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 Russo-Ukrainian War, and especially with the full-scale invasion of Ukraine in February 2022, Russia and Ukraine have been implicated in a significant increase in online censorship and attacks on internet infrastructure. We noticed two different types of research papers covering censorship in the Russo-Ukrainian War: the first observes the attacks that occurred immediately after the beginning of the full-scale war, while the second type focuses on current attacks. We are interested in providing a synthesis of censorship attacks that have occurred over the past four years, as the Russo-Ukrainian War is one of the most contemporary incidents of information warfare, and it provides insight on how such events play out in the current internet ecosystem. With this information, people are able to better prepare themselves against these forms of internet censorship and conduct further research into the topic.

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 categories: (1) general overviews of censorship and information control, (2) technical and measurement-based studies, and (3) socio-political ramifications of censorship and cyber operations.

General Overview

Scholars examining broad censorship and information-control practices highlight the legal, political, and institutional pressures shaping online speech during the conflict. Kaye provides an overview of Russian censorship, propaganda, surveillance, and the legal restrictions imposed on online platforms, as well as responses by Ukraine and the EU.[2] He argues that while states rely on frameworks such as the ICCPR and ECHR, wartime information-control measures raise tensions between national security and freedom of expression. Koltay similarly analyzes censorship as a tool against state disinformation, exploring the implications of speech restrictions and uneven enforcement across Europe.[4] Knockel et al. investigate platform-level censorship on VKontakte, showing how in-platform moderation practices shape the Russian online information environment.[3]

Technical and Measurement-Based Studies

Measurement-driven analyses constitute a large portion of research on wartime information controls. Singh and Acharya study censorship experienced by Ukrainian users, including DNS blocking, access failures, attribution using traceroute, and the potential role of Starlink in circumventing Russian interference.[7] Their findings show limited evidence of Russian-origin blocking and suggest that Starlink does not significantly alter the network-layer censorship landscape.

Ramesh et al. conduct a large-scale analysis of network responses immediately following the 2022 invasion, documenting routing changes, filtering mechanisms, outages, and the broader impact on internet freedom.[6] Eichensehr examines cyber operations such as the Viasat satellite attack, limited wiper malware deployments, DDoS campaigns, and the unexpectedly modest role of cyberattacks during the initial invasion.[1]

Tavakkoli et al. analyze attack patterns across sectors, identifying targeted disruptions against news media, government services, financial systems, and essential consumer platforms.[8] Their work shows strategic timing of attacks, repeated victimization of high-impact websites, and limited uptake of DDoS protection across affected domains.

Socio-Political Ramifications

Human-centered and socio-political studies emphasize the consequences of censorship and cyber operations on civilians. Kulyk et al. document how network outages, censorship, data breaches, impersonation, and disrupted communication produce cascading harms, including inability to verify safety of family members, loss of access to critical services, exposure of sensitive information, and increased psychological distress.[5] Their findings show that seemingly minor disruptions can trigger severe secondary harms, erode public trust, and impede effective decision-making during crises.

Tavakkoli et al. further emphasize how strategically timed cyberattacks—especially those targeting media and government services—can shape public perception, destabilize daily life, and create social unrest.[8]

Summary

Our work extends this literature by providing a systematic overview that integrates these technical, legal, and socio-political perspectives. Unlike studies that focus narrowly on short-term attacks or isolated mechanisms, we synthesize four years of censorship practices, infrastructure disruptions, and civilian impacts to offer a comprehensive map of information control throughout the ongoing Russia–Ukraine conflict.

3 Project Preparation and Prerequisites

As our work is a summary of existing knowledge on censorship in the Russo–Ukrainian War since 2022, we do not require any technical infrastructure or specialized tooling to complete the project. Our SoK relies on systematically collecting, reviewing, and synthesizing prior scholarship rather than generating new measurements or datasets.

Our preparation consists of assembling a comprehensive and reasonably scoped corpus of sources, including technical studies, legal analyses, and socio-political examinations of information control during the conflict. We then organize these insights into an accessible and coherent entry point for understanding internet censorship as it has evolved throughout the ongoing war.

4 Evaluation

Our evaluation focuses on the breadth and balance of coverage across the full timeline of the conflict. A fair SoK must avoid overrepresenting one side of the conflict or restricting its analysis to a narrow period of events. Accordingly, we assess our work by ensuring that censorship practices, disruptions, and information-control strategies from both Russia and Ukraine are represented and contextualized.

We also evaluate completeness by examining whether our synthesis captures major incidents and trends from the beginning of the full-scale invasion through the present. This approach allows us to provide a comprehensive overview rather than a partial or time-limited snapshot of wartime information controls.

5 Ethics

Our work does not introduce new data collection, experimentation, or interaction with human subjects. As a synthesis of publicly available research, it carries no direct ethical risks. We aim to present prior findings impartially and accurately within the constraints of our six-page format, acknowledging differing perspectives while avoiding normative judgments about state actions or policy decisions.

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.