"It's like an explosion": Cyberwarfare harms for civilian population in Ukraine during the Russian invasion

OKSANA KULYK and JARI KICKBUSCH, IT University of Copenhagen, Denmark
PETER MAYER, University of Southern Denmark, Denmark and Karlsruhe Institut für Technologie, Germany

Studies on civilian costs of cyberwarfare operations are crucial in understanding how to protect the population in large-scale cyberattacks conducted by state actors. In this preliminary study, we conduct interviews (N=5) focusing on the harms experienced by Ukrainian civilians due to Russian cyberwarfare operations since the start of the full-scale invasion in 2022 as well as mitigation measures for protection of the civil society. The findings include harms such as lack of information, lack of access to essential services, physical harms, anxiety and lack of trust in the government. The study shows that cyberwarfare operations have the potential of causing severe harm to civilians and that there is a need for future studies to be conducted and adopted by institutions in order to develop measures to mitigate, not only in Ukraine but in any countries in risk of such attacks.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**.

ACM Reference Format:
Oksana Kulyk, Jari Kickbusch, and Peter Mayer. 2025. "It's like an explosion": Cyberwarfare harms for civilian population in Ukraine during the Russian invasion. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3706599.3719906

1 Introduction

Much research on cyberwarfare centers discussions around weapon systems and military or strategic infrastructure as well as defenses against such attacks. Correspondingly, the conversations around cyberwarfare tend to center on the strategic effects of cyber operations, i.e., the ability to help the belligerent parties to achieve their desired military objectives. Meanwhile, the civilian costs of cyberwarfare operations remain understudied. Such studies, however, is crucial in understanding how to protect the population in case of large-scale cyberattacks by a hostile state actor, especially given the overall importance of research on human factors in cybersecurity. The study presented in this paper represents a first step in closing this research gap by conducting a preliminary qualitative study investigating (a) the harms experienced by Ukrainian civilians due to offensive cyberwarfare operations conducted by Russia in Ukraine since the start of the full-scale invasion in 2022, and (b) civilians' and government institutions' perception of the harms as well as the efficiency of the protection of the civil society. Namely, we focus on the following research questions:

RQ1 What are the harms caused to the civilian population via cyberwarfare activities?
RQ2 What mitigation measures have been applied to recover from harms?

We identify a number of harms caused to the civilian population by cyberattacks attributed to the Russian government or pro-Russian groups, including *primary harms* such as lack of information or lack of communication, and *secondary*

Authors' Contact Information: Oksana Kulyk; Jari Kickbusch, {okku,jark}@itu.dk, IT University of Copenhagen, Copenhagen, Denmark; Peter Mayer, mayer@imada.sdu.dk, University of Southern Denmark, Odense, Denmark and Karlsruhe Institut für Technologie, Karlsruhe, Germany.

Manuscript submitted to ACM

harms resulting from primary harms, such as physical harms or decision interference. We furthermore identify a number of measures aimed to mitigating harms, applied by authorities as well as individuals. Our results show that attacks aimed at information infrastructure can have a damaging impact on civilians, stressing the importance of developing both legal frameworks and crisis management measures to remedy such impact. In particular, our findings indicate the importance of timely and actionable communication both between authorities tasked with mitigating the attacks and between authorities and general population, provided reassurance and actionable guidelines. Our findings furthermore indicate the importance of local communities used for mutual reassurance, information sharing and support.

2 Background

Over the course of the last three decades, the definition of cyberwarfare has been subject for much discussion [2]. In particular, cyberwarfare has been commonly defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" [4] or "affecting data by using data" [24]. As our goal in this work is to understand the civil costs of such disruptions, we consider a broader outlook, including kinetic attacks that impact information infrastructure as well. In particular, we look at cyberwarfare activities against Ukraine which are attributed to Russia, including suspected individual attackers or pro-Russian hacker groups without an official affiliation to the Russian government.

Cyberwarfare in practice. Cyberspace offers nation states a battlefield in a grey zone where cyber attacks are launched with the specific objective of achieving strategic outcomes without the need of armed attack [11]. Among the most well-known examples on such attacks are NotPetya in 2017 [10], a destructive malware seeded in the Ukrainian IT infrastructure from where it spread across the world crippling thousands of businesses. Cyberwarfare can also serve as component or weapon in kinetic warfare and other armed conflicts, which we will focus on in this paper. An early example of that is the second Iraq war in 2003 where the US army attacked the military and civilian IT systems to make the kinetic attack easier and further used cyber-attacks to distribute e-mails and propaganda on internet media that aimed to demoralize the enemy, in place of former practise of dropping pamphlets [4].

