LSE Public Policy Review

Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience

RESEARCH

TETYANA LOKOT

LSE Press

ABSTRACT

Russia's full-scale invasion of Ukraine in February 2022 has seen the Kremlin mixing its usual external cyber warfare tactics with internet control and information manipulation approaches inspired by its internal networked authoritarian regime. I argue that Russia's interventions in the information spaces and telecommunications infrastructure in temporarily occupied Ukrainian territories demand greater scrutiny from the domains of internet governance and cyber warfare studies alike. This analysis of the 'networked authoritarian' creep of Russia's censorship and surveillance tactics beyond its borders as a part of its expanding war arsenal enables a comprehensive assessment of the impacts of both kinetic attacks on communications infrastructure and informational attacks on the digital communication space in Ukraine. The analysis also summarises Ukraine's observed capability for resistance and resilience in the face of Russia's networked authoritarianism in the context of the war and discusses the implications and lessons from the events of the full-scale invasion for the future rebuilding of Ukraine and for the broader international policymaking community.

CORRESPONDING AUTHOR:

Tetyana Lokot

Dublin City University, IE

tanya.lokot@dcu.ie

KEYWORDS:

Ukraine; Russia; networked authoritarianism; internet control; internet freedom; security

TO CITE THIS ARTICLE:

Lokot T. Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience. *LSE Public Policy Review*. 2023; 3(1): 7, pp. 1–8. DOI: https://doi.org/10.31389/lseppr.85

LSE Public Policy Review
DOI: 10.31389/lseppr.85

Russia's approach to governing the internet and telecommunications inside the country has seen significant scrutiny by internet governance and digital rights scholars. They, alongside internet freedom advocates, have been rightly concerned with the narrowing space for free expression and growing crackdown on digital freedoms inside Russia [1, 2]. At the same time, Russia's external cyberwarfare strategy has gained more attention in the global cybersecurity domain, with the Kremlin using cyberattacks belligerently to support conventional military incursions (e.g., in Georgia in 2008 or in Ukraine since 2014) [3, 4] or to intervene in Western political processes through a mix of hacking and information manipulation [5, 6].

Russia's full-scale invasion of Ukraine in February 2022, however, has seen the Kremlin mixing its usual external cyberwarfare tactics with approaches inspired by its internal networked authoritarian regime. I argue that Russia's interventions into the information spaces and telecommunications infrastructure in temporarily occupied Ukrainian territories demand greater scrutiny. I also contend that an understanding of the country's internal politics and its aspirations in the digital domain is necessary to assess the implications of Russia's actions and Ukraine's potential for resistance and resilience, as well as to inform appropriate and timely policy responses from the global community.

1. RUSSIA'S NETWORKED AUTHORITARIANISM

The internet in Russia initially developed as a predominantly free and apolitical space alongside increasingly co-opted mainstream media. But over time, independent news outlets and opposition actors have come to rely on digital platforms and networked media to promote alternative and often critical narratives about the regime. The Kremlin grew increasingly concerned about the internet's destabilising potential following the wave of discontent in the Middle East and North Africa (MENA) region in the early 2010s and the ensuing 2011–2012 political unrest in Russia [7]. Further spooked by the Revolution of Dignity in Ukraine in 2013–2014, the Kremlin went to considerable lengths to wrest control of the digital space away from diverse private actors and to centralise internet governance, online censorship, and content regulation. Roskomnadzor, the Russian state's regulatory agency overseeing the internet, media, and telecommunications, has taken on a more prominent role in enforcing the full suite of internet controls. At the same time, state-sponsored actors also capitalised on the power of social media, building a presence for state-funded media on YouTube and Twitter and creating a number of anonymous channels to publish political commentary, conspiracy theories, and leaks on Telegram, the most popular messaging service in Russia [8]. A host of laws adopted in the decade since 2012 have consolidated this state control. With the first tranche, the government limited online freedoms, enabled pervasive surveillance, and policed and filtered online speech. More recent legislation passed since 2017 has sought to secure greater control over national internet infrastructure and to bring foreign digital platforms to heel.

