Can encryption save lives? Secure messaging and its infrastructure as loci of convergence between cyber warfare and conventional warfare: The case of Ukraine

Ksenia Ermoshina, Francesca Musiani

This document is a pre-print of

Ksenia Ermoshina, Francesca Musiani, 2024, "Can encryption save lives? Secure messaging and its infrastructure as *loci* of convergence between cyber warfare and conventional warfare: The case of Ukraine", *Media, War & Conflict*, OnlineFirst.

Please refer to the published version for citing or quoting.

Can encryption save lives? Secure messaging and its infrastructure as *loci* of convergence between cyber warfare and conventional warfare: The case of Ukraine

Ksenia Ermoshina and Francesca Musiani
Centre Internet et Société, Centre national de la recherche scientifique (CNRS), Paris, France

Abstract
The controversies surrounding the right to privacy of individuals in a hyperconnected world are longstanding debates, where particular emphasis is placed on encryption technologies, which encode information by converting its original representations into alternative forms that computers cannot decipher, thus ensuring the security of communications. These technologies are at the heart of a public controversy, in which privacy advocates a clash with claims that encryption is a threat to general security as an enabler of subversive action. Recent developments in the armed conflict in Ukraine open up or renew questions such as: in times of war, what is the role of encryption and privacy technologies? How does armed conflict challenge existing threat models, what are the new risks for civil society? Can encryption save lives? This article addresses these questions by showing that encrypted messaging is the subject of convergence between the informational and physical aspects 'in the field' of war in the 21st century. The aim is to show how these messaging tools and the digital ecosystem that makes their deployment possible (interfaces, access providers, telecom operators) are now an integral part of a war and resistance infrastructure where the borders between cyber warfare and conventional warfare are becoming more and more blurred. However, we will also underline the limits of a tool-centred approach and demonstrate how, in the case of the war in Ukraine, physical threats to civilians and infrastructure damage mean that encrypted messaging is one among several innovative technical and social practices of holistic self-defence deployed by Ukrainians.

Keywords
armed conflict, cyber warfare, encryption, infrastructure, internet, internet governance, physical warfare, Russia, Ukraine

Introduction
To think about infrastructural politics today is to consider how internet infrastructures are defining contemporary geopolitical conflict.[1] In particular, the controversies surrounding the right to privacy of individuals, linked to their ever-increasing dependence on digital technologies, are longstanding debates. During these debates, special emphasis is placed on encryption technologies, which encode information by converting its original representations

into alternative forms that computers and unauthorized third parties are in principle unable to decipher, thus ensuring the security of communications.

These technologies are at the heart of a public controversy in which privacy advocates a clash with those who claim that encryption is a threat to general security because it enables terrorism and other forms of subversive action. We have previously analysed this controversy and others in a recent publication (Ermoshina & Musiani, 2022). In this publication, we have outlined the non-linear history of encryption that has led, in the recent decade (in particular after the Snowden revelations and their re-shaping of encryption as an issue of public interest) to the birth of an articulate – and at times confusing and fragmented – landscape of tools to satisfy user concerns. This has meant that a number of users with different profiles are unsure as to which messaging service to use and possibly converge to; developers, for their part, are in a state of 'flux' and engage in trade-offs between different design issues, most often in the absence of formal standardization processes (Ermoshina & Musiani, 2022: 23). The protocols and applications in the encrypted messaging field share a common objective, which is to provide some degree of digital concealment in order to enhance individuals' and groups' freedom to conduct activities or professions; however, their diversity is revealing of (and performs) imagined publics, values, or objectives. Secure messaging tools and protocols are conceived of, designed, produced and reappropriated; thus there is a need for critical interrogation of the 'concealment' process itself (Whelan, 2024).

Developments in the armed conflict in Ukraine make it even more pressing to answer the questions this publication had begun to open up: in times of war, what is the role of encryption and privacy technologies? How does armed conflict challenge existing threat models, what are the new risks for civil society? Can encryption save lives? This contribution proposes to address these questions by showing that encrypted communications and traffic obfuscation technologies are the subject of convergence between the informational and physical aspects, 'in the field' of war in the 21st century.[2]

This article develops a two-part argument. First, we will show how these messaging and connectivity tools, as well as the digital ecosystem that makes their deployment possible (interfaces, access providers, telecom operators), are now an integral part of a war and resistance infrastructure where the borders between cyber warfare and conventional warfare are becoming more and more blurred. In the second part, we will underline the limits of an exclusively tool-centred approach and demonstrate how, in the case of the war in Ukraine, physical threats to civilians and infrastructure damage make it so that encrypted messaging is only one among several innovative technical and social practices of holistic self-defence deployed by Ukrainians. The use of encrypted messaging in times of war includes the mobilization of both last-generation privacy-enhancing tools and of pre-Web 2.0 technologies that shift focus from innovation to tinkering, repairing, maintaining and recycling. The case of Ukraine, in particular, demonstrates the co-existence of these different tools, strategies and concerns they answer, as the country itself is divided and the usage of encrypted tools varies, not just depending on user profiles, but from its occupied to its non-occupied areas as well.

This article seeks to provide a valuable contribution on three levels. Firstly, it offers a perspective grounded in the 'material turn' and infrastructure studies currents of Science and Technology Studies (STS) to the study of the use and development of media and communication tools in times of war. Secondly, it brings to the scholarly discussion empirical material that is derived from understudied (and difficult-to-access) fieldwork, including interviews with Ukrainian war journalists, digital security trainers, Internet Service Providers

(ISPs) and high-risk users of communication tools. Thirdly, it proposes an argument and a set of findings that – beyond the intrinsic interest of examining the Ukrainian case – can be engaged with and applied by researchers in other contexts, to see how strategies of use converge or differ.