In Ukraine, cyberwarfare has been a component in the confrontation with Russia since the Revolution of Dignity in 2013-2014 [7]. The intensity of cyberattacks has furthermore increased since the full-scale invasion in 2022, with 2544 serious incidents recorded in 2023 by the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) [25]. The main targets of these attacks were in the energy sector, the telecommunication sector and IT, banking and software services. The SSSCIP report from 2024 [26] furthermore categorises attacks by their goals, which include destructive attacks leading to deletion of data or damage to systems, disruptive attacks impacting the connectivity and availability of vital services, espionage attacks, and disinformation attacks. Of particular relevance for our work is the attack on Ukraine's biggest telecommunications operator, Kyivstar, that left millions of users without mobile signal and internet for days in December 2023 [26, 29].

Impact of cyberwarfare on civilians. The intense use of cyberattacks as a means of warfare, has raised concerns about harm and impact caused to the civilian population, and the protection of civilians and civilian infrastructure, which are affected by both kinetic and cyberattacks [6]. As such, protection of civilians has been considered within the context of international law [22], and the Tallinn Manual [33] has been proposed as a legal framework for considering international law issues related to cyberoperations. Within recent years, representatives from organisations such as the International Criminal Court [17] and International Committee of the Red Cross [14] furthermore expressed concerns over the potential human cost of cyber operations.

At the same time, with cyberwarfare being an emerging research field, there is currently a gap in understanding the human impact with much of the literature focusing on understanding and conceptualizing the technical, political, legal, and military aspects [4, 16, 40]. Nonetheless, relevant insights can be gained from broader studies which have been conducted in the field of crisis informatics that are helpful in understanding how technologies, including social media, are used for crisis management [5, 12, 13, 19, 20, 27, 30, 31, 38, 39]. As such, a number of works focused on social media activities around the Russian annexation of the Crimea and the full-scale invasion in 2022 [9, 18, 21, 23, 28, 34], highlighting e.g. pro-Russian disinformation campaigns or investigating the way journalists use social media for their reporting. Of particular relevance for our work is the study by Schmuser et al. [34] that investigates security and privacy advice related to the Russian aggression after the full-scale invasion, exchanged over English-speaking social media. The results show a lack of advice prioritization, deemed to be especially detrimental during times of crisis, indicate an importance of offers for individual support published via social media as well as identify misinformation as a rising threat in general and for security advice specifically. A study by Shklovski et al. [35], furthermore, describes a study involving a field trip to Eastern Ukraine in 2018 (that is, before the full-scale invasion in 2022, but after the Crimea invasion and start of armed conflict in the region in 2014). The study shows that private mobile phones and computers became a crucial but ambiguous infrastructure despite the lack of durability in the extreme conditions of a military conflict as well as their government and military surveillance potential. The participants in the study relied on a combination of myths and significant technical knowledge to balance the possibilities mobile technologies offer and the life-threatening reality of enemy surveillance they engender. A few studies furthermore have focused on more technical aspects of cyberwarfare and investigated and presented methods for strengthening Cyber Situational Awareness (CSA), and the resilience of the internet in Ukraine [36, 41].

Cyber-harms and cyber risk management. A taxonomy of cybersecurity harms has been proposed by Agrafiotis et al. [1], defining such harms as "damage that arises as a direct result of an attack conducted wholly or partially via digital infrastructures, and the information, devices and software applications that these infrastructures are composed of". The authors define the categories of physical/digital (including both damage to data and bodily injuries), economic, psychological, reputational and social/societal harms. Similar taxonomy has been proposed by Citron and Solove [3] focusing on privacy harms, suggesting categorising such harms into physical, economic, reputational, relationship, discrimination, psychological and autonomy. Both of these works note a number of challenges in analysing corresponding harms, such as difficulty in estimating harms that are not easily quantifiable, or the complexity of considering harm propagation, i.e. as indirect harms from an initial attack or data breach including potential future consequences.

Assessing both the impact of a potential cyberattack, as the harms caused to the affected organisations, individuals or society as a whole, and the likelihood of such an attack, is an important component of cyber risk management frameworks [15, 32]. Empirical data from real-world attacks is commonly used as a source of such assessment, e.g. using data from cyber incidents and affected organisations or individuals (e.g. as case studies) for analysing the factors affecting the probability of an organisation being a target of a cyberattack, or the impact of cyber-incidents, including long-term effects [8].