To further support its goal of pervasive information control online, alongside seeking technological independence, Russia has adopted a far-reaching strategy of internet sovereignty. The strategy combines the Kremlin's desire to tightly control information flows and activity in digital domains inside the country that are viewed as posing threats to regime stability with a push for technological sovereignty, signalling the state's intention to develop and use homegrown technologies to avoid excessive dependency on foreign hardware, services, and software. To this end, over the past decade, Russia has introduced a robust legal framework and numerous regulations meant to shape its future sovereign internet, including further centralisation of online censorship mechanisms and the gradual takeover of telecommunications infrastructure and traffic exchange points.

Critics note that these steps remain mostly focused on securing greater control over citizen activity and anti-regime expressions within Russia [9]. But the state's lack of sufficient investment into domestic research, development, and production coupled with pressure from international sanctions mean the country is unable to completely decouple from the global internet and remains dependent on Western technologies in its public infrastructure and private sectors [10].

With the internet in Russia being pivotal to democratic transformations of the past decade, it is no wonder that control over digital space has also become a strategic priority for the regime. The

DOI: 10.31389/lseppr.85

Russian state has often taken advantage of the technologies used by people in everyday life to boost its control over its citizens and their data. The state has invested in technological innovation around e-governance services while also building extensive online censorship infrastructure, adopting restrictive data and internet regulations and enabling more sophisticated surveillance tools based on citizen data gathering and facial recognition technology. This has created a unique environment, best understood as networked authoritarianism [1], where the Russian state is both highly supportive of technological innovation and development while being increasingly restrictive and controlling towards digital spaces and online expression [11].

Although Russia's externally facing cyber warfare efforts and information manipulation tactics are receiving growing attention in foreign policy, cybersecurity, and defence policy circles, these discussions have mostly neglected to connect activity directed at foreign states or corporate actors with the internal networked authoritarian policies. With Russia's illegal annexation of Crimea and its occupation of parts of eastern Ukraine since 2014, and especially after Russia's full-scale invasion of Ukraine in February 2022, we have been able to observe the Kremlin's overlapping efforts to use cyberattacks to target Ukrainian critical infrastructure and state communications [4, 12, 13] and to impose key tenets of networked authoritarian governance in temporarily occupied Ukrainian territories [14, 15]. Understanding the impact of this two-pronged attack style and the response of Ukrainian authorities and allies on the ground is key to the successful rebuttal of Russian interference and to the strengthening of infrastructural, political, and societal resilience of the Ukrainian state and society in the context of the full-scale war.

2. THE ROLE OF DIGITAL WARFARE IN RUSSIA'S INVASION OF UKRAINE

As Boichak notes, digital technologies not only 'offer new capabilities in conducting military operations' but also bring warfare 'into the realms of communication and perception', reconstituting 'the social conditions shaping people's relationship to wars' [16 p511]. Highlighting the expanding role of digital media in modern wars, Boichak and Hoskins [17] note that while wartime information has always been contingent upon various types of communication infrastructure, the new networked environment enables a new kind of participatory warfare [18] wherein communication about – and participation in – wars is continuously shaped 'through personalised and individualised informational feeds' [17 p2]. This technology enables large-scale participation by both military and civilian actors through smartphones, messaging apps, and social media platforms. Consequently, in this new reality of war, made vivid in the 2022 Russian invasion of Ukraine, it is crucial to understand how the invading forces not only attempt to co-opt, corrupt, or control servers, energy grids, or telecommunications infrastructure remotely or kinetically but also attempt to exert influence on the occupied Ukrainian information and communication space using domestically developed networked authoritarian approaches. In the subsections below, I provide an overview of the various Russian tactics observed in temporarily occupied territories in the first year of the war in Ukraine. Within them, I discuss both Russia's kinetic attacks and its online interference and influencing activities.

2.1 TARGETING TELECOMMUNICATIONS INFRASTRUCTURE

Since it illegally annexed Ukraine's Crimean Peninsula in 2014, Russia has been targeting and weaponising internet connectivity in the Ukrainian regions under occupation. Instead of completely destroying occupied territories' internet and mobile infrastructure, Russia has instead partially subsumed it. Within Crimea and the occupied parts of the Donetsk and Luhansk regions, Russian forces have seized Ukrainian mobile base stations and internet service provider facilities, brought in domestic or newly formed mobile provider entities, and rerouted Ukrainian internet traffic through Russian exchange points. In 2014, they also laid a new undersea cable to Crimea from the Russian mainland [19].