Structure of the article

A first section will introduce the literature that we used in this research and that has been at the foundation of a longer investigation into encrypted messaging from a social sciences standpoint, started in 2016; this is followed by a short introduction to our methodology. The article then moves on to situate the subject of our inquiry within the broader history, and histories, of how communication devices are used strategically and/or as a survival tool in times of war. The subsequent two sections are the core of the article; in the first one, we discuss how encrypted messaging tools have been used in the context of the Russian invasion of Ukraine not only as an emergency communication device but also as a 'piece in the puzzle' of broader strategies for survival and military advantage. In the second one, we examine how such tools, despite their prominence, are only part of a broader infrastructure of information and communication in times of war that often resorts to 'simpler' and more basic communication devices and processes that are no less strategic and sometimes more adapted to specific war contexts than advanced privacy-enhancing technologies. The article concludes by briefly situating this research in the broader context of the 'global war for internet governance', which DeNardis (2014) has originally used as a metaphor, but acquires its very 'material' meaning in the present day.

A social sciences perspective on encryption and its infrastructure[3]

Over the years, scholars in STS have elaborated methodological tools to be able to read and narrate infrastructures, such as Star's (1999) 'ethnography of infrastructure', calling for an increased ethnographic sensibility to trace what is otherwise in the background, invisible and taken for granted, whose design processes, if empirically tested, can reveal passionate and sometimes confrontational stories of dissonances and attachments (Star and Ruhleder, 1994). Bowker and Star (1999) have labelled as 'infrastructural inversion' the double methodological gesture consisting of looking 'behind the scenes' of practices to retrace what has been enabled or constrained by design, and of looking 'in depth' to enable significations and meaning to emerge from technical standards, devices and apparatuses so as to understand where conflicts and controversies emerge and how they take shape *with* and *by* infrastructures.

Within this body of work, a particular focus exists on the transformations linked to the deployment of digital technologies in a variety of social worlds (Edwards, 2010). Indeed, when it comes to the internet and digital technologies, and information systems more broadly, scholars have acknowledged – and empirically analysed – that infrastructure also encompasses more abstract (and a priori immaterial) artifacts, such as protocols, standards (Bowker et al., 2010), software and code (e.g. Blanchette, 2011; Fuller, 2008), alongside the physical infrastructure supporting the functioning of digital networks, such as submarine cables, data centres, internet Exchange Points (IXPs) and so on. Elaborating on the idea – perhaps most famously summarized by legal scholar Lawrence Lessig's motto 'code is law' – that technical devices can be instruments for social control alongside other normative systems, a number of authors have refined our understanding of the arrangements of power inherent in, and revealed by, technical infrastructures and architectures of the internet and

digital/networked technologies. Exemplars of this research include Galloway's (2004) Foucault-inspired work on TCP/IP and DNS protocols as a means of control, DeNardis's (2009) analysis of the 'protocol politics' permeating the IPv4 to IPv6 transition, Gillespie's (2014) analysis of the 'relevance of algorithms' in internet content governance, as well as – especially relevant in the context of this article – the ensemble of works addressing 'privacy by design' and the extent to which privacy protection can be embedded and inscribed into technology (Cavoukian, 2012).

Encrypted tools, and the infrastructure that supports them and their functioning, are increasingly apprehended via these STS and infrastructure-based perspectives in order to shed light on the technical components and processes that are 'heavy with' political implications. Indeed, as it can hardly be disputed any more, Edward Snowden's 2013 revelations have been a landmark event in the development of the field of secure communications (see Snowden, 2019). Encryption of communications on a large scale and in a usable manner has become a matter of public concern, with a new cryptographic imaginary taking hold, one which sees encryption as a necessary precondition for the formation of networked publics (Myers West, 2018). Alongside the turning of encryption into a fully-fledged political issue, the Snowden revelations catalysed longstanding debates within the field of secure messaging protocols. The cryptography community (in particular, academic and free software collectives) renewed their efforts to create next-generation secure messaging protocols in order to overcome the limits of existing protocols. Protocols are a vital part of the internet's functioning, providing its conceptual model as well as the set of specifications that explain how data should be regrouped into packets, addressed, transmitted, routed and received; as Laura DeNardis (2009) made clear in *Protocol Politics*, the selection and adoption of particular protocols carries important political and economic implications, as well as technical ones.

Further, points of infrastructural control, beyond their originally intended function, can serve as proxies for different actors to regain (or gain) control or manipulate the flow of money, information and the marketplace of ideas in the digital sphere – what has been called the 'turn to infrastructure in internet governance' (Musiani et al., 2016). This can lead to a fully-fledged politicization of IG infrastructures, where a wide range of private and public actors seek to leverage particular socio-technical functions inscribed in digital infrastructures, including the infrastructures supporting encryption, as instruments of power (DeNardis, 2009). This issue is particularly important in sensitive contexts, including those of informational and/or armed conflicts, as the use of internet infrastructure to carry out functions diverging from their intended, original objective can lead to significant collateral damage to the stability and security of the internet and the protection of online civil liberties (DeNardis and Musiani, 2016).

For quite a long time, 'encryption' as a research subject has mostly been the prerogative of computer scientists, with more 'social' issues concerning it often being confined to debates about usable security, i.e. discussions taking place within the computer scientist community and based on survey-type studies that aim to find ways of making encrypted tools easier to use (see, e.g., Abu-Salma et al., 2017). A few studies have gone further in a sociological perspective on specific groups of users of particular encrypted tools or protocols (see, e.g., Braun and Oostveen's [2018] study of the characteristics and motivations of the Pretty Good Privacy encryption software). Since the Snowden revelations, encrypted communications are becoming a matter of widespread public debate, alongside the goals of privacy and security they seek to enhance; social sciences have taken up the challenge of investigating in depth how encrypted messaging tools are conceived and developed, adopted

by different user profiles – sometimes in unintended or unforeseen ways – how they inspire and are inspired by different imaginaries and how they eventually become the target of governance. Thus, they challenge notions such as the 'linearity' of protocol development or the inherent 'goodness' of particular privacy-enhancing or security-enhancing tools; instead, they propose a relational approach that moves beyond the naturalization of the relationship between digital tools, their underlying architectures and the variety of their uses. In doing so, they give visibility to the ongoing struggles around the daily 'making of' encryption and unveil how governance and contestation can happen in different arenas, and by various technical means.

