Russian war, smartphone, Ukraine

Introduction

Ukraine's civic resilience since the full-scale Russian invasion that began on 24 February 2022 has been widely documented (Melchior, 2022; Rating Group, 2022; Zarembo and Martin, 2022). With Ukraine's high degree of digitalization, it also immediately took a profound digital dimension as numerous actions, from army-oriented donations to enemy spotting to distribution of humanitarian aid, could take place online (StrategEast, 2022).

[1]Technical University of Darmstadt, Germany
[2]New Europe Center, Kyiv, Ukraine

Corresponding author:
Kateryna Zarembo, Technical University of Darmstadt, Karolinenpl. 5, Darmstadt 64289, Germany; New Europe Center, Kyiv, Ukraine.
Email: kateryna.zarembo@gmail.com

However, we still know relatively little about the role of information and communication technologies (ICT) within the Ukrainian resilience. Specifically, we are interested in how ICT could help enhance the resilience of civilians by means of a basic commonplace technology – a smartphone.

We thus ask the following questions: How did smartphones and smartphone applications contribute to civic resilience after the Russian fullscale invasion in Ukraine? How was the use of the smartphone by civilians modified and adapted during full-scale war in contrast to the period before 24 February 2022? How did the smartphone empower and disempower its users in wartime – which opportunities did it create for its users and was it possible for it to be used against them and, if so, how? Rather than reducing the role of a civilian in war to two options – fight or flight – looking at how the smartphone contributes to civic resilience during a war can shed light on both the role and function of smartphone applications in modern warfare.

This research is an interdisciplinary study, drawing on the literature of digital warfare and civic mobilization. To answer our research questions, we followed a mixed-methods approach: we first conducted an online survey with 1000 respondents in September 2022. This quantitative survey data was then complemented by 10 semi-structured interviews with civil society representatives during the course of autumn 2022, complemented by two additional interviews in October 2023.

This article is structured as follows: first, we outline our theoretical framework which is based on the participative warfare theory. We then present the literature review on the use of smartphones in war. The next section explains the choice of Ukraine as a case study, followed by a detailed description of the methodology. Our research findings are presented and discussed before we finally draw conclusions and suggest avenues for further research.

Smartphones, societies and war: What we know

As noted by O'Loughlin (2020: 123), new digital technologies 'have already been integrated into how militaries, media and *societies* wage, resist and understand war' (emphasis added). The advent of the participative war allowed 'everyone to experience and take part in the conflict' (Merrin, 2018: 195), thus blurring the lines of traditional warfare from a quadruple perspective: between online and offline participation (Couldry and Hepp, 2017, cited in Asmolov, 2022), between the geographical boundaries of participation (related to the 'remote warfare' concept (Crawford, 2015, cited in Asmolov, 2021), in the state's monopoly on the use of force (Boichak and Asmolov, 2021; Patrikarakos, 2017) and, most importantly, between civilians and the military (Boichak and Hoskins, 2022; Merrin, 2018; Patrikarakos, 2017).

It has been already observed that participative warfare, conceived by Merrin (2018) as primarily (self)mobilization into information war, has expanded into various other conflict-related domains: '"Hacktivism" (Lokot, 2017), the analysis of open source intelligence (OSINT), crowdfunding practices that support the purchasing of military ammunition, as well as the facilitation of conflict-related offline activities ranging from logistical assistance to actual participation in warfare' (Asmolov, 2021: 345), enemy spotting (Winther and Nilsson, 2023) and other practices. The literature on ICT and warfare tends to prioritize the digital space (e.g. the social media) as a research subject

(Boichak, 2017; Boichak and Jackson, 2020; Patrikarakos, 2017), rather the physical tools or gadgets through which they are used (Horbyk's [2022] study of the use of mobile phones among the military is a notable exception). A similar tendency is observed in the literature on the role of the media in civic mobilization in protests, revolutions and social unrest (Khamis et al., 2012; Metzger and Tucker, 2017; Onuch, 2015), where the emphasis is on the media rather than on the means to use them.

While ICT can denote a number of potential gadgets and digital access points, the role of the smartphone in warfare in view of its mobility and multiple functions deserves special attention. The smartphone is a piece of information technology, with which 'the user is no longer a passive actor who simply responds to stimuli (i.e. properties of the technology), but rather determines what the technology is to them through their participation with it' (Jung, 2014: 301). In fact, the crucial role of civilian communications technology, like smartphones, for war and defence has already been acknowledged. Winther and Nilsson (2023: 2) quote a US Army specialist who stated that 'no defense company in the world can beat the reliability and performance these small devices deliver.'

The research of smartphone use by civilians in wartime can be grouped into three broad thematic categories: (i) mundane use (see Schejter and Cohen, 2013; Tkach and Williams, 2018); (ii) flight (see Eriksen, 2020; Narli, 2018; Steinbrink et al., 2021); and (iii) resistance (Malka et al., 2015; Rohde et al., 2016). In this article, we focus on the latter. We aim to establish the role of the smartphone in everyday acts of individual civilian resilience in the face of a military invasion.

While we employ both the terms 'resistance' and 'resilience' in the text of the article, we should underline that there is a hierarchy between them. We rely on the definition of resilience adapted from Korostelina (2020): 'The resilience of a nation [is] a process enhancing a capacity of a national community to address conflict through adaptation, effectively *resisting* perpetrators of violence' (emphasis added). According to this definition, resistance is only part of resilience. The meaning of resistance itself, as we understand it in this study, is close to that of national civilian defence, as defined by Bartkowski (2015: 11) as 'a political struggle conducted . . . through flexible but integrated local and national networks of civilians that can mobilize hundreds of thousands or millions of people to engage in disciplined, self-organized, agile and flexible anti-aggressor actions'. As far as 'adaptation' is concerned, we borrow the definition from Rabinovych et al. (2023) who define it as 'the ability to deliberately change its practices and/or adopt new ones in response to a shock by linking resources (adaptive capacities) to shocks'.

The digital face of Ukraine's response to the Russian invasion

Civic mobilization in the face of the Russian aggression since 2014 is well documented in the literature (Puglisi, 2015; Zarembo, 2017), especially in the case of state weakness, which is 'the inability of the state to perform its functions with regard to the provision of security, civil rights, welfare services and other political goods' (Lorch, 2017: 10). While numerous studies offer analyses of Ukraine's civic mobilization in width and depth, Boichak (2017) and Boichak and Jackson (2020) wrote specifically about the role of social media in resistance and strengthening of national identity, starting with the response to Russian aggression since 2014.

