SoK: Internet Censorship in the Full-Scale Russian Invasion of Ukraine

Mushkie Gurevich (cmgurevich)
Elizaveta Kabaeva (ekabaeva)
Stella Lee (kangheelee)

Abstract

Since the beginning of the full-scale Russian invasion of Ukraine in February 2022, both Russia and Ukraine have enacted extensive online censorship practices and experienced attacks on internet infrastructure. Existing research falls into two categories: studies capturing censorship events immediately after the escalation of the war, and studies documenting ongoing or more recent incidents. In this SoK, we synthesize four years of censorship-related findings across technical, political, and social domains. By consolidating disparate measurement studies, legal analyses, and examinations of civilian harms, we provide an integrated understanding of how information control has evolved throughout the conflict. Our goal is to offer a comprehensive, up-to-date overview that can inform future research, help evaluate defensive strategies, and deepen understanding of information warfare in modern conflicts.

1 Introduction

Russia's full-scale invasion of Ukraine in February 2022 initiated one of the most significant periods of information warfare in recent history. Both Russia and Ukraine have engaged in censorship practices, internet restrictions, and information control strategies that affect civilian access to communication, the availability of online content, and the stability of critical services.

Although many researchers have examined censorship during this conflict, the resulting literature is fragmented. Early work concentrated on attacks and disruptions immediately following the invasion, while later studies analyze long-term patterns, evolving censorship mechanisms, and the broader social and political implications. As the Russo–Ukrainian War continues, a systematic appraisal of the entire body of censorship-related research is needed.

This SoK synthesizes findings across technical measurement studies, socio-political analyses, legal perspectives, and examinations of civilian harms. Our objective is to provide a clear and comprehensive understanding of how internet censorship has unfolded throughout the conflict, what mechanisms have been used, what consequences have emerged, and what gaps remain for future work.

2 Related Work

Existing research on censorship in the Russo–Ukrainian War falls into three main thematic areas: (1) general overviews of censorship and information control, (2) technical and measurement-based studies, and (3) socio-political analyses of legal and human-rights implications.

General overviews include discussions of propaganda, information control, and the legal frameworks that govern speech restrictions. For example, Kaye examines censorship, surveillance, and state pressure in Russia and evaluates responses by Ukraine, the EU, and technology companies, highlighting tensions between wartime measures and international human rights obligations.[2] Koltay similarly analyzes censorship as a tool against state disinformation and the implications for freedom of expression in the context of the Russian–Ukrainian War.[4]

Technical and measurement-based studies analyze censorship mechanisms, blocking behavior, cyberattacks, and network disruptions. Singh and Acharya evaluate whether Russian infrastructure influences blocking experienced by Ukrainian users and investigate the role of Starlink in maintaining connectivity.[7] Ramesh et al. document large-scale network responses to Russia's 2022 invasion, including routing changes, outages, and filtering behavior that affect internet freedom.[6] Eichensehr surveys cyber operations during the invasion—including the Viasat satellite attack and limited but targeted wiper and DDoS campaigns—and reflects on their implications for international law.[1] Knockel et al. focus on in-platform censorship on VKontakte, analyzing moderation practices and content control within a major Russian social network.[3]

Socio-political analyses and human-centered studies explore the lived effects of censorship and cyber harm. Kulyk et

al. document how network outages, censorship, data leaks, impersonation, and disruption of online services produce both primary and secondary harms for civilians, ranging from information vacuums and communication loss to physical danger and psychological distress.[5] Tavakkoli et al. study target preferences of pro-Russian and pro-Ukrainian groups, showing that news and media, government, business, and financial services are repeatedly attacked to disrupt information flows, public interaction, and economic stability.[8]

Our work extends these literatures by synthesizing them into a unified overview that spans the full timeline of the conflict and integrates both technical findings and their sociopolitical implications. Rather than focusing on a single measurement campaign, legal framework, or attack family, we provide a structured map of censorship practices and consequences in the ongoing Russia–Ukraine conflict as it unfolds on the internet.

3 Conclusion

The Russo–Ukrainian War demonstrates how modern armed conflict is deeply intertwined with information control, internet censorship, and cyber operations. Across four years of research, scholars have documented technical attacks, platform-level moderation, state-imposed legal restrictions, and the social and psychological harms experienced by civilians.

This SoK consolidates these findings to provide a comprehensive picture of censorship practices and their consequences. While both Russia and Ukraine have engaged in forms of information control, the motivations, mechanisms, and impacts vary widely. Measurement studies reveal mixed evidence regarding the origin of network interference; legal analyses highlight tension between wartime responses and human-rights standards; and human-centered work shows that even small disruptions can cascade into significant harm.

By synthesizing these perspectives, we aim to create a foundation for future research, support critical evaluation of defensive measures, and contribute to a broader understanding of information warfare as it continues to evolve.

References

[1] Kristen E. Eichensehr. “Ukraine, Cyberattacks, and the Lessons for International Law”. In: *AJIL Unbound* 116 (2022), pp. 145–149.

[2] David Kaye. “Online propaganda, censorship and human rights in Russia’s war against reality”. In: (2022).

[3] Jeffrey Knockel, Jakub Dalek, Levi Meletti, and Ksenia Ermoshina. “Not OK on VK: An analysis of in-platform censorship on Russia’s VKontakte”. In: (2023).

[4] András Koltay. “Censorship as a Tool Against State Disinformation: The Freedom of Expression Implications of the Russian–Ukrainian War”. In: *J. INT’L MEDIA & ENT L* 10.1 (2023).

[5] Oksana Kulyk, Jari Kickbusch, and Peter Mayer. “"It’s like an explosion": Cyberwarfare harms for civilian population in Ukraine during the Russian invasion”. In: Association for Computing Machinery, 2025. DOI: 10.1145/3706599.3719906.

[6] Reethika Ramesh, Ram Sundara Raman, Apurva Virkud, Alexandra Dirksen, Armin Huremagic, David Fifield, Dirk Rodenburg, Rod Hynes, Doug Madory, and Roya Ensafi. “Network responses to russia’s invasion of ukraine in 2022: a cautionary tale for internet freedom”. In: *32nd USENIX Security Symposium (USENIX Security 23)*. 2023, pp. 2581–2598.

[7] Gursimran Singh and HB Acharya. “A Cyberspace Study of the Russia-Ukraine War”. In: (2023).

[8] N. Tavakkoli, O. Çetin, E. Ekmekcioglu, et al. “From frontlines to online: examining target preferences in the Russia–Ukraine conflict”. In: *International Journal of Information Security* 24 (2025), p. 64. DOI: 10.1007/s10207-025-00981-w.