As a recent book-length effort to retrace the history of encrypted communication has shown, 'the twenty-first century risk landscape became infinitely more complex when Snowden highlighted to citizens the civil rights risks which must be managed alongside terrorism, criminal, and nation-state risks' (Jarvis, 2020: 390); indeed, encryption is a matter of competing imaginaries and of the visions, designs and implementations they co-create, as Sarah Myers West (2018) has argued. People think about encryption through cyphers (that transpose letters of an alphabet), and through codes (that replace words) in different social, cultural and political contexts. Encryption has built its different meanings in the realm of national security and secrecy and in that of democratic systems, in each of which it enables private communication and makes it possible to avoid surveillance and potential social or political sanctions. Myers West's investigation into encryption imaginaries has illustrated how similar technologies may acquire different meanings and roles in different cultural settings. The historical dimension of these socio-cultural contexts and their evolution over time should also be considered, as Isadora Hellegren (2017) points out in her work. In a previous study, we have described cryptographic imaginaries as technological projections of the 'worst of all possible worlds' and, as such, they should be approached dynamically, in relation to the so-called 'threat models' – the elaboration of an anticipatory framework that allows the precise identification of adversaries, their strengths and weaknesses, and the ways to address them – and to the permanent evolution of the adversarial technical capacities (Ermoshina & Musiani, 2018).

Hence, the multi-faceted meaning of encryption evolves not only across communities of developers and users, but also over time, and understanding how various actors have constructed specific meanings of freedom with regard to technologies like encryption is significant to internet historians, hackers, programmers and policy-makers as all these actors are involved in constructing the form, function, measure and meaning of internet freedom. Furthermore, encryption – and the debates around it and the infrastructure supporting it – are the result of multiple public spheres and expert circles embedded in broader internet and society questions such as the control of networked media, surveillance and the protection of personal data (Monsees, 2019). An early study (Dizon, 2024) of how meanings, principles and values of encryption are defined and prioritized between and across different categories of stakeholders (the general public, businesses and government) has shown commonalities across actors (privacy is overall considered the most significant principle and value of encryption). However, after privacy, several other values, processes and concerns are shown to make up the mosaic of the making and meaning of encryption, including data protection, information security, trust, national security and public safety, right to property, as well as secrecy of correspondence, law enforcement and lawful access, right against unreasonable search and seizure, and right against self-incrimination (p. 12).

This plurality of meanings, practices and experiences of encryption, in addition to the information and communication infrastructure that enables and supports it, are especially salient when examined in contexts of war. Indeed, understanding what is the most appropriate solution to safeguard security and privacy in these most sensitive contexts becomes, from a matter of democracy and public sphere-building, a matter of life and death. The extent to which encryption technologies have been and are a tool in what has been labelled 'information warfare' has been examined in relation to digital technologies since the mid-1990s (Klopfenstein, 1999; Libicki, 1995), with an overall tendency to conclude that 'information' warfare is a separate set of processes and has a separate set of objectives with respect to the wars fought with 'physical' weapons on the field.

The remainder of this article and its empirical core seek to provide a recent analytical illustration of how information and communication technologies become loci where information warfare and armed conflict converge. We seek to show this through a case study of Ukraine, examined both before and after the full-scale Russian invasion of it began in early 2022.

Methodology

This article is based on the field surveys carried out within the NEXTLEAP project first, and then the ResisTIC project (please refer to Funding section for further details on both projects). These two projects have made it possible to conduct several years of semi-structured interviews with developers and users of secure messaging in a variety of national contexts and at different levels of risk, including Ukraine and Russia (main focus of ResisTIC). Several moments of fieldwork took place in Ukraine, including month-long research periods in Kyiv in 2016, 2017 and 2018. In addition to interviews, these research periods included observation of four digital security trainings, **and** three conferences dedicated to journalist and NGO security in the context of war. A total of 50 interviews (60–90 minutes) with Ukrainian NGO activists, digital security trainers, war reporters, technical experts and politicians were conducted during these research periods. These interviews mainly focused on risk perception, threat models and digital self-defence strategies of Ukrainians whose work involved communicating with or visiting the temporarily occupied territories.
The contacts established during these periods made it possible after February 2022 to continue the interactions and follow-up interviews which focused on the practices of development and use of different messaging tools and digital security trainings in the light of the full-scale invasion. This second round of interviews included seven follow-up conversations with trainers, journalists and tech experts. The objective was to identify how threat models and self-defence practices changed with the full-scale invasion.
This article also benefits from a documentary analysis concerning legal and regulatory documents, in addition to guides on digital security produced by Digital Security Lab Ukraine and Nadiyno helpline, as well as technical documents related to the development of secure communication tools (bug reports, release notes, pull requests, etc.)

In addition, we have conducted web-ethnography with a focus on Telegram channels maintained by Ukrainian ISPs[4] that helped collect visual and textual testimonies of impacts of the war on communication infrastructures, circumvention technologies and repair and maintenance practices. Reports on internet shutdowns produced by AccessNow, Netblocks and data from IODA and Mozilla Network Outages Data Project were also used as valuable sources of information about Ukrainian connectivity in times of war.