Since then, Ukraine's digitalization and internet penetration have made a few steps forward. In 2019, the Ministry for Digital Transformation of Ukraine was established, with a mandate to replace face-to-face bureaucracy and paperwork with digital interaction between the state and the citizens. The Ministry has created and launched the mobile application 'Diia', also known as 'A State in a Smartphone', which contains the electronic versions of personal documents such as identity cards (ID), passports, driving licences, COVID vaccination certificates, etc. Ukraine became the first country in the world to recognize electronic ID cards on a bar with biometric 'traditional' ones. Ukraine's internet penetration rose from 37.49 percent in 2014 (Onuch, 2015) to 79 percent in 2021, according to the CIA (Central Intelligence Agency [CIA] World Factbook, 2023).

Ukraine's resistance to Russia's full-scale aggression on 24 February 2022 immediately took on a profound digital dimension. Laura Keenan (2022), commenting on the public addresses that President Volodymyr Zelenskyy recorded on his smartphone, correctly observed that:

> Zelenskyy recognized that his phone was a tool, circumventing traditional media gatekeepers. He became the strongest voice representing Ukraine to the world, but every Ukrainian citizen with a smartphone could follow his lead and become a de facto ambassador.

Raising awareness is just one of the smartphone's many functions that can be used by civilians at war. After Russia launched a full-scale invasion, new mobile applications appeared overnight, channelling the information both from the state to the citizens (as in eTryvoha, a mobile application that gives information about air alerts) and from the citizens to the state (as in eVoroh or Bachu.info which allow the citizens to report the enemy's whereabouts to the state), or ePPO, which can be used to report air threats such as Shaheed-136 drones, which Russia often used, by pointing the phone to the threat and pressing a red button (Winther and Nilsson, 2023: 2). The smartphone has become the tool through which the state can protect the citizen, while the citizen, in turn, can also extend security services to the state. Table 1 contains some examples of digital smartphone-accessible applications, indicating the direction of the information flow (citizens-to-state and state-to-citizens).

The opinion polls confirm that, in 2022, 60 to 80 percent of the Ukrainian citizens participated in resistance through various functions (Rating Group, 2022), from monetary donations to raising awareness, to supplying gear and ammunition to the frontline and to helping the affected civilians. It should be mentioned that neither the polls nor this study had a pre-defined 'minimum threshold' of how much one should do in order to be considered 'resistance participant'. Some observers remark that the digitalization of war allows one to have 'the feeling of having done something … without actually doing anything much at all' (Onuch, 2015), like sharing a post on Facebook, signing an electronic petition or making a small donation. It is important for us, however, not to discount such small acts of resistance, even if they are little. It is precisely what Ken Booth (1997) wrote about the role of an individual in security, 'I am a drop in an ocean' philosophy (FitzGerald, 2014), when many small individual efforts can contribute to a big cause. Researchers also warned against denouncing small digital acts of activism as

Table 1. Examples of digital applications and channels created in Ukraine in the aftermath of the Russian full-scale invasion.

Function	Examples of applications/channels	Direction of information flow
News and updates	*A variety of official Telegram channels (Ukraine's Airforce, Oblast-level State Administrations, Spravdi)*	state-to-citizens
Crowdfunding for Ukraine's Armed Forces	*Diia, Aid for Ukraine website (cryptocurrencies)*	citizens-to-state
Shelter and physical security	*eTryvoha, Povitriana tryvoha*	state-to-citizens
Surveillance	*eVoroh (Diia/Telegram), STOP Russian war bot (on Telegram), ePPO*	citizens-to-state
Social and humanitarian aid (veterans, internally displaced persons [IDPs])	*ePidtrymka (Diia), eDopomoha (Diia) UA Veteran Bot (Telegram)*	state-to-citizens
Documenting Russian war crimes	*russian_war_tribunal_bot (Telegram), warcrime_bot (Telegram, Viber), Dokaz.gov.ua*	citizens-to-state

Source: Authors' compilation based on StrategEast (2022) and own observations.

'slacktivism', offering more neutral terms like 'micro activism' or 'online activism' (Joyce, 2012), even if these are only the first rungs of the 'ladder of engagement'.

We thus ask the following questions: How did smartphones and smartphone applications contribute to civic resilience after the Russian full-scale invasion in Ukraine? How was the use of the smartphone by civilians modified and adapted during full-scale war in contrast to the period before 24 February 2022? How did the smartphone (dis)empower its users in wartime?

Methodology

The present article is an explorative study and derives its data from human evidence. It employs mixed-method research, combining a quantitative survey with qualitative in-depth interviews.

The *quantitative survey* was commissioned by the authors and conducted by the Info Sapiens polling agency as an online panel ($N = 1060$). Fieldwork took place from 29 August to 5 September 2022. The sample covers all regions of Ukraine controlled by the Ukrainian government as of February 2022. The sample was built according to the data of State Statistics Service of Ukraine on the structure of population of cities of 50K+, aged 18–55 by sex, age, pre-war region and settlement size. Of the survey participants, 47 percent were male and 53 percent were female. Nearly 69 percent of our respondents reported no change in residence, while 31 percent reported displacement. Of those surveyed, 14 percent (about half of those who experienced displacement) returned to their original place of residence.

The following limitations should be noted. Firstly, because of the online panel limitations, the sample did not include residents of towns and villages with a population of less

than 50,000 inhabitants and those aged over 55. This means that the survey sample covers only 41 percent of smartphone users (60% of the Ukrainian population used smartphones as of February 2022). Secondly, for the same reason, the survey sample is biased towards more educated, socially active and technically skilled respondents. Thirdly, the sample insufficiently covers Ukrainians abroad (they constitute 7% of the sample, but according to the estimations of the number of Ukrainian refugees this figure could be twice as high). Finally, those Ukrainians who lost internet connection due to the war were de facto excluded from the sample. Overall, this means that the survey is representative only for a restricted sample of urban, more educated, socially active and technically competent respondents and conclusions drawn from it cannot give a picture for all of society.

To shed light on the role of the smartphone in the Ukrainian resistance, we make use of the survey's data in two ways: first, we conduct descriptive statistics in the form of data visualizations that explore the importance of the smartphone in resistance activities and, second, we investigate the relationship between different types of resistance activities and smartphone apps.

