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 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 conflicts 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. Their analysis of 4,612 victim domains shows the pro-Ukrainian groups targeted 3,090 domains while pro-Russian groups targeted 1,522 domains, with both sides displaying distinct temporal and strategic patterns.

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" was the most frequently targeted sector, followed by "Government," "Business," "Finance," "E-commerce," and "Travel," reflecting attempts to disrupt information flows, public services, and everyday economic activity. Many of these domains faced repeated attacks, suggesting that deliberate, sustained pressure than incidental selection. Despite the scale of these operations, 77.9% of victim domains lacked DDoS protection, and few upgraded their security post-incident.

Overall, DDoS attacks in this conflict illustrate both the persistence of low-level, easily repeatable disruption tactics and the increasing significant role of hacktivist coordination. While early DDoS incidents reflected conventional state-linked operations, the subsequent surge in hacktivist-driven attacks demonstrates how DDoS campaigns have become 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 various vantage points. While DNS manipulation remains a small share of censorship techniques that have been used in this conflict, it has been observed to increase since the onset of the invasion (ramesh2023network).

DNS manipulation has been implicated in impeding reachability of Russia-based webpages for users outside the country, particularly government domains. Resolution for 18 of 623 (2.89%) tested Russian government domains consistently failed in at least one of 15 countries measured, compared to successful resolution from a Russian vantage point. Queries for a further five domains failed with a timeout in eight countries, with errors originating from the same two Russian name servers (ramesh2023network).

DNS has also been used to prevent Russian users from accessing foreign web pages, as part of the movement to impose sanctions on Russia following its invasion of Ukraine. Using a technique similar to traceroute to distinguish internal censorship from foreign geoblocking, DNS queries for 68 out of 8,763 of popular domains tested (0.78%) did not return IP addresses when sent from Russian vantage points. The failures occur at the authoritative nameserver or an organizational server, as opposed to local DNS resolvers in Russia. Many of the affected domains belong to foreign governments and educational organizations (ramesh2023network).

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 probed in July 2022, only to find that none of them were intercepted or spoofed, indicating normal behavior for DNS in Ukraine following the onset of the war (singh2023poster).

2.3 Transport Control Protocol (TCP) Manipulation

Traffic manipulation at the Transmission Control Protocol (TCP) layer was investigated during the early months of the war, with particular attention to whether Russian networks interfered with Ukrainian traffic using mechanisms such as TCP reset (RST) injection or connection termination. Using a multi-protocol traceroute tool capable of crafting packets across HTTP, TLS, DNS, UDP, ICMP, and specifically TCP, researchers examined whether censorship infrastructure along Ukrainian or Russian Autonomous Systems (ASes) actively disrupted TCP connections. Their methodology triggered censor responses, including TCP RST packets, at controlled hop distances, enabling the attribution of interference to specific network locations.

Despite concerns that Russian ASes might weaponize TCP-level filtering to cut off Ukrainian access to foreign websites, empirical evidence showed minimal use of TCP-based censorship. Across hundreds of tested domains, researchers found no cases where Russian ASes injected TCP RST packets to terminate Ukrainian client connections, with only a small number of exceptions involving Russian-hosted sites returning explicit block pages or 403 Forbidden errors. Russian networks did, however, appear on numerous routing paths, demonstrating visibility but not active TCP-layer manipulation. Surprisingly, researchers observed more TCP connection resets originating from non-Russian networks, including U.S.-based ASes terminating connections to major platforms such as Amazon and IMDb.

Temporal comparisons of measurements collected in March and July 2022 indicate that TCP-level censorship did not increase despite escalating conflict. In fact, the number of unreachable Ukrainian websites declined over time, and multi-protocol traceroute revealed no new use of TCP-based filtering, RST injection, or middlebox-level manipulation by Russian infrastructure. Starlink, although widely discussed as a censorship-resistant connectivity option, did not appear in any TCP-level network paths and therefore did not influence TCP-layer reachability in the study.

Overall, findings suggest that TCP-layer interference played a limited operational role in wartime censorship. While TCP RST injection is commonly associated with state-level censorship systems elsewhere (e.g. China's Great Firewall), such techniques were largely absent in the context of the Russo-Ukraine War. Instead, disruptions stemmed primarily from higher-level mechanisms, such as DNS

2.4 Hypertext Transfer Protocol (HTTP)

HTTP reachability was examined to determine whether Russian or Ukrainian networks engage in application-layer censorship during the early months of the war. Researchers conducted large scale tests of both HTTP and HTTPs access using automated browsing via Selenium, allowing them to capture HTTP response behaviours, including status codes, block pages, redirections, and content anomalies. These measurements provided insight into whether websites were inaccessible due to network layer filtering, server side restrictions, or protocol specific interference.

