



HAL
open science

Encryption as a battleground in Ukraine

Ksenia Ermoshina, Francesca Musiani

► **To cite this version:**

Ksenia Ermoshina, Francesca Musiani. Encryption as a battleground in Ukraine. Corinne Cath (ed.), Eaten by the Internet, Meatspace Press, pp. 82-88, 2023. hal-04272924

HAL Id: hal-04272924

<https://hal.science/hal-04272924>

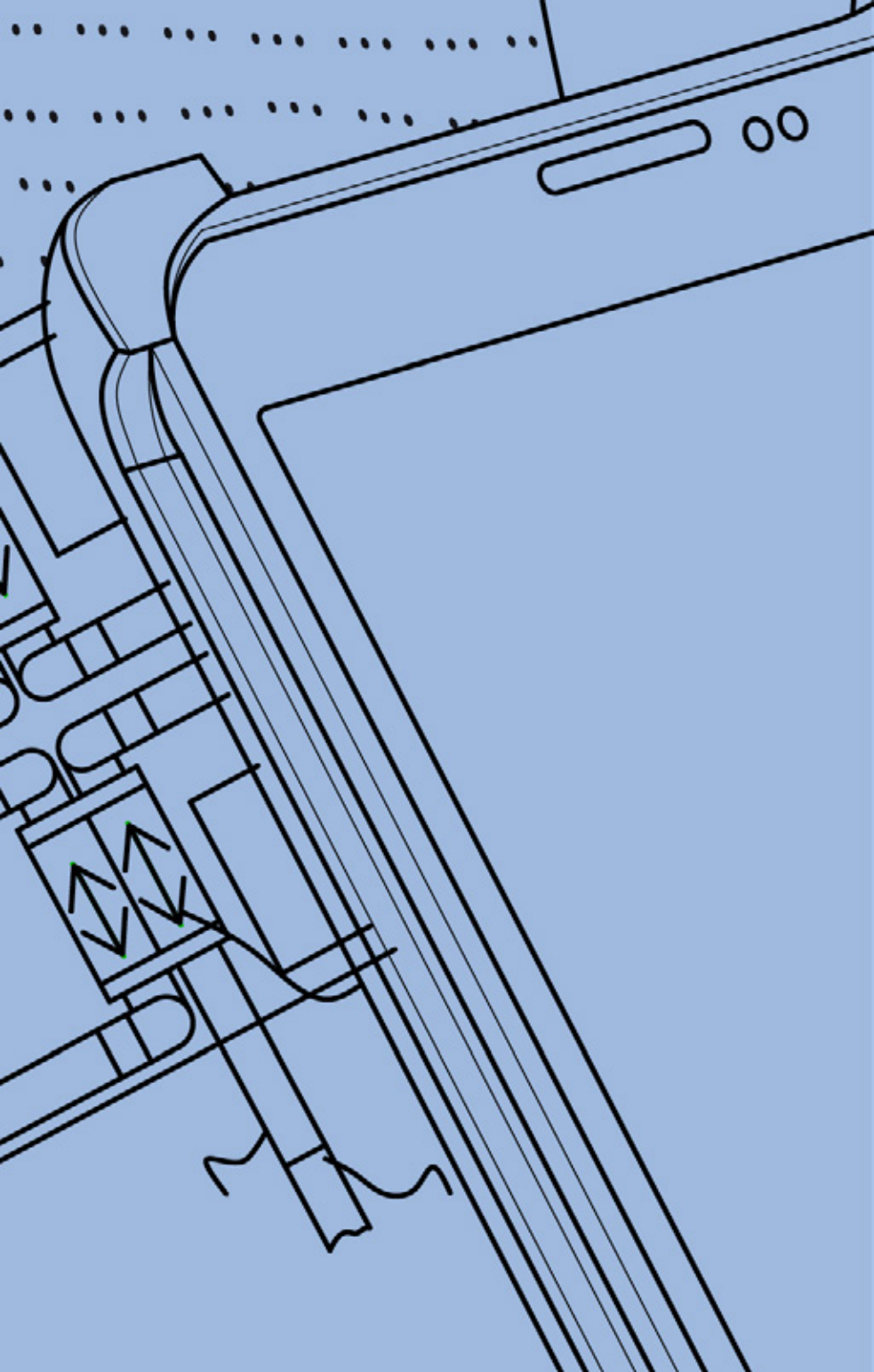
Submitted on 6 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - ShareAlike 4.0 International License



150 Encryption as a battleground in Ukraine

151 Ksenia Ermoshina Ksenia Ermoshina is an Associate Research Professor at the Centre for Internet and Society of CNRS (the French national research council), in Paris, France.

152 Francesca Musiani Francesca Musiani is an Associate Research Professor and Deputy Director at the Centre for Internet and Society of CNRS, in Paris, France.