While the quantitative survey contributed to establishing overall smartphone use tendencies, it did not allow for extracting in-depth explanations of the users' behaviour. Thus, the authors conducted 12 *semi-structured interview*s with civic activists (10 interviews took place between August and December 2022 and two additional interviews were conducted in October 2023). The candidates for the interviews were identified through Facebook, Instagram and Twitter. The criteria for selection were: permanent residence in Ukraine at the time of the start of the full-scale invasion, public online communication of their involvement in resistance and regional diversity. We tried to diversify the pool of respondents as much as possible: namely, the participants were 6 men and 6 women, with the youngest respondent in their 20s and the oldest in their 50s. Geographically, 4 respondents represented the northern part of Ukraine (Kyiv), 3 respondents stemmed from the East (Kharkiv, Kramatorsk and Slov'iansk), 3 respondents were from the South (Odesa and Kherson) and 2 respondents from the West (Lviv and Ternopil). Four out of 12 respondents were internally displaced as a result of the war of aggression and one was a refugee in the EU. One of the respondents had lived under occupation for two months (before escaping to the free territory). Profession-wise, the sample comprised a student, two journalists, an IT manager, three academics, two private business owners and three NGO workers. The purposeful selection of civic activists engaged in resistance allowed us to receive insightful and self-reflective responses during the in-depth interviews.

Given the displacement and/or high mobility of both the interviewees and the interviewing co-author, these interviews took place via Zoom. The interviews lasted 30 to 40 minutes and were conducted in Ukrainian. To ensure that the research was ethical, the following measures were taken: (1) the interviewee guide was examined and approved by the Ethics Commission of TU Darmstadt; (2) the interviewees were informed of the purpose of the interviews and provided their explicit written consent to participate; and (3) the interviewees' confidentiality was guaranteed.

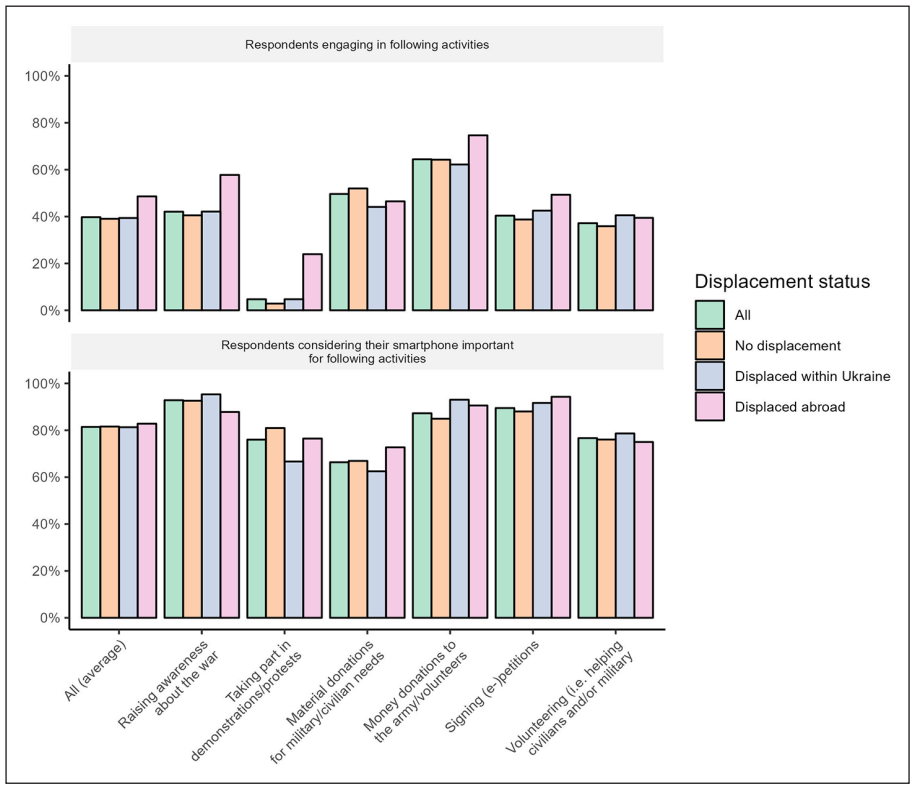


Figure 1. Combines the aggregated responses of survey question 3.2 ('Have you taken part in any of the following actions since the Russian full-scale invasion of 24 February 2022?') and question 4.1 ('How important is your smartphone for your activities: xx'), grouped by the respondents' displacement status.[1]

[1] Figures 1 to 3 do not distinguish between the experience of those who returned to the original place of residence (which was reported by about half of those who experienced displacement) and those who did not. Color figure available in online.

Results I: Smartphone as an online 'resilience hub'

Our study confirmed not only wide engagement but also the paramount importance of the smartphone in resistance among the citizens. Figure 1 illustrates how many respondents are engaged in different resistance activities (top) and how important their smartphone is to each of these activities (bottom) – grouped by displacement status.

Regarding the former, the survey shows that at least 40 percent of all respondents are involved in each resistance activity, with the exception of demonstrations, where only 5 percent of respondents are involved (demonstrations and public protests are restricted during the martial law according to the Ukrainian Constitution). Donating money is the most common resistance activity among all respondents, at 64 percent. Interestingly, the level of involvement seems to depend on the respondents' displacement status, i.e.

whether they had to move – either within Ukraine or abroad – due to the Russian aggression. Displacement seems to increase engagement in certain activities: for example, those who moved abroad engage more in raising awareness, demonstrating, donating money and signing e-petitions.

Regarding the latter, the absolute majority of all respondents of the survey rated the importance of the smartphone to their activities as high, from 76 percent for volunteering to 92 percent for raising awareness about the Russian war against Ukraine. The only exception is material (non-monetary) donations for military or civilian needs, for which the smartphone was important for 46 percent of all respondents. Location seems to play only a minor role in how important the smartphone is for different resistance activities. For respondents who moved abroad, the smartphone seems to be slightly more important on average than for others, especially for donating money and signing e-petitions. For respondents who moved within Ukraine, the smartphone seems to be particularly important for raising awareness, donating money and volunteering. However, these differences are in the small single-digit percentage range. These results suggest that the smartphone is generally an important tool of resistance for the respondents, regardless of their displacement status. However, the small differences that do exist between the groups could also be explained by their different opportunity structures. For the respondents dislocated abroad, the smartphone is one of the few channels through which they can effectively engage in resistance activities at a distance, making it all the more important.

The in-depth interviews confirmed that the smartphone, which is small, mobile and allows both mobile and internet connection, became a digital 'resilience hub', taking over the key life-sustaining functions. Almost all interviewees remarked that connectivity, which the smartphone allowed, was paramount for their resilience.

Many respondents reported setting up chats with their friends and colleagues from Ukraine and abroad. The functions of the chats were manifold. They were used to receive the most up-to-date information in the conditions of uncertainty:

> This chat was set up to exchange information about where the explosions are, who is alive, who goes where and with which route. It also helped us to look for accommodation, because people dislocated;

> My student chats became my road maps on where the jams are . . . how to get out of Kyiv, how to reach a certain place safely, where you can find gas. It was one of the most important resources – to get information about which petrol stations have gas.