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 complete non-responses (hard failures) or altered HTTP responses (soft failures), e.g. 403 Forbidden messages, CAPTCHA challenges, or custom block pages. By July 2022, these accessibility issues declined in detection, with only a small number of remaining failures being accredited to noise rather than systematic filtering.

To be able to distinguish between 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 approach revealed 163 instances of soft failure, where HTTP returned a valid 200 or 403 response but the delivered content revealed signs of blocking. Importantly, most of these soft failures reflected server level policies rather than state imposed HTTP filtering, especially for Russian websites restricting access from foreign countries.

Using a traceroute tool that collected HTTP-crafted packets, researchers attempted to locate censorship infrastructure that might intercept or modify HTTP traffic in transit. The results, however, showed no evidence of HTTP-level interference by Russian ASes toward Ukrainian users. No injection of block pages, keyword filtering, or HTTP payload manipulation was observed, and HTTP probing revealed no middlebox performing application layer censorship on paths through Russian networks.

Overall, while HTTP testing identified numerous temporary connectivity problems and server-enforced blocks, the study found no systematic use of HTTP paper censorship in the Russia-Ukraine conflict. Access issues stemmed primarily from server decisions, DDoS related overload, or transient network instabilities, rather than a protocol level manipulation of HTTP traffic.

2.5 Transport Layer Security (TLS) Handshake Delays

Time-series data shows that the time to establish a TLS handshake for Russian ASes takes significantly longer than normal, and these delays have increased up to a 3 second average (compared to a normal TLS handshake, which takes milliseconds) in the three year period since the invasion (February 2022–January 2025). The most likely explanation for this change over time is systematic packet inspection, with significant increases observed following the July 2022 Russian law that levied fines for telecommunication operators that have not installed TSPI devices (which are used for censorship), and the July 2023 announcement that these fines would be enforced. The websites with the longest delays (some so long they are effectively unreachable) are those for news, communication, and human rights organizations (saha2025internet). This study provides recent evidence that censorship in Russia is intensifying as the war continues.

2.6 Border Gateway Protocol (BGP) Withdrawals and Hijacks

The Border Gateway Protocol (BGP), which implements routing of information between computer networks, has been manipulated to segregate Russia from the global internet, especially since February 2022. A substantial increase in BGP announcements and withdrawals was observed leading up to and during the beginning of the invasion. Additionally, latency on paths from ASes to Ukraine to those in Russia has increased, partially due to the relationships between them switching from peering to transit (luconi2023impact). Geographic data has been used to establish a correlative link between Russian military attacks on Ukraine and BGP outages, with the peak interruption in Ukraine was on the day of the invasion, and for Russia several days later (tsiatsikas2022effects).

By making changes to BGP announcements, routes to certain ASes can be cut off, which Russia has done to enact censorship and limit the effects of censorship against them. For example, the withdrawal of the BGP routes to the Ukrainian and Moscow networks of Radio Free Europe is an instance of media censorship. Furthermore, Russian government agencies and businesses have withdrawn routes to their websites, presumably to prevent DDoS attacks against them (ramesh2023network).

An interesting incident involving BGP occurred in March 2022, after Russia prohibited access to Twitter and Facebook in the country. The Russian ISP RTComm, in trying to implement this censorship order, advertised a prefix belonging to Twitter to the global internet on March 28, 2022. Due to a similar incident involving Twitter and Myanmar in 2022, some ASes managed to avoid the hijacked route, as it was not authorized with RPKI validation (ramesh2023network).

2.7 Satellite Attacks

Cyber-attacks against Ukraine, including strikes to its physical internet infrastructure, escalated in the months and weeks leading up to the ground invasion. One of the most significant was an attack on February 24, 2022 against Viasat Satellite Communications, a network operated by an American company that provides broadband internet services across Europe. This attack, which Russia has been implicated in, caused disruptions not just to the Ukrainian government, military, and citizens, but had effects in other European countries, leading to widespread condemnation (kolovos2022commercial).

This major satellite attack motivated the Ukrainian government to request the help of Starlink, which has provided satellite service and ground terminals to increase connectivity in Ukraine and support the Ukrainian Armed Forces. However, Starlink infrastructure has also been subject to attack, including blocking of terminals, as well as threats from Russian government officials, who are considering missile strikes against satellites (kolovos2022commercial).

Starlink has positioned itself as a disruptor in the online conflict between Russia and Ukraine as well, pledging to provide support for internet users in Ukraine to use their systems to bypass Russian censors. However, any benefits of Starlink in Ukraine have not been observable at the network layer. Looking at the graph of major Autonomous Systems (ASes) in Ukraine reveals only one Starlink AS, which is a stub, connected only to the largest internet provider in the country, but not providing for any through traffic. The same study conducted many traceroute measurements from servers in Ukraine, and found no Starlink ASes in any of them, although many Russian ASes were still present (singh2023poster).