3 Methodology

We conducted semi-structured interviews ($N = 5$) with people living in Ukraine. The focus of our interviews were experiences of attacks that, as our participants believed, were conducted as a part of general warfare either by Russian government or pro-Russian non-governmental groups. Two of the participants (P1, P2) were civilians and three (P3, P4,

P5) were employees of government organisations. All of the interviews were conducted in Kyiv, the capital city, and all of our participants were residents of Kyiv, with one participant (P1) being a refugee from her home town of Mariupol due to the occupation by Russian forces. Two of the participants (P1, P2) were women, the rest (P3, P4, P5) were men.

Recruitment. The participants were recruited through our personal contacts, including contacts with people who were involved with cybersecurity-related activities in Ukraine and had connections with both governmental and non-governmental organisations. The goal of the recruiting was to reach out to individuals or organisations who either had personal experiences of being affected by cyberattacks or were involved in defending against cyberattacks or mitigating their impact.

Analysis. Our interviews were conducted in Ukrainian and English with translator present. The transcripts of the interview were edited and the original statements of participants translated from Ukrainian to English for the purpose of the analysis by one of the authors of the paper who is a native Ukrainian speaker. The resulting translated transcripts were analysed by two paper authors using an open inductive coding approach.

Ethical considerations. Our participants were presented with a consent form, informing about the goals of our research and that their interviews will be used in both academic and media publications, as well as ways in which their data will be processed and their rights regarding it according to the GDPR. The form was made available to the participants in both English and Ukrainian, and the participants were offered to ask questions if anything in the form was not clear or concerning to them. For meetings with employees of governmental organisations, accreditation from the Ukrainian government was obtained beforehand.

Positionality statement. While we, the authors of this paper, have seeked objectivity in this study, we are at the same time acknowledging our support to Ukraine in its fight against Russian aggression. This is also in line with the support expressed by the government of the country we reside and are employed in. Further, one of the paper authors was born in Ukraine and has family there, being familiar with the culture and having personal experiences related to the on-going war.

4 Results

We report on our findings on both, harms of cyberwarfare operations and mitigation measures against these harms. Note that for the sake of this work, we consider harms to be what our participants mentioned as harms.

4.1 Harms of cyberwarfare operations

Our analysis reveals primary harms, i.e., harms directly caused by an attack, and secondary harms that stem from one or more of the primary harms.

4.1.1 Primary harms. The primary harms mentioned by our participants include a lack of information, lack of communication, lack of access to essential services, disclosure of sensitive information, impersonation, and disruption of activities.

Lack of information. Participants mentioned being unable to access information, e.g., due to network outages (caused by either Ddos attacks or kinetic attacks damaging IT/communication infrastructure) or censorship induced by the occupying government: *"There is an example of information collapse, you are in an information vacuum. You don't understand what's going on. [..] We did not understand what is going on around us, in the city, in the country." (P1).* Such

a lack of information has also been accompanied by *disinformation*, spread by Russia, in an attempt to control the population in the occupied territories or force decisions from the population, e.g., to collaborate with the occupiers: *"When the Russian soldiers started communicating with us, they told that Ukraine, Kyiv has fallen, and no one is waiting for you. This was the first information, when we were told that there is nothing" (P4).* Another aspect related to lack of information is the ability to get information during a crisis, e.g. being able to understand what is happening, what needs to be done and what to expect. Not being able to get such information can lead to worsening of the anxiety: *"Shock and not realizing how long this could go on. I mean, there was uncertainty. We didn't get any information." (P2)*

Lack of communication. Disruptions in communication services were furthermore named as the source of harms. As such, our participants mentioned not being able to communicate with their family to tell them they were safe following the Kyivstar cyberattack (see Section 2) that resulted in outages in mobile communications (*"I wanted to call my mom and I couldn't do it" (P2)*), or on occupied territories, not being able to reach out to anyone in Ukraine because of censorship (*"You could call, but only to Russia, not to any Ukrainian number, only to Russian ones." (P1)*).