Since February 2022, Russian invaders have similarly targeted telecommunications infrastructure in frontline areas and newly occupied Ukrainian territories, with these areas suffering partial or complete communication blackouts. According to data from Ukraine's Special Communications Service published in October 2022, over 4,000 base stations of Ukrainian telecommunications

DOI: 10.31389/lseppr.85

providers have been seized or destroyed by Russian troops since the beginning of the full-scale invasion, and more than 60,000 kilometres of fibre-optic internet cables have been captured or damaged by the Russians [20]. Throughout the months of the invasion of Ukraine, large-scale internet disruptions in several Ukrainian regions have been reported by Netblocks, a service monitoring online censorship and shutdowns [21]. In some areas, such as Ukraine's second-largest city, Kharkiv, or the strategic port city of Mariupol in southern Ukraine, the internet was disrupted as early as the first day of the invasion. Russian shelling and missile attacks targeted civilian infrastructure. This coincided with a suspected Russian cyberattack on Viasat satellite internet network serving Ukraine and much of Europe, which experienced a partial outage on 24 February, 2022 [21]. On 26 February, as the Russian troops besieged the capital of Kyiv, Ukraine's backbone internet provider, GigaTrans, which supplies connectivity to several other networks in Ukraine, also experienced a major disruption [21]. On 28 March, Ukraine's national internet provider, Ukrtelecom, experienced an extended nationwide network disruption following a major cyberattack that lasted for over 15 hours [22].

In the southern Kherson region, which was occupied by Russian forces for several months in 2022, Netblocks registered a near-total internet blackout at the end of April 2022 that affected multiple Ukrainian providers, including Ukrtelecom, Kyivstar, Vodafone, and Volia [21]. On 1 May 2022, regional provider Skynet (Khersontelecom) was able to partially restored access, yet metrics showed that connectivity on the network had been routed via Russia's internet instead of through Ukrainian telecoms infrastructure. Netblocks reported that the rerouting was done through Miranda Media [21], a Russian internet provider. This internet service provider (ISP) was set up by Russia to service users in occupied Crimea, where Ukrainian connections had been severed after the occupation [14]. Over the course of the current stage of the war, some areas, such as Kherson and parts of the region, have been liberated and have had Ukrainian connectivity restored. But in regions which remain under Russia's control, internet traffic is still rerouted through Russian suppliers, while they also co-opt Ukrainian mobile infrastructure, bringing in Russian phone numbers and SIM cards.

2.2 CO-OPTING ONLINE INFORMATION FLOWS

Destroying connectivity in Ukraine has further isolated vulnerable communities in Russia-occupied areas. It has cut them off from trusted news sources and left them unable to report on instances of torture, hostage-taking, murders, and other war crimes. Reports instead only tend to emerge after areas are liberated by Ukrainian troops. An official with Ukraine's Ministry of Digital Transformation told *Time* magazine that as a result of the disconnections, 'the people living there don't know what's happening in Ukraine, they can't call family to describe the situation, they don't know whether their relatives are alive or not' [20]. At the same time, Russia's seizure of control over telecommunications infrastructure means Ukrainian civilians in occupied regions are increasingly subject to Russian internet regulations, surveillance, and censorship characteristic of the networked authoritarian regime. This means that citizens in these areas find themselves in an information ecosystem that distorts the reality of the war by spreading disinformation through anonymous pro-war Telegram channels, blocking access to Ukrainian and Western news websites and social media platforms, and feeding highly sanitised content on Russian state media. In essence, Ukrainians in Russian-occupied territories are subjected to the same networked authoritarian restrictions that distort the information reality for those living within Russia.