The closer the frontline or occupied territory, the more first-hand information from those who were at the site was valued by its receivers since it gave nuances that no media could take hold of or report.

The chats also immediately converted into volunteer coordination points, connecting people from different locations:

> Immediately on the first day of the full-scale invasion I got a request for walkie talkies. They told me there are no more in Kyiv, but one can get them from Poland. I shared this request

> immediately in the chat, where my friends, very different Ukrainians from all over the world, were and within hours we resolved how to deliver those walkie talkies from abroad to Ukraine. And this network became the base for all the following volunteering.

The smartphone also allowed the continuation of basic daily activities, such as work. One interviewee remarked that, as a working mum and an activist, she does not have an opportunity to work for hours at her laptop, so many things have to be resolved 'on the go', i.e. on the smartphone. Another remarked that a phone is easier to charge under the conditions of restricted electricity or a blackout than a laptop. For yet another, the smartphone allowed her to continue teaching because she used it as a mobile hot spot while delivering lectures from the shelter.

Last but not least, connection through smartphones was also a source of psychological relief to know that people you care about are safe (or not). Apart from exchanging calls and messages, the 'last was online' function, which some messengers, like Facebook messenger or WhatsApp, allow other people to see, has become in itself an information source for those who care about other people in potential danger, e.g. at the frontline, in occupation or in a place hit by a Russian missile attack. In case they cannot get in touch otherwise, the 'being online' notification indicates that the person was at least alive at the registered time.

Results II: Resilience as staying connected

The smartphone allowed people to stay connected which amounted to being able to do and accomplish virtually everything:

> I really remember that feeling when we were in the basement . . . and the mobile connection is shown by only one line, there is shelling outside, but you can open a euro account, share bank details, raise money [for ammunition]. This gave us the feeling of invincibility.

> While at the beginning of the war I was not physically close to [other] volunteers, I managed to help them exclusively via internet, via mobile phone.

However, the mobile internet, let alone Wi-Fi, is not always available even in peaceful times, to say nothing of war time. The interviewees reported various tactics in order to ensure that they always remained connected. Many reported having acquired sim-cards of all available mobile operators, to secure as much access to the internet as possible. Some have also bought additional power banks, always keep their phones charged and even have additional phones, in case the battery of the other one dies:

> I have a back-up phone with a more powerful battery. I have [sim-cards] of all mobile operators: Life, Kyivstar and Vodafone. So in case one provider's connection fails, I can switch on the other phone and find the internet through a different one.

One interviewee also reported relying on Starlink – satellite high-speed internet systems which are frequently used by the Ukrainian military.

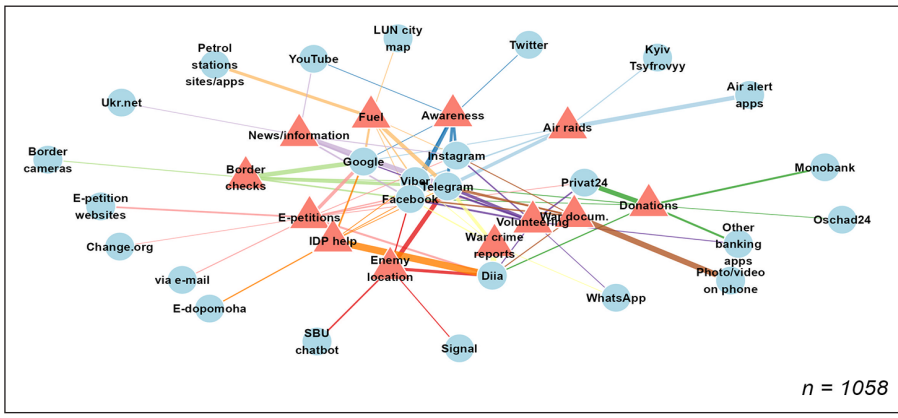


Figure 2. Bipartite network graph of all respondents. Smartphone-related resistance activities are represented by triangles, smartphone apps by circles. The thicker the edges between two nodes, the stronger their relationship. The more central an app is, the more connected it is to the activities (degree centrality). Generated with R using the 'igraph' package (Kamada-Kawai layout algorithm).
Color figure available in online.

The interviewed person who was displaced in the EU remarked on another aspect of the staying-connected strategy. While they did not experience any internet shortages or power blackouts, they had to retain their Ukrainian phone number in order to stay connected to resistance networks and at the same time had to get a second, new phone number from the local provider. They admired the mobile application which allowed them to acquire a virtual sim-card and thus retain both numbers (Ukrainian and local) simultaneously.

Results III: Social media as a resilience tool: 'The Telegram case'

We asked the respondents which mobile applications they use for their resistance activities. The results are presented in Figures 2 and 3. Both figures show so-called bipartite network graphs, with Figure 3 differentiating between the three residential groups and Figure 2 displaying all data. Both visualize the relationships between 12 types of resistance activities (triangles) and different smartphone applications (circles). The thickness of the edges, i.e. the connections between the circles and triangles, represents the frequency of how many people use a smartphone app for a specific activity. For example, Figure 2 shows that for the activity 'war documentation', the respondents primarily rely on the camera of their phones (see the thick edge between 'war documentation' and 'photo / video on phone'). The apps 'Facebook', 'Telegram', 'Diia' and 'Instagram' also have a link to 'war documentation', which means that they are also used for this activity. However, because their nodes are less thick, they are used less frequently for this purpose. Frequencies lower than 2 percent were excluded for clarity reasons. For better