Encrypted messaging: A strategic tool

Mobile technology has been an essential piece of equipment in times of conflict for many years. To cite an emblematic example, in 2011, when civil war broke out in Syria, large swathes of the country had uninterrupted network coverage and telephones were of paramount importance (Rohde et al., 2016). Armed fighters used their phones to communicate with each other, sending critical information about their opponents' locations and movements. Camera-equipped phones also became essential for transmitting images to the outside world that laid bare the realities of war, such as photographs revealing the consequences of the use of chemical weapons against civilians. Disturbing footage of this nature, filmed by citizen journalists and posted on the websites of major international media outlets, led to sanctions imposed by the US against senior Syrian officials in 2017 (Cliff et al., 2013).

During one of our field visits in Ukraine in 2018, when travelling in the company of a Spanish colleague on a train from Kharkiv to Kyiv, we encountered a Ukrainian officer in his 50s. Intrigued by the presence of a younger foreigner, who had also had experience of war (as a war journalist covering the Rojava resistance movement) the officer quickly became talkative. He shared his experience of war and enthusiastically showed us photos from the frontlines that he was sharing with fellow soldiers over Viber. The officer was not aware of the weaknesses in Viber's encryption, or of the fact that Viber had located part of its servers in Russia in 2015 to comply with Russian legislation.[5] He confessed that he used Viber to talk to Russian officers whom he had known during the Chechen war where he went to serve as a contract soldier. They used Viber to negotiate on organizing exchanges of imprisoned men from both sides. For this officer, as it must be for many others, the comfort, reliability and speed of communications over Viber acquired greater relevance than the doubtful security and privacy policies of this communication system.

In 2014, Viber scored 1 out of 7 points on the (now out-of-date) Electronic Frontier Foundation's 'Secure Messaging Scorecard',[6] because of the absence of end-to-end encryption. It meant that messages sent via Viber were only encrypted in transport, but not on the company servers. The Scorecard, produced by a highly respected NGO, served for several years as a performative measurement tool (Musiani & Ermoshina**,** 2017) and led to implementation of a new encryption protocol in 2016, based on the state-of-the-art protocol developed by the Signal team. It used the 'Double Ratchet' mechanism that generates keys per each communication session established between two devices. Viber's protocol was not standardized nor open until very recently, making this messenger an unpopular choice for a tech-savvy audience.

This field anecdote reveals several aspects of the usage of encryption during war. First, it shows that security properties of a messaging application do not always define users' choices. In the case of Viber, it is the popularity of the tool (it is the most popular messaging app in Ukraine) and the subsequent network effects this popularity generates. Second, when put in perspective with the recent evolution of the Ukrainian–Russian war, it sheds light on the difficulties of developing a coherent security culture and organizational policies to regulate communications within the military at times of open warfare. Indeed, as our interviews with digital security trainers show, soldiers on the ground used to tinker with, and rely on, a diverse set of applications for internal communications as well as for relations with family and friends. With the war grown into a full-scale invasion, stricter recommendations were developed for the Ukrainian Defence Forces, imposing usage of Threema, a closed-source Swiss-based end-to-end encrypted messenger that is also used by the Swiss army itself.

However, for many units of the Ukrainian Defence Forces, in addition to messaging apps, social media such as Instagram or YouTube have become a crucial tool for fundraising for equipment and drones, as well as an important tool of external communication about the successes of the Ukrainian army. Footage and photos of military in action are circulating across social media platforms with little or no anonymization measures taken. For the Russian army, on the other hand, Telegram became the main communication tool regardless of absence of end-to-end encryption by default.

Alongside the military, encrypted chat and messaging apps have been essential communication tools for civilians caught in the middle of violent conflict and for those living under authoritarian regimes. For parties to conflicts, these apps have provided critical public safety information and up-to-date news on the locations of invading forces. For people living in authoritarian countries, encrypted messaging has facilitated a channel of communication that avoids the surveillance of spyware, which provides these governments with mines of information allowing the arrest and imprisonment of political opponents. These email services offer end-to-end encryption to prevent anyone except the sender and recipient from monitoring communications. The information sent through these apps is converted into a set of random characters and symbols which makes the original message completely secure with a special key to unlock it. Short message services (SMS), on the other hand, are generally unencrypted, leaving users at the mercy of hacking software that can be deployed to read all communications sent through this medium.

Encrypted messaging has proven vital in the conflict in Ukraine. Viber and Telegram were particularly helpful: these two tools have the highest penetration rates at 98 percent and 86 percent, respectively. Their high usage can largely be explained by how the Ukrainian Ministry of Health has relied on these apps to relay critical health communications during the COVID-19 pandemic, but interestingly these messaging services were reoriented following the Russian escalation. The main Telegram channel dedicated to reliable information on coronaviruses in Ukraine is managed by a private company but works closely with the government and is verified by Telegram: a communication channel that was a priori apolitical can evolve ‘to become an important tool of communication citizenship in times of war’ (Trauthig, 2022). The Ukrainian example is arguably the most recent and stark example, but not the only one of the growing importance of encrypted messaging apps and services in armed conflict.

Ukrainians living in occupied territories, for example, face problems such as surveillance by Russian occupants to which encryption seems an obvious solution. They also experience intense online censorship, disinformation and propaganda. Since January 2023, internet service providers (ISPs) on temporarily occupied territories have to install the so-called SORM middleboxes for lawful interception and for the storage of their clients’ metadata This has been viewed by our respondents as one of the major big changes the the landscape of threats after the full-scale invasion:

What has definitely increased, if comparing 2014–2022 and 2022–2023, are the blockages of websites and services, for example, messengers through which people could and did transmit information about the location of military equipment, monitoring of internet activity, and inspection of smartphone contents for the presence of Ukrainian symbols, pro-Ukrainian content, and photographs of military (occupiers) and everything related to this. (P, digital security trainer connected to Nadiyno helpline, interview 27 December 2023)

Thus, both specialized organizations, such as DSL Ukraine or Nadiyno helpline, and peer dynamics help spread the usage of certain secure messaging applications that contribute to protecting the content of communications from a third party via advanced cryptographic protocols such as end-to-end encryption. Virtual Private Networks (VPN) that both obfuscate some of the user's browsing activities and help bypass censorship are other crucial tools. Given that many Ukrainians in the occupied territories are involved in communicating sensitive information – for example, details about the disposition of Russian troops – considerable effort has been expended toward promoting encrypted tools for this group of Ukrainians and the particularities of the hardships they face.