Disclosure of sensitive information. As certain population groups (e.g. activists) are specifically targetted by combatants, disclosure of information about such groups can be critical. As such, a participant who was involved in local politics mentioned being wary of providing her identifying information to the occupiers, even if it was required from her in order to receive humanitarian aid: *"But to get food, you need to show your passport. This is why I gave my passport as the last one in the family, because I did not want them to take note. I did not want that, because I worked with the government." (P1).* The same participant also mentioned leakage of a database with personal data of other activists: *"This database was hacked, and given to the occupiers. By collaborators. So the key point here is that the database of our registrations, email addresses, all was given away." (P1).*

Lack of access to daily tasks and services. As a result of cyberattacks focused on disruption of critical services (such as the Kyivstar cyberattack), people reported their daily tasks interrupted (e.g. not being able to do their work) or not having access to essential services, such as buying groceries, taking their car, conducting bank operations or accessing healthcare services. One respondent reports not being able to get medical help for her sick relative due to communication outage in Kyiv: *"We go in, we make an appointment with the doctor [..] we go through [communication system affected by the attack], I could not do it." (P2).* Another respondent mentioned disruption of the air raid alert service (*"You have, in some areas we had no air alerts, because no connectivity" (P5)*) and of banking operations as well as other operations requiring two-factor authentication: *"You need a verification sent through a mobile, and without a mobile, without a financial phone number you are basically blocked from any financial transactions, which radically decrease the quality of life, to be honest." (P5)*

Impersonation. Impersonation of both individuals and organisations has been mentioned as a result of either hacking attacks, disinformation campaigns or attackers getting physical access to the victim's devices and thus, to their accounts. Such attacks can be furthermore accompanied by *disinformation.* As such, our participants describe two incidents of attackers spreading false statements on behalf of high-ranked Ukrainian officials (*"the Russians hacked several websites and posted an announcement there. It was Zaluzhny's* [1] *appeal to the military [to convince them to surrender]" (P4)*), or hacking into the news channels and replacing the broadcast feed (*"hackers hacked into a satellite with a [Ukrainian TV channel] signal and put Russian content there" (P4)*). While the aforementioned incidents were aimed at a broad

[1]Valeriy Zaluzhny was at the time the Commander-in-Chief of the Armed Forces of Ukraine.

audience, another incident on a smaller scale was mentioned by one of the participants, describing impersonation of members of an activist organisation either via direct contact (*"they [the Russians/local collaborators] knew that we are [the activist organisation] and started to write to some members of [activist organisation] [..] asking them to come back to [an occupied city], there will be a new DPR* [2] *[activist organisation] created here" (P1)* or social media (*"A member of [activist organisation], she fled her house and left her tablet there [..] someone was writing from her account in social media, Telegram, Facebook." (P1)*)

4.1.2 Secondary harms. The secondary harms include physical harms, anxiety, lack of trust in government and decision interference.

Physical harms. Participants reported experiencing or risking physical harms as the result of the primary harms. As such, abuse by the hands of occupying authorities was reported as the result of sensitive data disclosure, as people fleeing the occupied city had to go through checkpoints controlled by the Russian forces: *"When [members of an activist organisation] left [the city], because they were [members of an activist organisation], especially the guys, were very severely beaten, almost to death." (P1).* The same participant reported having to risk their lives by going outside during the bombing of the city, in order to get information about the current situation from the people fleeing past them: *"It was a risk for us to go out in the open. [...] we could just stay in the cellar. But we went out to talk, to find [something] out." (P1).* Another participant in Kyiv reports deterioration of health of her sick relative, as she was not able to get healthcare for her because of communication outages: *"Let's say we don't get a bandage change for three days, that's it, it's already worsening [...] this deterioration, it turns out, led to the fact that I had to think about surgery." (P2).*

Anxiety. People reported being in a fragile mental state due to general uncertainty and the need to adapt to a new situation: *"it was the feeling same as to when rockets fly [..] it's like an explosion. [..] you are paralyzed, you have to adapt, to understand what you need to do, what you need to fix, who you need to help, who you need to save" (P2).* Not knowing what is happening and not being able to reach out to their friends and family left people similarly anxious: *"When you are sitting without information, it cannot even be described. You are just alone by yourself. So that you don't lose your mind." (P1).* Further anxiety is caused by uncertainty about what to expect, e.g., in terms of future attacks: *"And after the hacking of Kyivstar, there were great fears in society, including both Kyiv residents and [governmental institution] employees. There were fears that other mobile operators could be hacked, not only mobile operators, but also energy operators. [...] So there are such fears. And this is what I was talking about, the element of panic." (P3)*