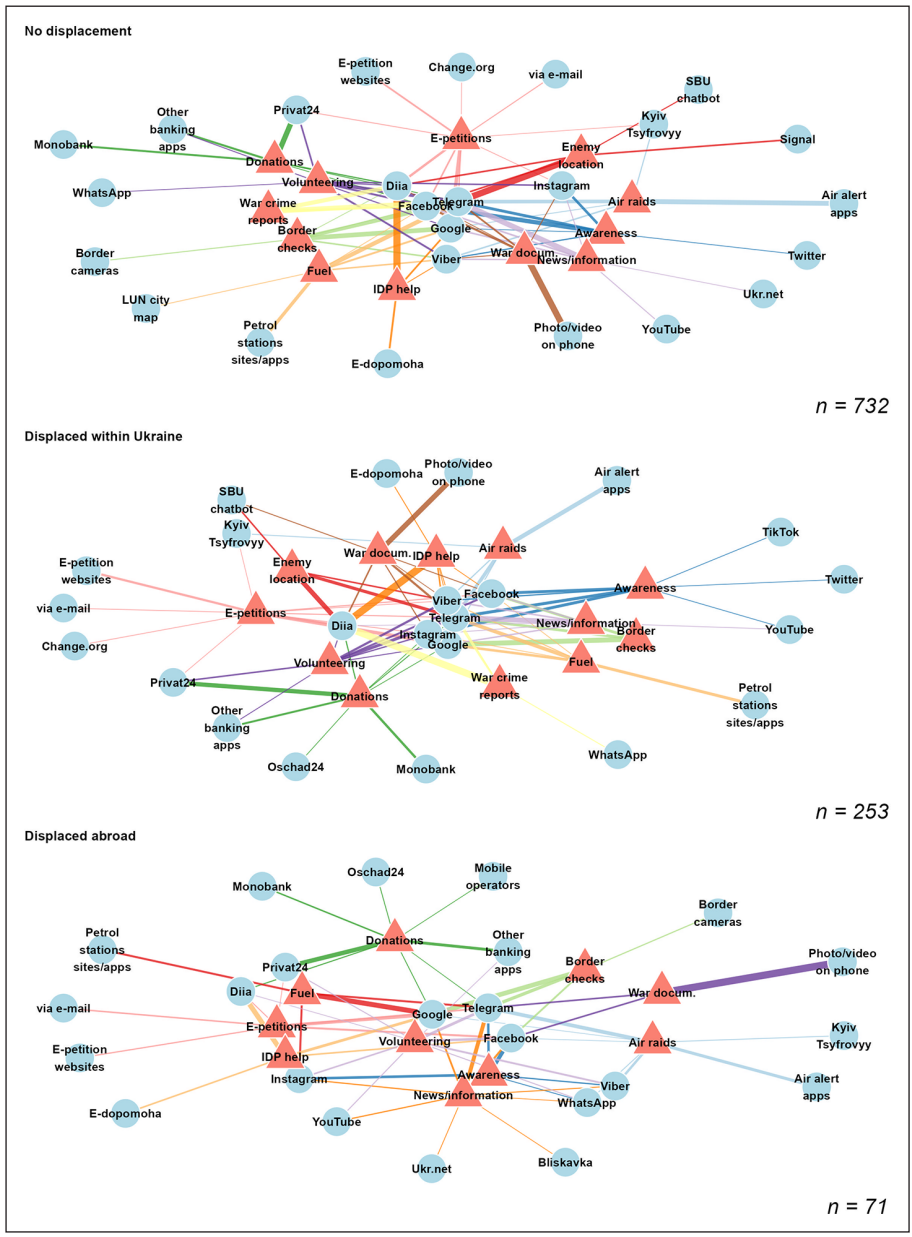


Figure 3. Bipartite network graph by displacement status (see description of Figure 2). Color figure available in online.

visibility, we have assigned the same colour to all links from the same resistance activity. Moreover, the more links an application node has, the higher its *degree centrality* and the

Table 2. Which new mobile applications did you start to use after 24 February 2022 (top 6 answers)?

Smartphone application	Share (%)
Application of air alert/map of air alert	23.79
Telegram	20.91
Diia	8.62
Google/Google maps	3.54
Signal	3.36
Petrol station sites/applications of fuel	2.73%
None/without changes	21.78

more centrally it is positioned in the graph. In other words, the more central an application is in the network graph, the more resistance activities it is used for. Conversely, the more peripheral an application is, the more specific its use in resistance.

The most striking finding is that the social media apps Facebook, Telegram, Viber and Instagram seem to play a central role in the smartphone-based resistance activities – they are in the centre of the network graph in Figure 2. Meanwhile, other social media apps are used for only a few activities. The messenger app Signal is apparently only used to locate enemies, but again it plays a minor role compared to Telegram. WhatsApp is more widely used, but its share of usage is also low.

However, these findings do not hold true for all subgroups. Figure 3[1] shows that the use of smartphone apps for resistance activities differs depending on the experience of dislocation. For respondents who stayed in Ukraine, the apps Diia, Facebook, Telegram, Viber and Instagram are central to their resistance efforts. Among respondents who have moved abroad, Telegram and Facebook are central for their activities, while Diia, Viber and Instagram seem to be used less. The drop-out of Diia and Viber can be specifically explained by the fact that Diia's usability is reduced abroad (e.g. a digital ID or driving licence is recognized in Ukraine, but not in other countries), while Viber as a messaging application is more popular in Ukraine than in some other European countries where the respondents could have been displaced to. The persistence of Telegram in all groups is explained further below.

Moreover, the survey data also indicate that Telegram was boosted with the beginning of the war: looking at the answers the respondents gave when asked about the new applications that they started using after the full-scale invasion, one can see that Telegram comes second only to the air alert application, with 21 percent of the respondents (see Table 2). Another prominent finding is the use of the Ukrainian state application 'Diia' which is situated centrally on a par with the international social media. Table 2 also confirms 'Diia' as the third-ranking application which the respondents started to use after the full-scale invasion. This may be explained by the wide array of functions that 'Diia' offers (in addition to electronic ID), like donations ('Army of Drones' project), enemy spotting (eVoroh), registration as an internally displaced person, maps of 'Points of Invincibility' (specially organized sites where people can get access to warmth, water and electricity in case of a blackout), etc.

The results of the in-depth elite interviews offer a slightly different picture of social media use, with Twitter and WhatsApp featuring as prominently as Facebook, Telegram and Instagram, while Viber is largely dismissed. Telegram is highlighted in the interviews as prominently as in the survey.

One of the interviewees offered a rather detailed explanation of social media functions in Ukraine at war:

> All communication with volunteers most often took place in a social medium or a messenger . . . I realized that Twitter works well in order to ask for a money donation. And for the Western audiences it is only Twitter that works. However, if you need to find a contact in Ukraine, people in Ukraine, organize the unloading of aid or something – you use Messenger from Facebook. For media interviews, Western and not only, I use WhatsApp. And for staying in touch with the close people it depends. With the older generation you use Viber. For friends we established special chats in Signal, moving there from Telegram. And I use Telegram for my students.

The use of Telegram merits special attention here. After the start of the full-scale invasion, the total time of Telegram usage in Ukraine increased eightfold (Myronova, 2022). This is primarily connected to the fact that numerous news channels appeared on Telegram, including the channels established by the central and local government for public communication (e.g. Spravdi, Ukraine Now, channels of local government administration) as well as non-governmental information channels. As one respondent put it:

> The most [often used] messenger is Telegram. Actually, I still don't understand, why. I mean, everyone knows that it is Russian and actually there are many questions about its reliability. However, everyone continues to use it, all the news is there. All the chats are there. It is weird, but it is still so . . . My parents, for example, downloaded Telegram because all the news was there. So it was really a matter of security for us.

