

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

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

Abstract

Russia’s full-scale invasion of Ukraine in February 2022 initiated a long period of censorship attacks affecting civilian populations and critical infrastructure. This systematization of knowledge summarizes research across technical measurements, socio-political analyses, and legal perspectives to provide a comprehensive understanding of how internet censorship has been used throughout the conflict, examining techniques including DDoS attacks, DNS and BGP manipulation, TCP/HTTP interference, TLS handshake delays, satellite attacks, and wiper malware deployments. Our analysis reveals that while Russia initially attacked Ukrainian infrastructure, it has since focused predominantly on isolating itself from the global internet and censoring its own citizens, with evidence showing intensifying restrictions through 2025. We also identify a significant lack of technical studies on recent developments and insufficient attention to domestic censorship as a war tactic.

1 Introduction

Russia’s full-scale invasion of Ukraine on February 24, 2022 initiated one of the most significant periods of information warfare in recent history. Both Russia and Ukraine, as well as other countries taking sides in the conflict, have engaged in censorship practices, internet restrictions, and information control strategies that affect civilian access to communication services and online content, and the stability of critical services. Russia is the main offender, using censorship techniques to effectively isolate itself from the global internet, but the retaliatory actions of other countries have exacerbated the situation. 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 the few later studies that exist analyze evolving censorship mechanisms and the broader social and political implications. As the Russo-Ukrainian War continues, a thorough review

of the entire body of censorship-related research is needed. This summary of knowledge (SoK) synthesizes findings across technical measurement studies, socio-political analyses, and legal perspectives. 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 Technical Overview

2.1 Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks have played a prominent and evolving role throughout the Russia–Ukraine conflict, appearing both in the early stages of the invasion and in the sustained hacktivist campaigns that followed. In the weeks immediately preceding the February 2022 invasion, Russian military-linked actors conducted a DDoS attack that briefly disrupted access to several Ukrainian government websites and the country’s two largest banks, representing one of the first visible indicators of coordinated online operations targeting Ukrainian institutions.

As the conflict progressed, DDoS attacks became the most common form of cyber activity, driven not only by state actors but overwhelmingly by pro-Ukrainian and pro-Russian hacktivist collectives. DDoS attacks constituted 71–87% of all recorded cyber incidents in Ukraine across late 2022 and early 2023, and similar surges were observed in Russia and other countries. Analysis of 4,612 victim domains shows that pro-Ukrainian groups targeted 3,090 domains while pro-Russian groups targeted 1,522 domains, with both sides displaying distinct temporal and strategic patterns [13].

The timing of attacks reveals coordinated campaigns rather than ad hoc disruption. Pro-Ukrainian groups exhibited peak activity in May–July 2022, including a large-scale campaign on February 26, 2022 that targeted more than 150 Russian domains. Pro-Russian activity intensified later in the year, with

notable peaks in May, June, September, and October, often in response to political events such as sanctions, mobilization announcements, or restrictions on Russian transit. Both sides showed a tendency to concentrate efforts on specific days, with attacks occurring most frequently on Saturdays, Sundays, and Mondays.

Sector-level analysis indicates that DDoS attacks were not aimed primarily at military infrastructure but rather at civilian-facing and high-visibility domains. News and media sites were the most frequently targeted sector, followed by government, business, finance, e-commerce, and travel services. Many of these domains faced repeated attacks, suggesting deliberate, sustained pressure rather than incidental selection. Despite the scale of these operations, 77.9% of victim domains lacked DDoS protection, and few upgraded their defenses following attacks [13].

Overall, DDoS attacks in this conflict illustrate both the persistence of low-level, easily repeatable disruption tactics and the increasing significance of hacktivist coordination. While early incidents reflected conventional state-linked operations, later surges demonstrate how DDoS campaigns became a central tool for influencing public perception, straining online services, and imposing cumulative psychological and economic pressure during wartime.

2.2 Domain Name System (DNS) Manipulation

Censorship via manipulation of the Domain Name System (DNS) protocol to block access to webpages has been observed in Russia and Ukraine since February 2022, implemented both by and against Russia. DNS-based censorship is generally detected by sending DNS queries to target name servers and observing their behavior from multiple vantage points. While DNS manipulation remains a relatively small share of censorship techniques used in this conflict, it has increased since the onset of the invasion [9].