Lack of trust in the government. Our participants mentioned how visible effects of cyberattacks can cause panic among the population and their distrust in governmental services. This effect can be amplified in case of disinformation, e.g., spreading narratives in absence of access to information refuting them: *"Such attacks, when the website of authorities, any kind of authorities, is shut down, the goal is to show that the authorities are no longer functioning. It is like a signal. And this is exactly the purpose of such attacks: to show that any government agency is no longer functioning. And this is a threat, a panic. This is exactly what such attacks are aimed at." (P3)*

Decision inference. The role of attacks in attempting to influence decisions of Ukrainian people, including military, has been mentioned by several of our participants. As such, censorship and the resulting disinformation on occupied territories was mentioned as a way to control the local population: *"In the conditions of this complete information*

[2]Donetsk People's Republic was a separatist state, later claimed by Russia to be a part of Russian territories, established on occupied parts of Donetsk oblast in Eastern Ukraine

isolation, the people of [occupied city] were told that Russian tanks were already near Lviv [3]*, and when people did not have complete information, they made decisions about how to survive. They made decisions in favour of the Russians." (P4).* The participant furthermore mentioned that such decision interference can be plausibly considered to be one of the main goals of cyberattacks: *"The main goal of behavioural change is to make Ukrainians, first of all, not trust the government, the military, politicians. First, and second, that they stop armed resistance to the Russian army. These are the two main narratives. That's why these cyberattacks are being carried out." (P4).*

4.2 Harm mitigations

Our participants reported both measures conducted by the authorities to mitigate harms, as well as different ways they themselves or their community coped with the impact.

4.2.1 Authorities. Our participants mentioned mitigation measures conducted by authorities as mitigating actions aimed at detecting and stopping an attack, as well as communication of relevant information about the attack to the population.

Mitigation actions. Our participants mentioned actions aimed at detecting and mitigating ongoing attacks, stressing the importance of a timely reaction: *"If we hadn't fixed the situation quickly, maybe there would have been consequences" (P3).* Well-established collaboration between different governmental and non-governmental agencies (*"the State Special Communications Service, the Security Service of Ukraine, the cyber police. If it concerns a particular ministry or department, they report it. Then, of course, the media is involved. All possible media are involved, as well as NGOs working in the field of cybersecurity" (P4)*). The involvement and help of private companies (*"We collaborate with the multiple companies, including Microsoft. They recognize the expertise they are willing to share information and that's bidirectional exchange of information." (P5)*) and international partners (*"all of cybersecurity, it's a team sport. No single country can do it by itself." (P5)*) were also mentioned as crucial component of a successful national cyberdefense.

Communication. Proper communication to the population has been mentioned as a critical component by both civilians and government employees among our respondents. As such, following up on the attack on Kyivstar, one respondent noted the importance of the communication by the company about the status of the mitigating measures had: *"it's important to have information, what it is, how long it will last, and some recommendations, let's say, what you can do [..] And then the information started to come from Kyivstar, when there will be restoration [..] on a certain day we can send SMS, on a certain day, when there will be connection." (P2).* Providing guidelines to the population has furthermore been mentioned, either as a warning not to spread disinformation (*"Be careful, don't jump in this Telegram, fake news from some unknown source, because only from us you will receive proper information. And it actually stopped this propaganda wave which they planned."* (P4)) or regarding specific recommendations on how to mitigate the impact of an attack, such as getting a SIM card from a different mobile operator (*"We made graphic explainers, video, text statements and disseminated as much as possible, how to recover from this situation, that is, explaining to people the algorithm on how to do it"* (P4)). Such communication furthermore was not limited to a time of a crisis only, instead participants reported implementing on-going efforts to inform the population about security risks and protection measures (*"General public awareness about cyber security and cyber hygiene [..] We have short videos published [on an online education platform], and we work on more courses to be published that are for teenagers, for mature adults, for specific public servants, etc." (P5)* as well as about preparedness measures that can mitigate the impact of an attack (*"Before the war, we launched this*

[3]Lviv is a city in the western part of Ukraine far away from the frontlines

advice, in case of war, or emergency situations [..] One of the recommendations was to buy radio stations. [..] We need to diversify the phone connection, radio stations, other sim cards... we prepared people in advance." (P4)).