Digital security trainers developed specific recommendations for Ukrainians living under occupation, which emphasized the importance of using pseudonymous messengers that are not dependent on a phone number.[7]

Canadian NGO eQualit.ie, for example, deployed an initiative called dComms, with servers in several major Ukrainian cities, including in places that were formerly under Russian occupation (namely, Kherson). This project allows people to communicate locally by using federated end-to-end encrypted tools, such as Element[8] or Delta Chat.[9] Using encrypted VoIP calls (over Signal or WhatsApp, for instance), instead of relying on simple GSM calls, quickly became a common practice and a recommendation[10] for escaping surveillance on the occupied territories.

Local ISPs and the international technical community make a special effort to keep occupied Ukrainian territories connected[11] to Ukrainian and international cyberspace, including uncensored access to Ukrainian and foreign media, and absence of Russian surveillance. Yet, the digital security practices of high-risk users in Ukraine reveal that encryption is both crucial in conflict situations and at the same time, in particular contexts, less important than one might think. For instance, many recommendations focus on account protection using two-factor authentication, or other non-cryptographic recommendations:

We still remind people of the same things, the basics, like enabling 2FA, choosing strong passwords and so on … obvious things like protecting your phone with a password instead of biometrics. The new thing is power outages, having power banks and chargers with you at all times, and in general being ready for emergencies. (M, digital security trainer, follow-up interview, November 2023)

Surprisingly, many of the security practices of Ukrainians have not radically changed in the face of the full-scale Russian invasion, even if internet infrastructure is becoming an important battlefield over power. In several instances, the physical and material aspects of the digital ecosystem, notably the access to any kind of connectivity, become more vital in times of war than having access to advanced encryption.

Beyond encryption: Communication infrastructures as survival tools in wartime

Despite their prominence, encrypted communication techniques are only part of a broader infrastructure of information and communication in times of war that often resorts to 'simpler' and more basic communication devices and processes which are no less strategic and sometimes more adapted to specific war contexts than advanced privacy-enhancing technologies.

Since the very early stages of Russia's invasion of Ukraine, the Russian army has shown a propensity to target information and communication infrastructures. Traffic control and Border Gateway Protocol (BGP) hijacking in frontline zones have been actively employed as a strategy of information warfare by Russia. One of our interviewees, a Ukrainian war photographer, shared his experience of a mission he was on in 2017 near the demarcation line in the Donetsk region (on the Ukrainian side). He was using Wi-Fi connection in one of the few working cafés to upload photos he just took to a cloud storage and to share some of them with a newsroom he was working with. However, he noticed that the website of his medium was blocked and he was shown a Russian blockpage. Upon checking his network information, he found out that he was routed via a Russian upstream provider.

This situation is an example of a broader information control strategy that we call 'traffic wars' (Ermoshina, 2024). Since 2022, Russia has repeatedly hijacked Ukrainian ISP infrastructures on occupied territories and rerouted end-user traffic via its uplinks, some of which were created with this goal in mind; namely, the infamous operator Miranda-Media, an offspring of Russian Rostelecom, introduced in 2014 to take over routing in Crimea (as is documented in detail in a dedicated publication; see Fontugne et al., 2020). For Ukrainian civilians and military, this means Russian censorship, disinformation and surveillance, with a higher risk of being de-anonymized and tracked for online activities. Hence the need for stronger protection of all online communications (and, for some of the military, a strict ban on all social media public activities).

In early 2022, an intense battle for control over Ukrainian informational infrastructures took place on its temporarily occupied territories, including over its landlines, cables and cell towers. This battle culminated between May and November 2022, when Russian operator Miranda-Media took over routing in territories controlled by Russia. This consisted of physical seizure of ISP equipment, but also of important changes in BGP settings that made small local ISPs use Russian upstream traffic. For the citizens living in the occupied territories, this implies the establishment of censorship and surveillance with sound digital security becoming increasingly important for them.

In other cases, the Russian army has appeared at least partially unaware of what their destruction of specific and sensitive components of Ukraine's communication infrastructure would cause to its own military efforts. Indeed, according to fact-checking group Bellingcat (relayed by several other media), in early March 2022, the Russian military was forced to use unencrypted, commercial telephone lines after their own attacks on Ukrainian 3G towers impeded the use of the Russian government-built 'Era' cryptophone, which needs 3G and 4G to function and that was intended for troops to securely communicate with each other. This security breach eventually led Ukraine's defence intelligence agency to be able to confirm that Russian general Vitaly Gerasimov had been killed.[12]

Since the Russian invasion in February 2022, Ukrainians have lived in an 'asymmetric risk' scenario, meaning that risk is not equally distributed across the population. Many Ukrainians have left the country, others have joined the army and remain at the epicentre of events, the majority live under a permanent risk of air raids and a large group of Ukrainians faces the hardships of life under Russian occupation. All are at risk of being disconnected.
In this 'asymmetry' of risks, there is no consensus as to preferred encrypted communication tools or 'best tactics' of digital self-defence. Instead, we witness a variety of contexts that require different tools and sets of recommendations.

Internet shutdowns, total or partial, are very frequent (see Figure 1);[13,14] infrastructures are targeted in bombing attacks because connectivity is a strategic resource in times of war. Being disconnected can mean the difference between life and death when digital communication tools are key in asking for food aid, medical help, electricity and other key services. The conflict plays out through internet infrastructure.