DNS manipulation has been implicated in impeding the reachability of Russia-based webpages for users outside the country, particularly government domains. Resolution for 18 of 623 tested Russian government domains consistently failed in at least one of fifteen countries measured, compared to successful resolution from a Russian vantage point. Queries for an additional five domains failed with timeouts in eight countries, with errors originating from the same two Russian name servers [9].

DNS has also been used to prevent Russian users from accessing foreign webpages as part of post-invasion sanctions. Using a technique similar to traceroute to distinguish internal censorship from foreign geoblocking, researchers found that

DNS queries for 68 out of 8,763 popular domains did not return IP addresses when sent from Russian vantage points. These failures occurred at authoritative or organizational name servers rather than local resolvers, and many affected domains belonged to foreign governments and educational organizations [9].

However, no clear evidence of DNS manipulation has been found to affect users in Ukraine. DNS queries for 612 websites identified as potentially blocked in Ukraine in March 2022 were re-tested in July 2022, revealing no interception or spoofing and indicating normal DNS behavior following the onset of the war [12].

2.3 Transmission Control Protocol (TCP) Manipulation

Traffic manipulation at the Transmission Control Protocol (TCP) layer was investigated during the early months of the war, focusing on whether Russian networks interfered with Ukrainian traffic through TCP reset injection or connection termination. Using a multi-protocol traceroute tool capable of crafting packets across HTTP, TLS, DNS, UDP, ICMP, and TCP, researchers examined whether censorship infrastructure along Ukrainian or Russian autonomous systems actively disrupted TCP connections.

Despite concerns that Russian networks might weaponize TCP-level filtering, empirical evidence showed minimal use of TCP-based censorship. Across hundreds of tested domains, researchers found no cases where Russian networks injected TCP reset packets to terminate Ukrainian client connections, aside from limited instances involving Russian-hosted sites returning explicit block pages or HTTP 403 errors. Russian networks appeared on many routing paths, demonstrating visibility but not active TCP-layer manipulation [12].

Temporal comparisons of measurements collected in March and July 2022 indicate that TCP-level censorship did not increase as the conflict escalated. In fact, the number of unreachable Ukrainian websites declined over time, and no new use of TCP-based filtering or middlebox interference was observed. Although Starlink was widely discussed as a censorship-resistant connectivity option, it did not appear in TCP-level routing paths and did not influence TCP-layer reachability in these measurements [12].

Overall, TCP-layer interference played a limited operational role in wartime censorship. While TCP reset injection is commonly associated with large-scale censorship systems elsewhere, such techniques were largely absent in the Russo-Ukrainian War, with disruptions instead stemming from higher-level mechanisms such as DNS and application-layer controls.

2.4 Hypertext Transfer Protocol (HTTP)

HTTP reachability was examined to determine whether Russian or Ukrainian networks engaged in application-layer censorship during the early months of the war. Researchers conducted large-scale tests of HTTP and HTTPS access using automated browsing via Selenium, capturing response behaviors such as status codes, block pages, redirections, and content anomalies.

When HTTP requests were issued from Ukrainian vantage points in March 2022, 396 websites failed to load despite being reachable from U.S.-based control servers. These failures manifested as either hard failures or soft failures such as HTTP 403 responses, CAPTCHA challenges, or custom block pages. By July 2022, the number of detected failures declined significantly, with remaining issues attributed primarily to measurement noise rather than systematic filtering [12].

To distinguish genuine censorship from server-side access control, researchers analyzed HTTP response bodies and lengths, identifying pages containing terms such as “access denied” or “forbidden.” This analysis revealed 163 instances of soft failure, most of which reflected server-level policies rather than state-imposed HTTP filtering, particularly for Russian websites restricting foreign access.

Traceroute measurements using HTTP-crafted packets revealed no evidence of HTTP-level interference by Russian networks toward Ukrainian users. No payload modification, keyword filtering, or injected block pages were observed, and no application-layer middleboxes were detected on paths traversing Russian autonomous systems. Overall, access issues stemmed primarily from server decisions, DDoS-related overload, or transient network instability rather than protocol-level manipulation of HTTP traffic.