Punishments for Ukrainians violating the draconian Russian internet regime in occupation are similar to those habitually faced by Russians. Russia-installed authorities physically examine the smartphones of those evacuating to Ukraine-controlled territories in search of 'patriotic' Ukrainian content and have used online surveillance to identify users whom they consider to be critical of the occupying regime or collaborating with or passing information to the Ukrainians [23]. Something as innocuous as a photo of the Ukrainian flag or Ukrainian numbers listed in a smartphone's call history has reportedly led to Ukrainians across Russia-controlled regions being detained, questioned, and abused by Russian forces [24]. As evident from the cases above, control over infrastructure and influence over information flows go hand in hand in Russia's networked authoritarian logic and are also visible in the war it is waging in Ukraine. These 'hybrid' threats to both military operations and civilian connectivity are what Ukrainian authorities and citizens have been grappling with for the past year.

DOI: 10.31389/lseppr.85

3. UKRAINIAN RESISTANCE, RECOVERY, AND RESILIENCE

Ukraine's resistance efforts in the face of Russia's attack on networks, communications, and information platforms have taken various forms. According to a July 2022 report by Microsoft [25], the Ukrainian government has successfully sustained its civil and military operations by distributing its digital infrastructure into the public cloud, where it has been hosted in data centres across Europe, to minimise the effects of both cyber- and kinetic attacks. In addition to the governmental cyber defence measures Ukraine has been taking with international partners to resist a higher percentage of Russian cyberattacks [25], there have also been more horizontal instances of resistance by grassroots hacker groups [26]. Additionally, government cybersecurity officials have successfully rallied an informal community of IT specialists and hackers in Ukraine and abroad to target Russian state and military targets online [27].

Despite electricity shutdowns and pressure and censorship by occupying authorities, Ukrainians across the country have continued to use digital communication spaces. Within these spaces, Ukrainians have had ongoing conversations about Ukraine's response to Russian invaders, the impact of the war on their lives, and the stories of Ukrainian resistance. Constellations of citizens mobilising into networked publics online to strategically use digital technology to support the resistance effort and propagate their ideas to broader audiences at home and abroad have played an important part in establishing state legitimacy and spreading unifying national narratives [16]. In occupied territories such as Kherson and Crimea, grassroots partisan movements such as Yellow Ribbon have been going offline to avoid digital surveillance and online censorship, instead plastering the city walls with printed posters and painting Ukrainian flags on every available surface [23]. Citizens active online have adopted anonymisation and circumvention tools, using virtual private networks and more secure messaging alternatives such as Signal. Others have resorted to deleting their messaging history and social media profiles, disguising their online identities, and protecting themselves from online surveillance and censorship.

Ukrainian authorities have reacted swiftly to disruptions in connectivity across the country. In some cases, as with the traffic rerouting in Kherson, there were successful attempts to reroute traffic back through Ukrainian channels days after the initial takeover [21]. Recognising the importance of this connectivity, in regions liberated from occupation, telecommunications and emergency workers have consistently been among the first to arrive, often risking their lives in areas close to the frontline to repair base stations and fibre-optic cables and reconnect infrastructure back to Ukrainian networks. In October 2022, Ukraine's Ministry of Digital Transformation reported that Ukrainian mobile operators had rebuilt 71 of their base stations in towns and cities liberated from Russian occupation since the beginning of the September counteroffensive [20]. From March to October 2022, Ukrainian telecommunications workers had restored 1,232 base stations in areas previously occupied by the invading army [20]. A number of international partners have provided Ukraine with assistance and support in rebuilding the country's bruised and battered infrastructure.

In liberated areas of Ukraine which bore the brunt of Russian destruction, officials have been setting up makeshift charging stations and wireless internet access spots using Starlink satellite internet technology [15]. In April 2022, Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, shared an image of a crowd of locals clustered around a Starlink terminal in the village of Ivankiv, in the Kyiv region, which had been liberated from Russian control days before. 'Operation of electricity and mobile communications has not been yet restored,' Fedorov wrote, 'but Starlink came on time. Locals finally are able to tell relatives that they are alive' [28].

The longer-term recovery and resilience of Ukraine's internet connectivity and information space depends on the state and industry bolstering their technological capabilities. After the physical damage and cyberattacks, the country must rebuild its infrastructure and engage ordinary citizens in the processes of countering Russian networked authoritarian influence, control, and manipulation in online spaces. As the ongoing war in Ukraine illustrates, while there are differences between these threats, the Kremlin does not pursue them separately, nor should we place them in separate analytical categories. Investments in more modern and robust telecommunications networks should go hand in hand with further decentralisation of state and critical industry data storage and cloud infrastructure.