153 Keywords: encryption, geopolitics, resistance, routing, Ukraine

154 To think about infrastructural politics today is to consider how internet infrastructures are defining contemporary geopolitical conflict. Russia's invasion of Ukraine in early 2022 instigated an intense battle for control over Ukrainian informational infrastructures on its temporarily occupied territories, including landlines, cables, and cell towers. The most intense period of this battle happened between May 30 and November 11, 2022, when Russian operator Miranda-Media took over the routing of internet traffic in territories controlled by Russia. This telecommunications company was initially established to aid Russian efforts in its occupation of Crimea, rerouting local traffic and making it easier for the Russian state to filter and censor the Ukrainian Internet. The very existence of this company, which eventually operated in other occupied parts of Ukraine, speaks to the key role of internet infrastructure in geopolitics.



Political use of internet infrastructure in war zones is more and more common. This makes encryption—an important but much less visible aspect of infrastructure than, for example, broken cables or shot down cell towers—an important battleground in Ukraine. By extension, this means digital security is one of the crucial components of the physical security of people living under Russian occupation. However, researching Ukrainian users' online practices in times of war shows that, paradoxically, advanced encryption is not always key to security. Rather, the war in Ukraine demonstrates that the physical and material functions of digital infrastructure, such as connectivity and internet access, can be more vital than privacy-enhancing technologies.

GENERAL DIGITAL SECURITY PRACTICES UNDER RUSSIAN OCCUPATION

All Ukrainians who remained in the country after the invasion are at risk of being disconnected, put under digital surveillance, and experiencing online censorship and filtering. Internet shutdowns, total or partial, are very frequent; 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. At the same time, some Ukrainian users face higher risks than others. We need to understand these differences through first-hand research. Stressing the nuances of connection and internet infrastructure politics under severe geopolitical

stress helps us to provide adequate and regionally appropriate support.


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. Ukrainians living in occupied territories, for example, face problems like surveillance of their daily communications by Russian occupants, to which encryption seems an obvious solution. Using encrypted calls (over WhatsApp, for instance) to speak with relatives who live outside occupied territories, instead of relying on simple GSM calls, quickly became common practice for avoiding surveillance. Ukrainians under occupation also experience intense online censorship and disinformation campaigns pushing Russian propaganda.


In response, both specialised digital security trainers and ordinary citizens help spread Virtual Private Networks (VPN) and secure messaging applications, for example Signal, to protect the content of communications and circumvent censorship. Canadian NGO eQualit.ie, for example, set up servers in several major Ukrainian cities, including in places under Russian occupation. These servers allow people to communicate locally by using federated end-to-end encrypted tools, such as Element  or Delta Chat , which work even during internet shutdowns. As many Ukrainians in the occupied territories are involved in communicating sensitive information, like details about the position of Russian troops, considerable effort has been expended toward promoting these encrypted tools.

155, 156



Is encryption the answer for high-risk users?

Encryption is not always—or not only—the 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 Crimea or Kherson . These users' digital security practices included secure messaging tools and other privacy-enhancing technologies. But rather than focusing on downloading encryption tools, such as Tor, or encrypted messaging services, such as Signal, high-risk users, and the digital security trainers that advise them, instead focus on developing tailored

responses. Digital security trainers understand risk as highly contextual and rapidly changing, which makes digital security a multi-layered, social—rather than purely technical—process .

This localised understanding of threat led us to conclude that more, or better, encryption is not always the answer for high-risk users, unlike what many advocates of privacy-enhancing technologies believe. In Kherson, an important port city under Russian occupation, Ukrainian users are at a high risk of device seizure. As a result, they consider relying on less commonly used or more technically sophisticated encrypted messengers a risk in its own right. The mere fact of having certain apps on one's phone (such as Signal, Tor or even Telegram) can raise suspicion and result in bodily harm or even life-threatening situations at the routine phone checks conducted by Russian soldiers.

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. We also found that digital security trainers emphasise the importance of communicational autonomy and physical security, given that shutdowns and blackouts are the main concern of Ukrainian users both in occupied and unoccupied territories. Power banks, solar batteries, extra phones, mobile routers, and even Starlink antennas became the focus, alongside psychological self-help tutorials and first-aid classes. Encryption receded into the background, while the accessibility of communication became vital.

THE IMPORTANCE OF CONTEXT

For the specific threats that many high-risk users in occupied Ukraine face, the particularities of the Russian Occupation turn out to be key in defining people's communication practices. Or put more plainly, when it came to ensuring safe communication for those most at risk—like, for example, the occupied peoples of Kherson—the familiarity with and inconspicuousness of particular tools 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. 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. Our thinking of infrastructural politics—or security in war situations—should always begin with this fact.

159 Notes:

155. <https://element.io>

156. <https://delta.chat/fr>

157. Ermoshina, K. and Musiani, F. 2022. *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties*. Manchester, UK: Mattering Press.

158. See Ermoshina and Musiani, op. cit.; see also Kazansky, B. 2021. 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society* 8 (1). <https://doi.org/10.1177/2053951720985557>