2.8 Wiper Malware Deployment

In contrast to expectations that Russia would rely heavily on destructive cyber operations during the invasion, researchers observed only sporadic deployments of data-wiping malware in Ukraine. Wipers, or malware designed to irreversibly corrupt and destroy data, were discovered both in the weeks leading up to the invasion and immediately afterwards, yet their overall operational impact remained surprisingly limited.

Multiple strains of wiper malware were detected on Ukrainian networks, including newly identified families such as CaddyWiper [1], as well as others linked to Russian military intelligence. These wipers were deployed against government and critical infrastructure systems, but available evidence indicates that the malware caused minimal damage at scale, failing to produce the widespread disruption that many analysts anticipated at the outset of the conflict.

The limited effect of these operations has prompted competing explanations to its ineffectiveness. One possibility is that Ukrainian and allied cyber defenses successfully mitigated or neutralized wiper infections, reflecting years of experience responding to Russian cyber intrusions. Researchers note that government agencies and private companies, particularly Microsoft [2], rapidly detected and shared indicators of compromise, allowing patches and signatures to be deployed within hours. Another possibility is that Russia chose not to conduct broader destructive operations, whether due to operational constraints, strategic miscalculation, or concerns about uncontrolled spillover similar to previous destructive incidents such as NotPetya [3].

Despite their modest scale, these wiper deployments highlight the persistent threat posed by low-level destructive cyber operations during armed conflict. They exemplify the broader pattern of gray-zone cyber activity observed throughout the war, operations that are disruptive enough to generate uncertainty and impose recovery costs but fall short of producing large scale, strategically decisive effects.

3 Socio-Political Implications

The conflict has provided fresh examples of the blurring between state and non-state actors, with hackers aligning themselves with both sides. Ukraine's minister of digital transformation created an “I.T. army” that drew thousands of participants who have taken Russian entities offline, while ransomware groups aligned with Russia, promising to retaliate against the West. This raises complex legal questions about state responsibility [1].

Russia adopted and implemented laws to quash independent reporting, criticism, and dissent, constructing an aggressively restrictive information space. The Russian government emptied public space of independent media and dissent while filling it with turbo-charged disinformation, undermining public institutions and individuals' ability to distinguish fact from fiction.

The Council of the European Union prohibited the broadcast of RT and Sputnik within the EU, citing disinformation, foreign interference, influence operations, and threats to public order and security. However, the researcher questions whether this ban satisfies international human rights law standards.

Technology companies found themselves caught between business models valuing user-generated content and official demands restricting that content, facing intense pressure from both the Ukrainian government to exit the Russian market and Russian government demands for content removal [2].

While disinformation efforts may pose greater risk in fragile democracies like Ukraine, undermining the information space is destructive to every democracy. The document raises concerns about paternalism, questioning whether EU citizens should not be able to see Russian propaganda products and make critical analyses themselves.

Major social media companies relaxed enforcement of their rules involving threats against Russian military personnel, with Meta allowing calls for violence against Russian and Belarusian leaders and Russian soldiers in the context of the Ukraine invasion. This represents a dangerous development where platforms change boundaries of free speech at will, without constitutional guarantee or supervision [4].

The primary harms of censorship mentioned by the participants (both civilians and politicians) of another study include a lack of information, lack of communication, lack of access to essential services, disclosure of sensitive information, impersonation, and disruption of activities. Censorship created information vacuums in the occupied territories, where residents couldn't understand what was happening around them, in their city, or in their country. Russian forces deliberately spread disinformation, telling civilians that Kyiv had fallen and no one was waiting for them, aiming to control the population and force collaboration with occupiers.

Censorship and disinformation were used strategically to influence Ukrainian behavior, with two main narratives: making Ukrainians distrust their government and military, and convincing them to stop armed resistance against Russian forces. Impersonalisation is one of the most common ways of disinformation that has relatively cheap costs so it is widely employed by Russian attackers. Russian forces hacked several websites and posted false announcements, including a fabricated appeal from Valeriy Zaluzhny (then Commander-in-Chief of the Armed Forces of Ukraine) to the military attempting to convince them to surrender. Hackers also infiltrated satellite signals for Ukrainian TV channels and replaced the broadcast feed with Russian content. These incidents aimed at broad audiences to undermine military morale and public confidence in Ukrainian leadership. Moreover, Russian forces or local collaborators know about civil activist organization members and contact them directly, impersonating the organization to ask members to return to occupied cities, claiming a new separatist version of the organization would be created there [5].

The "News and Media" sector experienced the highest number of DDoS attacks, with 687 domains targeted – the most of any sector. This sector was consistently attacked every month throughout the study period and saw the highest frequency of attacks on weekends. This systematic targeting demonstrates a deliberate strategy to control information flow and disrupt access to news, creating information vacuums that prevent populations from understanding current events [8].

4 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.

5 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.

6 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.