2.5 Transport Layer Security (TLS) Handshake Delays

Time-series measurements indicate that the time required to establish TLS handshakes for Russian autonomous systems increased significantly following the invasion, reaching average delays of up to three seconds between February 2022 and January 2023. This contrasts sharply with normal TLS handshake times, which typically occur within milliseconds.

The most likely explanation for this increase is systematic packet inspection. Notable increases in latency followed a July 2022 Russian law imposing fines on telecommunications operators that failed to install traffic inspection equipment, and a July 2023 announcement enforcing those penalties [8]. The longest delays were observed for websites related to news, communication, and human rights organizations, with some sites becoming effectively unreachable [10]. These findings

provide recent evidence that censorship within Russia has intensified as the war continues.

2.6 Border Gateway Protocol (BGP) Withdrawals and Hijacks

The Border Gateway Protocol (BGP), which governs inter-network routing, has been manipulated to isolate Russia from the global internet since February 2022. A substantial increase in BGP announcements and withdrawals was observed during the lead-up to the invasion, accompanied by increased latency on paths between Ukrainian and Russian networks as relationships shifted from peering to transit [8].

Geographic correlation analysis links Russian military activity to BGP outages, with peak interruptions in Ukraine occurring on the day of the invasion and disruptions in Russia peaking several days later [14]. Russia also withdrew BGP routes to certain media organizations, including Radio Free Europe, constituting a form of media censorship. In addition, Russian agencies and businesses withdrew routes to their own websites, likely to mitigate DDoS attacks [9].

In March 2022, following the prohibition of Twitter and Facebook, the Russian ISP RTComm inadvertently advertised a Twitter prefix to the global internet. Due to the absence of RPKI authorization, many networks rejected the route, limiting the scope of the hijack [9].

2.7 Satellite Attacks

Cyber and physical attacks on Ukrainian internet infrastructure escalated in the weeks leading up to the invasion. On February 24, 2022, an attack against Viasat’s satellite network disrupted communications for Ukrainian government, military, and civilian users, with spillover effects across Europe [5].

This incident prompted Ukraine to seek support from Starlink, which provided satellite connectivity to maintain communications. Starlink infrastructure itself became a target, with reports of terminal blocking and threats of missile strikes against satellites [5]. Despite its strategic importance, Starlink’s impact was not observable at the network layer. Traceroute measurements from within Ukraine revealed no Starlink autonomous systems on routing paths, indicating limited integration into broader internet traffic [12].

2.8 Wiper Malware Deployment

Contrary to expectations of widespread destructive cyber operations, researchers observed only sporadic deployment of data-wiping malware in Ukraine. Multiple wiper families, including CaddyWiper, were detected before and shortly after the invasion, primarily targeting government and critical infrastructure systems [2].

Despite their destructive intent, these wipers caused limited large-scale disruption. One explanation is the effectiveness of Ukrainian and allied cyber defenses, with rapid detection and response by government agencies and private companies such as Microsoft [11]. Another explanation is strategic restraint by Russian actors, potentially informed by concerns about uncontrolled spillover similar to previous incidents such as NotPetya [3].

Although their impact was limited, these deployments highlight the persistent threat of low-level destructive cyber operations. They exemplify the gray-zone tactics characteristic of the conflict, imposing recovery costs and uncertainty without producing strategically decisive effects.

3 Socio-Political Implications

The conflict has blurred the line between state and non-state actors, with hackers aligning themselves with both sides. Ukraine’s minister of digital transformation created an “IT Army” that mobilized thousands of participants to disrupt Russian entities, while ransomware groups aligned with Russia promised retaliation against Western targets, raising complex questions of state responsibility [1].

Russia enacted laws to suppress independent reporting and dissent, constructing a highly restrictive information space. Independent media outlets were removed from public discourse and replaced with state-sponsored disinformation. In response, the European Union banned broadcasts from RT and Sputnik, citing disinformation and security concerns, though scholars question whether such bans meet international human rights standards [4].

Technology companies faced conflicting pressures from governments and users. Platforms were urged by Ukraine to exit the Russian market while simultaneously complying with Russian censorship demands [4]. Social media companies also altered enforcement policies, with Meta temporarily permitting calls for violence against Russian military personnel, a shift that raised serious concerns about unchecked private governance of speech [6].