The ubiquitous use of Telegram is controversial, to say the least. Its origins stem from Russia. Telegram founder Pavel Durov created and used it to manage Russian social media VKontakte (which is under Mail.ru control starting from 2014). Telegram was blocked in Russia in 2018, but the blocking was lifted in 2021 for a publicly unknown reason (Avdieieva, 2022). Journalists revealed that Telegram was used by Russia to create local Telegram channels which pretended to be Ukrainian but disseminated fake news and Russian propaganda – they revealed at least 120 such channels having been created in the first weeks of the full-scale invasion aiming at the cities and towns where the Russian army was advancing (Drozdova et al., 2022). More worrying, however, is the amassing of information and personal data (e.g. 'eVoroh' spotting function of 'Diia' leads the user to a Telegram chat-bot where one can insert information) whose further storage and use is unknown (Avdieieva, 2022).

What accounts then for the enormous popularity of Telegram in wartime Ukraine? Interviews, as well as an expert brainstorming[2] which took place in October 2023, helped shed light on this. To begin with, Telegram offers unique functions no other social media have. One can set up a channel and stream information and the audience can view it algorithm-free. Whereas, for example, Facebook or Instagram algorithms decide which

content the user sees first, last or not at all, on Telegram one can view full content of all their subscriptions. In addition, it offers hundreds of news channels. The information there may lack verification but seems to give the users a sense of security, driven by access to 'exclusive' information – for example, about what type of air threat is incoming (a missile or a drone) and from which direction. Another instance of Telegram use reported by a journalist-interviewee is for monitoring the informal Russian Telegram chats and groups: 'Russians created a lot of military groups on Telegram, dedicated to the war. Monitoring of these groups [in combination with Ukrainian sources] allows more or less balanced information to be obtained [about the situation on the frontline].' One interviewee also mentioned that Telegram is useful for transferring large files without condensing them. Still others explained that they just used the messenger which was already in wide use by their personal network before the full-scale invasion.

Results IV: Digital security

According to the results of the survey, 82 percent of the respondents consider data security and privacy as important or very important. However, there seems to be a rather loose understanding of what exactly is meant by data protection, with the respondents resorting (or not) to various measures at will. When asked, which mobile applications (if any) they rejected after 24 February as not secure enough, 89 percent answered 'none', followed by a margin of error figures (around 2% each) for Viber and WhatsApp. However, when asked which of the mobile applications they used after 24 February were more secure than others, the respondents named Telegram as the first option. The in-depth interviews reveal some strategies to ensure the confidentiality of the information exchange, such as using the disappearing messages function in Signal or WhatsApp. As Table 2 reveals, Signal also belongs to the top five applications which the respondents started to use after the full-scale invasion. The interviewees explained that Signal was most often used for communication with the military. One interviewee described Signal as 'the national security standard'.

This trade-off between a potential digital threat and the immediate probability of not getting things done was also illustrated in the interviews:

> I think that the proximity of physical threat encouraged us not to think about these [digital] threats. So since we had this infrastructure in this social medium [Telegram], we just used it, taking it for a smaller danger in comparison to a missile which can hit you or humanitarian aid not delivered in time.

Results V: When smartphone and resilience do not come together

The above-mentioned manifold functions of the smartphone – information storage, dissemination and connection – can all become a potential source of danger and insecurity. The gravest condition for it, reported by the interviewees, is the case of a real or potential Russian occupation: 'I realized that if I end up under occupation, my smartphone [contents] totally gives me, my actions, my connections, my photos, my contacts, etc. away. Most likely it would mean a death sentence for me.'

The interviewees admitted that they would have to, or did in fact, have to get rid of all the digital content which could disclose their pro-Ukrainian position or activities, or that of other people: 'I had to delete all the pictures of the demonstrations [against the occupants], about something like this. Delete everything, so that they can't find it.'

An interviewee who survived the occupation also shared that they bought another phone to take outside while the 'real' phone would be stored and used only at home.

Yet another respondent reflected on the geolocation function, which can be used by the enemy to locate the person or a base (when many phones are switched on), 'so when I know the phone can be intercepted, I just switch it off.'

Other negative effects of the smartphone reported by the interviewees concerned psychological effects: information addiction, anxiety, the possibility of being an object of manipulation, disinformation and fake news. Several interviewees mentioned their need of restricting information for themselves, prioritizing some social media and news channels over others:

> I want to switch to some 'information diet' now, reading the news one-two times a day, in the morning and in the evening. Because when you follow everything, it paralyzes you, you're immersed in the news all the time. I want to distance myself a bit to be more productive.

Perhaps the bottom line of the case of the smartphone being a double-edged sword is best summarized by an interviewee who said: 'We often use the phone as a weapon and as a resistance [tool] but it is also a weapon which is used against us to break our resistance.'

Discussion

The results of our exploratory analysis paint a revealing picture of the role the smartphone can play for civilians in war. Firstly, our research demonstrates that smartphones are a fully-fledged tool for civic resilience in the face of the foreign military invasion owing to the internet access they provide, their wide array of multifunctional applications and their mobility. They empower users through connection to people and information beyond geographical boundaries, converting them into a 'resilience hub' and comprising many new functions which were absent or limited in relatively peaceful times, like becoming a mobile office, an online volunteer (frontline logistics and procurement) hub, an air threat warner, a first-hand news source, etc. In a horizontal resilience network, every smartphone becomes a node of information reception and dispatch.

While civilian access to digital warfare is confirmed as challenging the traditional state monopoly on the use of force, our research takes this point further. It demonstrates that state and society exchange information through smartphone applications, helping each other's resilience and sustainability. The state smartphone application 'Diia', acting as a simultaneous hub of information provision and reception, features prominently among the top applications used by our respondents in the aftermath of the Russian full-scale invasion. This is the novelty that the Ukraine's case contributes to the studies of digital space in warfare and civic mobilizations.

Our research also revealed the 'dark side' of the smartphone in wartime. We found that under life-threatening circumstances users choose disconnection, rather than connection. Kaun and Treré (2020: 707) described this phenomenon as 'disconnection as resistance', which they define as 'the use of tactics that force adversaries to disconnect, along with the (almost) complete eschewing of digital media and the partial disconnection from specific platforms as forms of political resistance'. Kaun and Treré refer to peacetime conditions in their research but the definition is also fully applicable to war time. Switching the phone off, erasing all the data on it, and/or using a substitute 'empty' phone were strategies reported by citizens who experienced the occupation or were physically close to the frontline. The intensified datafication (Couldry and Hepp, 2017) seems to be an inevitable consequence of mass personal data dispatched to platforms and applications. While it was an acceptable trade-off for the respondents in view of more immediate threats, this is a tendency which could potentially hinder civic resilience in the long run.