4.2.2 Individuals.

Risk-avoiding behaviour. As a reaction to incidents and harms that they experienced, our participants mentioned engaging in behaviour aimed to mitigate risks of these harms. Such behaviour included behaviour during the crisis, such as refusing to share their personal data with occupation authorities or getting rid of personal items that can contain sensitive information (*"we hid or burned our [member cards of an activist organisation] so that we don't show them." (P1)*), as well as change of attitude affecting their behaviour after the crisis: *"I pay attention to the fact that we should also think about the security of the programs that are in the phone." (P2)*, *"We understood that everyone can be attacked. One just needs to be careful, what you share, where you go, which website." (P1).*

Use of tools and services. To deal with communication disruptions, our participants mentioned relying on alternative communication channels such as getting a second SIM card or using internet-based services to make calls (*"But thanks to friends who told me that one can get online, for example, a SIM card of another provider [..] you can use Telegram for phone calls." (P1).* In particular as a low-tech solutions, use of landline phones in particular for emergency calls was mentioned: *"As [doctors] said at the time, what saved us in that situation, we were left with these [landline] phones [..] the phone was ringing all the time." (P2).* A general strategy of having backup options and *"diversifying risks" (P4)* was furthermore mentioned.

Community support. Participants reported relying on their local community, e.g., getting help or advice from friends and neighbours: *"If an extreme situation happens, we raise our heads and look, we exchange information not so much electronically, but among ourselves, as it can be. [...] I mean people from the another phone company just gave their phones [to people] and said call whoever you need to call, call whoever you need to call." (P2).* Such involvement of the community has also been the source of comfort in times of crisis: *"There was a lot of emotion, there were a lot of tears and there was something that was a sense of admiration. Why? Because of how people self-organize." (P2).*

5 Discussion and conclusion

The results of our study show that cyberwarfare operations and attacks on information infrastructure have the potential of causing harms to the civilian population. These harms varied in both their type, covering multiple categories from cybersecurity and privacy harm taxonomies [1, 3], and in the impact depending on the nature of the attack and the affected population groups, ranging from relatively minor inconveniences (e.g. having to buy a second SIM card) to more severe consequences threatening one's life or physical health. Nonetheless, some of the harms identified in our study might seemingly have a minor direct impact on civilians, yet can potentially lead to more damaging chain reactions. This is in line with the arguments from previous research stressing the complexity of indirect and long-term harm estimation [1, 3]. As such, disinformation directed at military officers might go unnoticed by civilians at first, but would, if successful, have an impact on the state's capability in defending against a military invasion. Similarly, an outage of a government website can contribute to overall lack of trust towards the government, which further might potentially lead to a political turmoil, even if the website itself is of little significance for most citizens' daily lives. Considering potential cyberwarfare harms and their mitigation measures is therefore of crucial importance not only in Ukraine but in other countries that might be at risk of such attacks.

Some of the harms we identified have furthermore been mentioned in previous research, most particularly, disinformation. In our results, disinformation has been presented both as the main goal of the attack (e.g., as a disinformation campaign as spreading false narratives over social media appears to be the main goal of the attack) or as being particularly enabled by a primary harm (e.g., in cases of impersonation or spreading of false information after blocking communication with reliable sources).

Our results stressed the role of communication in harm mitigation, both on the part of the authorities and in discussions between the citizens, including social media. In particular, our results comprised three out of four cooperation modes from the Crisis Communication Matrix [31]: authorities to authorities (talking about importance of collaboration and timely communication), authorities to citizens (communication of mitigation status and guidelines) and citizens to citizens (exchanging information). The citizens to authorities mode was not mentioned in our interviews. However, the extent to which authorities rely on information or feedback from citizens to mitigate the impact of cyberattacks remains a promising direction for future investigations. Future research also needs to look at ways to facilitate this communication, both in exchanging information between citizens while avoiding misinformation or disinformation, and in communication from the authorities, making sure that it effectively serves a role in reassuring citizens and providing them with actionable advice. The role of societal trust in such communication, including trust of citizens in authorities, needs further to be considered.

While some of the discussed attacks can be attributed to pro-Russian groups with a high level of confidence (e.g., by said groups claiming responsibility), the attribution of other attacks is more challenging, which is a known problem due to a variety of methods attackers can use to avoid being detected or to shift the blame on another party [37]. Even if an attribution is made by authorities, the extent to which evidence can be communicated and understood by the general public is often challenging to estimate. The question of attribution, however, is crucial not only for establishing and maintaining trust between the population and the government, but also for being able to establish legal evidence that can hold up during prosecution. The latter is in particular relevant for the development and implementation of legal frameworks aimed at the persecution of cyberattacks that might be deemed as war crimes.