Figure 1. Infographics based on Mozilla Network Outages Data Project produced at the Hackathon Without Borders in Berlin on 29–30 April 2023.

At the same time, some Ukrainian users face higher risks than others. For instance, journalists or humanitarian workers whose missions take place on the frontlines, or civilians who are actively supporting the Ukrainian Defence Forces while living under Russian occupation. Due to the variety of profiles and risk levels of these users, encryption is not always, or not the only solution. Our research on the use of encrypted messaging systems in Ukraine, conducted between 2016 and 2019, focused on especially high-risk users, such as journalists, human rights defenders and inhabitants of key battlefields like the Crimea or Donetsk and Luhansk regions **(**Ermoshina & Musiani, 2022). These users' digital security practices included secure

messaging tools and other privacy-enhancing technologies. But, rather than focusing on explaining advanced tools, such as The Onion Router (Tor) or PGP (Pretty Good Privacy), the digital security trainers that advised them instead focused on developing tailored and sometimes counterintuitive responses. The trainers understood risk as highly contextual and rapidly changing and 'security' as a multilayered process (Ermoshina & Musiani, 2018; see also Kazansky, 2021). This localized and holistic understanding of the threat led to the conclusion that more or better encryption is not always the answer for users, in contrast to what many advocates of privacy-enhancing technologies believe.
In a recent round of interviews with Ukrainian users, digital security trainers and technical operators, we found that, since February 2022, digital security trainers emphasized the importance of communicational autonomy and physical security. Power banks, solar batteries, extra phones, chargers and cables, mobile routers and even Starlink antennas became the new focus of training sessions, alongside psychological self-help tutorials and medical first-aid classes. Encryption receded into the background, while the mere accessibility of any kind of communication means became vital.

Many efforts from the ISPs were invested in timely repair of damaged infrastructures (involving risks to life when working under bombing) and to bring WiFi as far as into the anti-bomb shelters. The role of ISPs at war has become a public controversy and a challenge for internet governance. Since the beginning of the full-scale invasion, Ukrainian ISPs have often been working under bombings to repair their infrastructures. Local, small or medium-size providers were among the first to react and bring the connectivity back in town. The Ukrainian Association of ISPs tried to request armed vehicles for providers from the Ukrainian government but could only obtain case by case help and providers had to collect funds themselves to buy better and more secure vehicles.

Frequent blackouts have considerably impacted the work of Ukrainian ISPs, making access to electricity the top priority. The international fund 'Keep Ukraine Connected' and Canadian NGO eQualit.ie were providing targeted help to Ukrainian ISPs in the non-occupied territories by shipping them generators and batteries. Blackouts have had a profound impact on the internet infrastructures in Ukraine, making network engineers seek new solutions to saving power or even finding ways to provide internet without electricity. This led to the popularization of PON (Passive Optical Network) technology. PON's architecture is point-to-multipoint which allows a provider to serve many customers connecting to them directly via optical fibres that are independent of electricity. If the office of the ISP has current, the clients will have access to the internet even when their homes are out of power. Our analysis of Ukrainian ISP's Telegram channels revealed that this community was highly innovative and supportive to their customers beyond the purely commercial attitude. Thus, some providers were organizing power stations inside or outside their office in order to provide people with access to power plugs and give them the possibility of charging their devices.

However, access to internet connectivity in the occupied areas is a topic of public controversy: while technicians continue to support their clients whose life and freedom depends on connectivity, they are also formally collaborating with Russian occupational administration. The case of a provider from Kherson, SkyNet, has become an example of this dual role of ISPs in time of war. SkyNet was serving people in Kherson throughout the whole time of the Russian occupation and organized a local forum for its clients who were able to communicate with each other even without connection to the global web. They also set up a power station for customers to charge their phones. However, with the end of the occupation, they had to close down since they were considered to be 'collaborators'.

While possibilities of blackouts are shared by all the Ukrainian territory (even if not equally distributed), the usage of devices and associated risks are different in territories controlled by Ukraine and in occupied parts. In Kherson, an important port city under Russian occupation between April and November 2022, Ukrainian users were at a high risk of random identity control and interrogations by the Russian military, which included device seizure. As a consequence, using less commonly used or more technically sophisticated encrypted messengers was considered a risk in its own right. The mere fact of having certain apps on one's phone (such as Signal, Tor, a VPN or even Telegram) could raise suspicion and result in bodily harm or even life-threatening situations at the routine phone checks conducted by Russian soldiers.

In occupied territories there are blockposts everywhere and people get their phones taken and apps and chats are scrutinized. So you can only use apps that raise no suspicion: of course Signal is out of scope, you can get arrested for having it. Only Viber, WhatsApp or Telegram are possible. And again, you have to be very careful with how you write and to whom. Basically, users rely on self-censorship, disappearing messages and sometimes even self-made cyphers. (D, digital security trainer, Ukraine, interview 12 April 2024)

The context of military occupation brings back older pre-internet practices of obfuscation, such as cyphers or Aesopian language. It redefines the role of encryption and shows how each messaging app actually refers to certain communicative cultures and user-groups.
In a strategy that might initially seem counterintuitive to those not in war situations, digital security trainers aware of this context advise their high-risk users to use WhatsApp and Gmail instead of Signal or a PGP-encrypted form of email.

Since WhatsApp adopted end-to-end encryption, we usually do not spend that much time on instant messaging encryption [during trainings] and recommend staying with WhatsApp if people already use it. So they can still communicate with all of their friends, and also … it looks familiar, and does not shock them. And people say [during trainings] if they use WhatsApp it's less suspicious than if they use a special app for activists. ('I', female informational security trainer, Ukraine, 2017)

In this context, extra-cryptographic factors, such as 'ephemeral' (disappearing) messaging, turned out to be key in defining people's communication practices. Or, to put it more plainly, when it came to ensuring safe communication for the occupied peoples of Kherson, the familiarity with and inconspicuousness of particular tools won out over sophisticated privacy-enhancing technologies. On top of that, the low learning curve associated with already-popular tools, as well as the fact that these tools already have a built-in network of skilled users, proves to be a more crucial advantage than the privacy protections guaranteed through better encryption technologies.