Last but not least, the present research reveals the 'smartphone as a weapon' narrative as problematic. While the proliferation of the 'citizen-soldier with a smartphone' metaphor (Patrikarakos, 2017) can be appealing, the extent of the civilian participation in warfare should be viewed as a continuum and not used to conflate the meaning and value of different roles in a war. Boichak and Hoskins (2022: 7) rightly argue that 'each user may choose or be drawn into participating in wars in a myriad of ways, yet this participation does not make them equally positioned with regard to the devastation and suffering brought about by warfare.' The smartphone may be an empowering tool in wartime, but it can, however, both be targeted against the owners themselves, or used by the owner to target the adversary, depending on the conditions.

Conclusion

Based on the quantitative survey and qualitative interviews, our research confirms the assumption of the smartphone's instrumental role in Ukraine in response to the full-scale Russian invasion and makes yet another contribution to our knowledge about digital warfare. The smartphone not only allows civilians to adapt to living in conditions of constant threat and power shortages but also enables them to respond and support the defence from the rear, engaging those not in the armed forces or are even abroad. Thus, the smartphone becomes a crucial resilience tool, allowing adaptation, positive functioning and coping under extreme circumstances such as an invasion.

While the smartphone becomes an 'online resilience hub' and a node in the horizontal societal resilience network, it can simultaneously be a source of anxiety for its user and even put their lives in danger due to its function as a data carrier (in the case of foreign military occupation) or a signal emitter (potentially even being located by the adversary's radio location system close to the frontline). Further research into the role of the smartphone in warfare would be welcome in other settings. Moreover, the 'malevolent' nature of the smartphone, as opposed to its empowering and 'benevolent' functions, remains hitherto overlooked and merits scholarly attention in further 'smartphone studies'.

Acknowledgements

The authors would like to thank Roman Horbyk, Inna Volosevych and Tetiana Kostiuchenko as well as the anonymous reviewers for their valuable comments on earlier drafts of this paper.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work has been funded by the LOEWE initiative (Hesse, Germany) within the emergenCITY center.

ORCID iD


Kateryna Zarembo https://orcid.org/0000-0002-0101-3183

Notes

1. The figure does not reflect how the experience of returning to the original place of residence (which was reported by about half of those who experienced displacement) affected the use of smartphone applications.
2. The expert brainstorming, comprising some 20 experts in digital resilience of Central and Eastern Europe and the Baltic States, took place during the interdisciplinary workshop "How to Be Prepared? Governance for Societal Resilience in the Baltic Sea Region and Eastern Europe", which took place on 12–13 October 2023 at Södertörn University, Sweden. During the workshop the participants exchanged their views and experiences regarding the popularity of Telegram in Ukraine.

References

Asmolov G (2021) From sofa to frontline: The digital mediation and domestication of warfare. *Media, War & Conflict* 14(3): 342–365.

Asmolov G (2022) The transformation of participatory warfare: The role of narratives in connective mobilization in the Russia–Ukraine war. *Digital War* 3: 25–37.

Avdieieva T (2022) Non-star wars: Social media in the times of armed conflict. Center for Democracy and Rule of Law. 27 September. Available at https://cedem.org.ua/en/analytics/sotsmerezhi-zbroyni-konflikty/ (accessed 15 January 2024).

Bartkowski M (2015) Nonviolent civilian defense to counter Russian hybrid warfare. The Johns Hopkins University Center for Advanced Governmental Studies.

Boichak O (2017) Battlefront volunteers: Mapping and deconstructing civilian resilience networks in Ukraine. In: #SMSociety'17: Proceedings of the 8th International Conference on Social Media & Society, Toronto, 28–30 July, 1–10. New York, NY: Association for Computing Machinery.

Boichak O and Asmolov G (2021) Crowdfunding in remote conflicts: Bounding the hyperconnected battlefield. In: Selected Papers of #AoIR2021: The 22nd Annual Conference of the Association of Internet Researchers (held online).

Boichak O and Hoskins A (2022) My war: Participation in warfare. *Digital War* 3: 1–8.

Boichak O and Jackson S (2020) From national identity to state legitimacy: Mobilizing digitally networked publics in eastern Ukraine. *Media, War & Conflict* 13(3): 258–279.

Booth K (1997) Security and the self: Reflections of a fallen realist. In: Krause K, and Williams MC (eds) *Critical Security Studies: Concepts and Cases*. London: Routledge, 83–120.

Central Intelligence Agency (2023) Internet users. *The World Factbook*. Available at: https://www.cia.gov/the-world-factbook/field/internet-users/ (accessed 15 January 2024).

Couldry N and Hepp A (2017) *The Mediated Construction of Reality*. Cambridge: Polity Press.

Crawford E (2015) *Identifying the Enemy*. Oxford: Oxford University Press.

Drozdova Y, Dukach Y and Kelm N (2022) Telegram occupation. How Russia wanted to breed a media monster, but ended up with a paper tiger. *Texty.org.ua*, 15 November.

Eriksen TH (2020) Filling the apps: The smartphone, time and the refugee. In: Jacobsen CM, Karlsen MA and Khosravi S (eds) *Waiting and the Temporalities of Irregular Migration*. London: Routledge, 57–73.

Fitzgerald N (2014) From Ukraine's Independence Square, the art of the revolution. *The Washington Post*, 2 May.

Horbyk R (2022) 'The war phone': Mobile communication on the frontline in Eastern Ukraine. *Digital War* 3: 9–24.

Joyce M (2012) Five reasons not to use the word 'slacktivism'. *Open Society Foundations*. Available at: https://www.opensocietyfoundations.org/voices/five-reasons-not-use-word-slacktivism (accessed 15 January 2024).

Jung Y (2014) What a smartphone is to me: Understanding user values in using smartphones. *Info Systems Journal* 24(4): 299–321.

Kaun A and Treré E (2020) Repression, resistance and lifestyle: Charting (dis)connection and activism in times of accelerated capitalism. *Social Movement Studies* 19(5/6): 697–715.

Keenan L (2022) How Ukraine seized the initiative on the digital front of the war with Russia. Modern War Institute. Available at: https://mwi.usma.edu/how-ukraine-seized-the-initiative-on-the-digital-front-of-the-war-with-russia/ (accessed 1 June 2023).

Khamis S, Gold S and Vaughn K (2012) Beyond Egypt's 'Facebook revolution' and Syria's 'YouTube uprising:' Comparing political contexts, actors and communication strategies. *Arab Media & Society* 15: 1–30.

Korostelina K (2020) National resilience to protracted violence in Ukraine. *Peace and Confict Studies* 27(2): 4.