Limitations. Being a preliminary study, we had a limited sample of a small size, consisting of people with a general pro-Ukrainian position living in the capital region and connected to us via our personal networks. Future studies therefore would recruit a more diverse sample of people impacted by cyberwarfare activities, including doing studies in smaller towns or areas that suffer a more significant impact of the war (e.g. being close to the frontline or experiencing Russian occupation), where the reach of Ukrainian authorities and overall access to technology and various communication channels can be limited. Furthermore, while the attacks mentioned in our interviews were attributed by our participants to either Russian government or pro-Russian activist groups, the reliability of this attribution could not always be independently verified.

Acknowledgments

This work was supported by funding from the Danish National Defence Technology Center (Nationalt Forsvarsteknologisk Center, NFC) for the project "Optimering af Danmarks Cybernødberedskab" under the grant no. 24078. It has furthermore been supported by the Topic Engineering Secure Systems of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs. We furthermore thank our participants and local contacts in Ukraine who supported us in organising the interviews.

References

[1] Ioannis Agrafiotis, Jason RC Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4, 1 (2018), tyy006.

[2] Cameran Ashraf. 2021. Defining cyberwar: towards a definitional framework. *Defense & Security Analysis* 37, 3 (2021), 274–294.

[3] Danielle Keats Citron and Daniel J Solove. 2022. Privacy harms. *BUL Rev.* 102 (2022), 793.

[4] R.A. Clarke and R. Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins.

[5] Nic DePaula and Ersin Dincelli. 2018. Information strategies and affective reactions: How citizens interact with government social media content. *First Monday* (2018).

[6] Stéphane Duguin and Pavlina Pavlova. 2023. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. *Policy Department for External Relations Directorate General for External Policies of the Union. https://www. europarl. europa. eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI (2023) 702594_EN. pdf* (2023).

[7] Dominika Dziwisz and Błażej Sajduk. 2023. The Russia-Ukraine conflict from 2014 to 2023 and the significance of a strategic victory in cyberspace. *Applied Cybersecurity & Internet Governance* 2, 1 (2023), 1–20.

[8] Martin Eling, Michael McShane, and Trung Nguyen. 2021. Cyber risk management: History and future research directions. *Risk Management and Insurance Review* 24, 1 (2021), 93–125.

[9] Dominique Geissler and Stefan Feuerriegel. 2024. Analyzing the strategy of propaganda using inverse reinforcement learning: evidence from the 2022 Russian invasion of Ukraine. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW2 (2024), 1–25.

[10] Andy Greenberg. [n. d.]. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired* ([n. d.]). https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[11] Richard J Harknett and Max Smeets. 2022. Cyber campaigns and strategic outcomes. *Journal of Strategic Studies* 45, 4 (2022), 534–567.

[12] Y Linlin Huang, Kate Starbird, Mania Orand, Stephanie A Stanek, and Heather T Pedersen. 2015. Connected through crisis: Emotional proximity and the spread of misinformation online. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. 969–980.

[13] Muhammad Imran, Carlos Castillo, Fernando Diaz, and Sarah Vieweg. 2015. Processing social media messages in mass emergency: A survey. *ACM Computing Surveys (CSUR)* 47, 4 (2015), 1–38.

[14] International Committee of the Red Cross. [n. d.]. Cyber and information operations. https://www.icrc.org/en/law-and-policy/cyber-and-information-operations. Accessed 2025-01-17.

[15] International Committee of the Red Cross. 2023. Risk management. https://www.ncsc.gov.uk/collection/risk-management. Accessed 2025-03-04.

[16] Sushil Jajodia, Paulo Shakarian, VS Subrahmanian, Vipin Swarup, and Cliff Wang. 2015. *Cyber warfare: building the scientific foundation*. Vol. 56. Springer.

[17] Karim A.A. Khan KC. [n. d.]. Technology Will Not Exceed Our Humanity. *Digital Front Lines* ([n. d.]). https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

[18] Valerio La Gatta, Chiyu Wei, Luca Luceri, Francesco Pierri, and Emilio Ferrara. 2023. Retrieving false claims on Twitter during the Russia-Ukraine conflict. In *Companion Proceedings of the ACM Web Conference 2023*. 1317–1323.