The Ukrainian approach to security underlines that risk is relational and local. Therefore, no consensus exists as to 'the best encrypted messaging app'. Security should be considered a multi-layered complex process, in which the digital layer is just one of many. The practices of Ukrainian users teach us that the protective potential of encryption is always and intrinsically linked to physical, psychological and operational politics – as well as infrastructural concerns.

Conclusion and future research: Encryption between the 'war for internet governance' and the new war(s)

The deployment of secure messaging as a strategic tool in times of war invites itself into the broader debates concerning the expansion of the regulation of digital technologies by states, one of the central issues of what Laura DeNardis (2014) has called the 'war for Internet Governance'. Referring to the importance of encrypted messaging in conflict zones like Ukraine, several position papers have reaffirmed[15] the need for strong encryption, while proponents of weakening it say such technology makes it more difficult for law enforcement to monitor apps for human rights abuses and crimes. Industry experts point to the possibility that the door could be opened to increased government surveillance, as well as exploitation by hackers trying to steal sensitive financial data. Companies that run encrypted messaging are aware that their platforms are being used as essential lifelines by some actors and exploited to spread propaganda by others, but their responses have so far been inconsistent. Between the privatization of regulation and the need for digital and physical protection, the encryption of communications has not yet finished being a controversial issue – and shows how internet governance is increasingly inviting itself into the conflicts of the 21st century.
At the same time, the unique character of the war in Ukraine redefines the role of encryption, as well as the choices made by actors about when to rely on it and which tools to choose. As the country remains under partial occupation, this creates disparities in terms of access to online services and risks faced by its populations. Encrypted messengers are still preferred to unencrypted ones across all territory, but the realities of war condition individuals' and groups' choices of messengers, making them more inclined to select more reliable and more popular ones. Other techniques, such as self-censorship or self-made cyphers, still persist, which demonstrates the importance of personal connections, group agreements and ad-hoc practices as an addition (or even a replacement) to sophisticated digital tools in times of major crises.

With this article – addressing the particularly sensitive scenario of Ukraine's response to invasion, at the crossroads of information warfare and physical warfare – we suggest that attention should be paid to the 'mundane practices' that build, on a daily basis, informal structures of information and internet governance (Epstein et al., 2016). Ultimately, we propose that future research should pay closer and more frequent attention to the ways in which these practices reveal what makes 'good' security in today's networked (and war-fraught) society.

Funding
This research has received the support of the European project NEXTLEAP (nextleap.eu, 2016-2018) first, then of the ResisTIC project (resistic.fr, 2018-2022), funded by the French National Agency for Research (ANR), and most recently of the French Foundation for the Social Sciences (*Fondation pour les sciences sociales, sous l'égide de la Fondation de France*, 2023-2024) and the ANR project DIGISOV (https://cis.cnrs.fr/digisov/, 2024-2027).

Notes
1.A much-shorter version of this article was published as a chapter in a (2023) publication aimed at a broad readership (see Ermoshina & Musiani, 2023).
2.This research has received the support of of the European project NEXTLEAP (nextleap.eu, 2016-2018) first, then of the ResisTIC project (resistic.fr, 2018-2022), funded by the French National Agency for Research (ANR), and most recently of the French Foundation for the Social Sciences (*Fondation pour les sciences sociales, sous l'égide de la Fondation de France*, 2023-2024) and the ANR project DIGISOV (https://cis.cnrs.fr/digisov/, 2024-2027).
3.Part of this section has been re-elaborated from the introduction of **(**Ermoshina & Musiani, 2022).

4.For instance,
see https://t.me/tk_group; https://t.me/fifthua; https://t.me/kyivlink; https://t.me/skynet_ks_info; https://t.me/ponKabzdec https://t.me/lanetua, etc.
5.See: https://www.neweurope.eu/article/viber-moves-data-storage-to-russia/
6.See: https://www.eff.org/pages/secure-messaging-scorecard
7.See, for instance, this article recommending the use of secure messenger Threema, rather than Signal: https://nadiyno.org/chomu-threema-krashhe-za-signal-v-okupacziyi/
8.See: https://element.io
9.See: https://delta.chat/
10.Digital security helpline Nadiyno has published several articles dedicated to the choice of apps for secure communications on temporarily occupied territories; see, for example, https://nadiyno.org/yak-zahystyty-golosovi-povidomlennya-cherez-mesendzher-na-okupovanij-terytoriyi/#
11.See, for instance, the Keep Ukraine Connected initiative, https://nogalliance.org/our-task-forces/keep-ukraine-connected/
12.See: https://www.datacenterdynamics.com/en/news/ukraine-russian-militarys-own-encrypted-phones-impacted-after-destroying-3g4g-towers-allowing-comms-to-be-intercepted/
13.See: Access Now report https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine/
14.See, as well the interactive map of shutdowns in Ukraine, https://public.tableau.com/app/profile/nika.aleksejeva/viz/InternetOutages_UA_RU_DE/Maps_DB
15.See: https://www.bcs.org/articles-opinion-and-research/removing-end-to-end-encryption-would-do-more-harm-than-good-says-poll-of-it-professionals/