Krihel M and Lukashova S (2022) Persha informatsiyna viyna. Mykhailo Fedorov rozpovidaie, yak Ukraina vouie z Rosie una kiberfronti (The first digital war. Mykhailo Fedorov's account of how Ukraine is fighting Russia on cyberfront). *Ukrainska Pravda*, 27 June.

Ling R and Yttri B (2002) Hyper-coordination via mobile phones in Norway. In: Katz JE, and Aakhus MA (eds) *Perpetual Contact: Mobile Communication, Private Talk, Public Performance*. Cambridge: Cambridge University Press, 139–169.

Lokot T (2017) Public networked discourses in the Ukraine–Russia Conflict: 'Patriotic hackers' and digital populism. *Irish Studies in International Affairs* 28: 99–116.

Lorch J (2017) *Civil Society and Mirror Images of Weak States Bangladesh and the Philippines*. London: Palgrave Macmillan.

Malka V, Ariel Y and Avidar R (2015) Fighting, worrying and sharing: Operation 'Protective Edge' as the first WhatsApp war. *Media, War & Conflict* 8(3): 329–344.

Melchior J (2022) Civil society is Ukraine's secret weapon against Russia. *Wall Street Journal*, 4 April.

Merrin W (2018) *Digital War: A Critical Introduction*. London: Routledge.

Metzger M and Tucker JA (2017) Social media and EuroMaidan. *Slavic Review* 76(1): 169–191.

Myronova N (2022) Za chas povnomasshtabnoi viynu ukraintsi chastishe korystuiutsia zastosunkom Telegram, 17 June. Available at: https://speka.media/rosiiska-agresiya/za-cas-povnomasstabnoyi-viini-ukrayinci-castise-koristuyutsya-zastosunkom-telegram-9ezl19 (accessed 1 June 2023).
Narli N (2018) Life, connectivity and integration of Syrian refugees in Turkey: Surviving through a smartphone. *Gender of the Controversies* 33: 269–286.
Norris FH and Stevens SP (2007) Community resilience and the principles of mass trauma intervention. *Psychiatry: Interpersonal and Biological Processes* 70(4): 320–328.
O'Loughlin B (2020) Towards a third image of war: Post-digital war. *Digital War* 1(1): 123–130.
Onuch O (2015) 'Facebook helped me do it': Understanding the EuroMaidan protester 'Tool-Kit'. *Studies in Ethnicity and Nationalism* 15: 170–184.
Patrikarakos D (2017) *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*. New York, NY: Basic Books.
Puglisi R (2015) *A People's Army: Civil Society as a Security Actor in Post-Maidan Ukraine*. Rome: Istituto Affari Internazionali.
Rabinovych M et al. (2023) Explaining Ukraine's resilience to Russia's invasion: The role of local governance. *Governance*. DOI: 10.1111/gove.12827.
Rating Group (2022) The 8th national poll: Ukraine during the war, 6 April.
Rohde M et al. (2016) Out of Syria: Mobile media in use at the time of civil war. *International Journal of Human–Computer Interaction* 32: 515–531.
Schejter A and Cohen A (2013) Mobile phone usage as an indicator of solidarity: Israelis at war in 2006 and 2009. *Mobile Media & Communication* 1(2): 174–195.
Slovo i dilo (2021) Yak zminuvalasia chastka IT-haluzi v zahalnomu obsiazi VVP Ukrainy, 15 September. Available at: https://www.slovoidilo.ua/2021/09/15/infografika/ekonomika/yak-zminyuvalasya-chastka-it-haluzi-zahalnomu-obsyazi-vvp-ukrayiny (accessed 13 June 2023).
Steinbrink E et al. (2021) Digital privacy perceptions of asylum seekers in Germany: An empirical study about smartphone usage during the flight. *Proceedings of the ACM on Human–Computer Interaction* 5: 1–24.
StrategEast (2022) Ukrainian digital resistance to Russian aggression.
Tkach B and Williams AA (2018) Mobile (in)security? Exploring the realities of mobile phone use in conflict areas. *Information, Communication & Society* 21(11): 1639–1654.
Winther P and Nilsson PE (2023) Smart tactics or risky behavior? The lawfulness of encouraging civilians to participate in targeting in an age of digital warfare. The Hague Center for Strategic Studies.
Zarembo K (2017) Substituting for the state: The role of volunteers in defense reform in post-euromaidan Ukraine. *Kyiv-Mohyla Law and Politics Journal* 3: 47–70.
Zarembo K and Martin E (2022) Did Ukraine's civil society help turn back the Russians? *New Eastern Europe*, 4 May.

Author biographies

Kateryna Zarembo, PhD, is a visiting fellow at the Technical University of Darmstadt (Germany), a non-resident fellow at the Central European University (Vienna, Austria) and an associate senior fellow at New Europe Center (Kyiv, Ukraine). Her research interests sit at the intersection of international relations, security studies and civil society studies. Dr Zarembo is a recipient of a number of scholarships and awards, including Emma Goldman Snowball Award and Kyiv School of Economics Talents for Ukraine award. She has published widely in academic and policy outlets, including *European Societies, European Security, Problems of Post-Communism* as well as with New Europe Center and Carnegie Europe.

Michèle Knodt, PhD, is Professor of Political Science, Jean Monnet Chair (ad personam) and Director of the Jean Monnet Centre of Excellence 'EU in Global Dialogue' (CEDI), Director of the Jean Monnet Centre of Excellence 'EU@School', leader of the COST Action 17119 'EU Foreign Policy facing new Realities (ENTER), Co-leader of the LOEWE Centre of Excellence 'emergenCITY', and Co-leader of the DFG Research Training Group 'Critical Infrastructures'. She serves as Research Area Leader of the Cluster Project 'Clean Circles' and Research Area Leader in the Kopernikus Project 'Ariadne – Evidence-Based Assessment for the Design of the German Energy System Transformation' and leader of smaller cooperative and interdisciplinary projects. She has published widely on EU multi-level governance, is especially interested in resilience and emergency topics as well as energy and climate governance and has received research grants from the German Federal Ministry of Education and Research (BMBF), German Federal Ministry of Economic Affairs and Energy (BMWi), the German Research Council (DFG), the Volkswagen Foundation and the European Commission.

Address: Technical University of Darmstadt, Karolinenpl. 5, Darmstadt 64289, Germany. [email: knodt@pg.tu-darmstadt.de]

Jannis Kachel, MSc, is a research associate at the Technical University Darmstadt.

Address: Technical University of Darmstadt, Karolinenpl. 5, Darmstadt 64289, Germany. [email: jannis.kachel@gmail.com]