[19] Alex Leavitt and Joshua A Clark. 2014. Upvoting hurricane Sandy: event-based news production processes on a social news site. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1495–1504.

[20] Alex Leavitt and John J Robinson. 2017. The role of information visibility in network gatekeeping: Information aggregation on Reddit during crisis events. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. 1246–1261.

[21] Mykola Makhortykh and Yehor Lyebyedyev. 2015. # SaveDonbassPeople: Twitter, propaganda, and conflict in Eastern Ukraine. *The Communication Review* 18, 4 (2015), 239–270.

[22] Nils Melzer. 2011. Cyberwarfare and international law. (2011).

[23] Alan Mishler, Erin Smith Crabb, Susannah Paletz, Brook Hefright, and Ewa Golonka. 2015. Using structural topic modeling to detect events and cluster Twitter users in the Ukrainian crisis. In *HCI International 2015-Posters' Extended Abstracts: International Conference, HCI International 2015, Los Angeles, CA, USA, August 2–7, 2015. Proceedings, Part I*. Springer, 639–644.

[24] Daniel Moore. 2022. *Offensive Cyber Operations: Understanding Intangible Warfare*. Hurst Publishers.

[25] State Service of Special Communications and Information Protection of Ukraine. 2023. *Russian Cyber Operations. APT Activity Report #3, H2 2023*. Technical Report. https://cip.gov.ua/en/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku

[26] State Service of Special Communications and Information Protection of Ukraine. 2024. *Russian Cyber Operations. APT Activity Report H1 2024*. Technical Report. https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report

[27] Alexandra Olteanu, Sarah Vieweg, and Carlos Castillo. 2015. What to expect when the unexpected happens: Social media communications across crises. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. 994–1009.

[28] Mervi Pantti. 2019. The personalisation of conflict reporting: Visual coverage of the Ukraine crisis on Twitter. *Digital Journalism* 7, 1 (2019), 124–145.

[29] Jessica Parker. [n. d.]. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *BBC News, Kyiv* ([n. d.]). https://www.bbc.com/news/world-europe-67691222

[30] Christian Reuter, Amanda Lee Hughes, and Marc-André Kaufhold. 2018. Social media in crisis management: An evaluation and analysis of crisis informatics research. *International Journal of Human–Computer Interaction* 34, 4 (2018), 280–294.

[31] Christian Reuter and Marc-André Kaufhold. 2018. Fifteen years of social media in emergencies: a retrospective review and future directions for crisis informatics. *Journal of contingencies and crisis management* 26, 1 (2018), 41–57.

[32] Ronald Ross. 2012. Guide for Conducting Risk Assessments. https://doi.org/10.6028/NIST.SP.800-30r1

[33] Michael N Schmitt. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Vol. 32. Cambridge University Press.

[34] Juliane Schmüser, Harshini Sri Ramulu, Noah Wöhler, Christian Stransky, Felix Bensmann, Dimitar Dimitrov, Sebastian Schellhammer, Dominik Wermke, Stefan Dietze, Yasemin Acar, et al. 2024. Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–16.

[35] Irina Shklovski and Volker Wulf. 2018. The use of private mobile phones at war: Accounts from the Donbas conflict. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.

[36] Gursimran Singh and Hrishikesh B Acharya. 2023. POSTER: A Cyberspace Study of the Russia-Ukraine War. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*. 1016–1018.

[37] Florian Skopik and Timea Pahi. 2020. Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity* 3 (2020), 1–20.

[38] Irina Temnikova, Sarah Vieweg, and Carlos Castillo. 2015. The case for readability of crisis communications in social media. In *Proceedings of the 24th international conference on world wide web*. 1245–1250.

[39] Zheye Wang and Xinyue Ye. 2018. Social media analytics for natural disaster management. *International Journal of Geographical Information Science* 32, 1 (2018), 49–72.

[40] Christopher Whyte and Brian Mazanec. 2023. *Understanding cyber-warfare: Politics, policy and strategy*. Routledge.

[41] Markus Wurzenberger, Stephan Krenn, Max Landauer, Florian Skopik, Cora Perner, Jarno Lötjönen, Jani Päijänen, Georgios Gardikis, Nikos Alabasis, Liisa Sakerman, et al. 2024. NEWSROOM: Towards Automating Cyber Situational Awareness Processes and Tools for Cyber Defence. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*. 1–11.