References

Abu-Salma R et al. (2017, May) Obstacles to the adoption of secure communication tools. In: 2017 IEEE Symposium on Security and Privacy (SP), May: 137–153.
Blanchette J-F (2011) A material history of bits. Journal of the Association for Information Science and Technology 62: 1042–1057.
Bowker GC and Star SL (1999) Sorting Things Out: Classification and its Consequences. Cambridge, MA: The MIT Press.
Bowker GC et al. (2010) Toward information infrastructure studies: Ways of knowing in a networked environment. In: Hunsinger Jet al. (eds) International Handbook of Internet Research. Berlin: Springer, 97–117.
Braun S and Oostveen AM (2018) Encryption for the masses? An analysis of PGP key usage. Mediatization Studies 2: 69.
Cavoukian A (2012) Privacy by design: Origins, meaning, and prospects for assuring privacy and trust in the information era. In: Yee G (ed.) Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards. Hershey, PA: IGI Global, 170–208.
Cliff D, Moul R and Jugieux A (2013) Chemical weapons detection: Inspecting Syria. VERTIC BRIEF 22: 1–7.
DeNardis L (2009) Protocol Politics: The Globalization of Internet Governance. Cambridge, MA: The MIT Press.
DeNardis L (2014) The Global War for Internet Governance. New Haven, CT: Yale University Press.
DeNardis L and Musiani F (2016). Introduction: Governance by infrastructure. In: Musiani F et al. (eds) The Turn to Infrastructure in Internet Governance. New York: Palgrave-Macmillan, 3-21.

Dizon MAC (2024) Socio-legal study of technology: A norms and values approach to hacking and encryption law and policy. Computer Law & Security Review 52: 105958.
Edwards PN (2010) A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming. Cambridge, MA: The MIT Press.
Epstein D, Katzenbach C, Musiani F (2016) Doing internet governance: practices, controversies, infrastructures, and institutions. *Internet Policy Review 5*(3): 1-14.
Ermoshina K (2024) "Voices from the Island": Informational annexation of Crimea and transformations of journalistic practices. *Journalism 25*(3): 528-546.
Ermoshina K, Musiani F (2023) Encryption as a battleground in Ukraine. *In:* Cath C (ed.), *Eaten by the Internet.* Manchester (UK): Meatspace Press, 82-88.
Ermoshina K, Musiani F (2022) *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties.* Mattering Press.
Ermoshina K and Musiani F (2018) Hiding from whom? Threat models and in-the-making encryption technologies. *Intermédialités: histoire et théorie des arts, des lettres et des techniques* 32. DOI: *10.7202/1058473ar*
Fontugne R, Ermoshina K, Aben E (2020) The Internet in Crimea: a case study on routing Interregnum. In: 2020 IFIP Networking Conference (Networking). IEEE, 809-814.
Fuller M (ed.) (2008) Software Studies: A Lexicon. Cambridge, MA: The MIT Press.
Galloway AR (2004) Protocol: How Control Exists After Decentralization. Cambridge, MA: The MIT Press.
Gillespie T (2014) The relevance of algorithms. In: Gillespie T et al. (eds) Media Technologies: Essays on Communication, Materiality, and Society. Cambridge, MA: The MIT Press.
Hellegren ZI (2017) A history of crypto-discourse: Encryption as a site of struggles to define internet freedom. Internet Histories1(4): 285–311.
Jarvis C (2020) Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. London: CRC Press (Taylor & Francis).
Kazansky B (2021) 'It depends on your threat model': The anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society 8(1).
DOI: 10.1177/2053951720985557.
Klopfenstein DR (1999) Deciphering the encryption debate: A constitutional analysis of current regulations and a prediction for the future. Emory Law Journal 48: 765.
Libicki MC (1995) What Is Information Warfare? Report, National Defense University, The Center for Advanced Command Concepts and Technology. Available at: https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf (accessed November 13, 2024).
Monsees L (2019) Crypto-Politics: Encryption and Democratic Practices in the Digital Era. Abingdon: Routledge.
Myers West S (2018) Cryptographic imaginaries and the networked public. Internet Policy Review 7(2). DOI: 10.14763/2018.2.792.
Musiani F et al. (2016, eds.). The Turn to Infrastructure in Internet Governance. New York: Palgrave-Macmillan.
Musiani F and Ermoshina K (2017) What is a good secure messaging tool? The EFF secure messaging scorecard and the shaping of digital (usable) security. *Westminster Papers in Communication and Culture 12*(3).
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(7): 515–531.
Snowden E (2019) Permanent Record. New York: Henry Holt and Company.
Star SL (1999) The ethnography of infrastructure. American Behavioral Scientist 43(3): 377–391.

Star SL and Ruhleder K (1994) Steps towards an ecology of infrastructure: Complex problems in design and access for large-scale collaborative systems. In: Proceedings of the Conference on Computer Supported Cooperative Work. Chapel Hill, NC: ACM Press, 253–264.
Trauthig IC (2022) Chat and encrypted messaging apps are the new battlefields in the propaganda war. Lawfare, 27 March. Available at: https://www.lawfareblog.com/chat-and-encrypted-messaging-apps-are-new-battlefields-propaganda-war (accessed November 13, 2024).
Whelan A (2024) Review of Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties (Ksenia Ermoshina and Francesca Musiani, 2022). Internet Histories 8(1/2): 208–212.

Author biographies

Ksenia Ermoshina is Associate Research Professor (chargée de recherche) at the French National Centre for Scientific Research (Centre national de la recherche scientifique, CNRS) and member of Centre Internet et Société (CIS). Ksenia's research interests are on the intersection of infrastructure studies, surveillance studies, STS, political sociology and usability studies. She is interested in the design of encryption protocols, as well as in the transformation of Internet infrastructures within geopolitical conflicts.

Francesca Musiani is Research Professor (directrice de recherche) at CNRS, and deputy director of CIS. Francesca's recent research has focused on the use of artificial intelligence in public action projects, the development and use of encryption technologies in secure messaging, and "digital resistances" to censorship and surveillance in the Russian Internet. Francesca's theoretical work explores STS approaches to Internet governance, with particular attention paid to socio-technical controversies and to governance "by architecture" and "by infrastructure".