Censorship produced significant civilian harms, including lack of access to information, communication, and essential services. In occupied territories, information vacuums prevented residents from understanding local and national events. Russian forces disseminated disinformation to undermine trust in Ukrainian leadership and encourage collaboration, including impersonation of officials and hijacking of broadcast signals [7].

The news and media sector experienced the highest volume of DDoS attacks, with consistent targeting throughout the conflict. This sustained pressure reflects a deliberate strat-

egy to disrupt information flows and prevent populations from accessing reliable news, reinforcing the broader socio-political impacts of wartime censorship [13].

4 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.

5 Conclusion

Our summary of knowledge has established that censorship in the Russo-Ukrainian war comes from many sources, but impacts Russian citizens the most. During the beginning of the war, Russia carried out attacks on Ukrainian internet infrastructure, but since then has focused more on withdrawing access to its information from the global internet and censoring its own citizens. The Russian government systematically reduces democratic information sources, causing citizens to be isolated from critical thinking and free speech. Additionally, censorship has created severe information vacuums in occupied Ukrainian territories, preventing residents from accessing reliable information about events in their cities and country. This also results in populations on both sides of the conflict being less willing to engage with political information and people in uninvolved countries being less aware of the situation as it unfolds. While many studies on censorship and other forms of internet attacks were done in the year following the invasion in February 2022, the pace of research on this conflict as it develops has slowed down, even as the studies that have been done on more recent developments have shown an increase in censorship. Moreover, current research centers on cross-border cyberattacks, while overlooking domestic censorship as a war tactic. Political and legal studies have realized the implications of Russia’s split from the global internet and the retaliation in the form of internet sanctions taken on by tech companies, as well as educational and government organizations, but minimal technical research has focused on recent developments in implementation. Further research should expand the present state of knowledge around censorship in this war by analyzing the changes in previously observed patterns to determine the areas in which censorship has increased, decreased, or shifted in its implementation, as well as the impacts, especially on Russian citizens and occupied populations.

References

- [1] Kristen E Eichensehr. “Ukraine, cyberattacks, and the lessons for international law”. In: (2022).
- [2] Sergiu Gatlan. “New CaddyWiper data wiping malware hits Ukrainian networks”. In: *Wired*, March (2022).
- [3] Andy Greenberg. “The untold story of NotPetya, the most devastating cyberattack in history”. In: *Wired*, August 22 (2018).
- [4] David Kaye. “Online propaganda, censorship and human rights in Russia’s war against reality”. In: (2022).
- [5] Alexandros Kolovos. “Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict”. In: *Air & Space Management and Control Laboratory, OCCASIONAL PAPER 3* (2022).
- [6] 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).
- [7] Oksana Kulyk, Jari Kickbusch, and Peter Mayer. ““It’s like an explosion”: Cyberwarfare harms for civilian population in Ukraine during the Russian invasion”. In: *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 2025, pp. 1–7.
- [8] Valerio Luconi and Alessio Vecchio. “Impact of the first months of war on routing and latency in Ukraine”. In: *Computer Networks* 224 (2023), p. 109596.
- [9] 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.
- [10] Dheeman Saha, Afsah Anwar, and Abdullah Mueen. “Internet Censorship through the Lens of Time Series Analysis”. In: *Proceedings of the 17th ACM Web Science Conference 2025*. 2025, pp. 534–539.
- [11] David E Sanger, Julian E Barnes, and Kate Conger. “As tanks rolled into Ukraine, so did malware. Then Microsoft entered the war”. In: *The New York Times* 28 (2022).
- [12] Gursimran Singh and Hrishikesh B Acharya. “POSTER: a cyberspace study of the Russia-Ukraine war”. In: *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*. 2023, pp. 1016–1018.
- [13] Nasim Tavakkoli, Orçun Çetin, Emre Ekmekcioglu, and Erkey Savaş. “From frontlines to online: examining target preferences in the Russia–Ukraine conflict”. In: *International Journal of Information Security* 24.1 (2025), p. 64.
- [14] Zisis Tsiatsikas, Georgios Karopoulos, and Georgios Kambourakis. “The Effects of the Russo-Ukrainian War on Network Infrastructures Through the Lens of BGP”. In: *European Symposium on Research in Computer Security*. Springer. 2022, pp. 81–96.