Sustained support from European and Western allies plays a crucial role in this. In June 2022, the EU launched a digital tech hub in Slovakia to make it easier for European companies to donate equipment to sustain and rebuild Ukraine's digital and telecommunications sector and to coordinate technical support across the EU [29]. In September 2022, the European Commission agreed to associate Ukraine to the Digital Europe Programme, bolstering funding and support for industry and state institutions in the areas of computing, AI, and digital skills [29]. The country has seen similar support from corporate giants like Amazon, which in 2022 helped Ukraine transfer critical government, business, and property databases into the company's data cloud [30]. Such intergovernmental and industry efforts need to redouble after Ukraine's victory in the war. Ukraine's battle for reconstruction and sustainable connectivity is a long-term one – and it demands working with international partners whose technologies can provide the country with stable long-term support.

To counteract Russia's networked authoritarian policies, Ukraine will benefit from strengthening international cooperation in the area of cybersecurity and defence. The country's accession to the NATO Cooperative Cyber Defence Centre of Excellence in early 2023 [31] is a good example of building alliances to support efficient responses to cyberthreats – Russian and otherwise. Continued involvement in initiatives such as the EU–Ukraine Cybersecurity Dialogue and collaboration between the Ukrainian State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) should further buttress Ukraine's cyber defence capabilities.

Ukrainian citizens, whether military or civilian, will benefit from a broadening effort to increase digital literacy, empowering them to protect their privacy and their security online and to make informed decisions about verified information sources and trustworthy digital actors. The country is making visible progress in expanding digital services and data access for Ukrainians – the government should now pay the same attention to ensuring citizens' data and identities are protected from external threats, as well as giving users more control over their privacy and information (while adhering to the universal digital rights, freedoms, and norms). This can be achieved through aligning national regulatory frameworks with the best practices and policies of the European Union and other international bodies on countering disinformation and protecting internet freedom. Equally important is that state regulators and policymakers are receptive to the interventions of local and international digital rights groups calling for more citizen agency, stronger remedy and redress mechanisms, and greater platform accountability and transparency. Such efforts will make for a more equitable, more responsible, and thus a more secure and resilient internet that will contribute to the future rebuilding and revival of Ukraine.

Future-focused plans for Ukraine call for a coordinated and comprehensive strategy to strengthen defences against the full range of cyber-destructive interventions, espionage activities, and information manipulation operations, build reliable digital infrastructure, and craft robust privacy and digital rights regulations serving the interests of citizens. Meanwhile, the country's partners would do well to learn from Ukraine's lessons and pay closer attention to the full spectrum of Russia's networked authoritarian policies and activities at home and abroad.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR INFORMATION

Tetyana Lokot is Associate Professor in Digital Media and Society at the School of Communications at Dublin City University, Ireland. Her research focuses on digital media, networked authoritarianism, digital resistance, and internet freedom. She is the author of *Beyond the Protest Square: Digital Media and Augmented Dissent* (Rowman & Littlefield, 2021).

AUTHOR AFFILIATIONS

Tetyana Lokot orcid.org/0000-0002-2488-4045
Dublin City University, IE

REFERENCES

1. **Maréchal N.** Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and Communication*. 2017 Mar 22; 5(1): 29–41. DOI: https://doi.org/10.17645/mac.v5i1.808
2. **Lonkila M, Shpakovskaya L, Torchinsky P.** The occupation of Runet? The tightening state regulation of the Russian-language section of the internet. In: Wijermars M, Lehtisaari K (eds.), *Freedom of expression in Russia's new mediasphere*. London and New York: Routledge. 2020; 17–38. DOI: https://doi.org/10.4324/9780429437205-2
3. **Deibert RJ, Rohozinski R, Crete-Nishihata M.** Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*. 2012 Feb; 43(1): 3–24. DOI: https://doi.org/10.1177/0967010611431079
4. **Lokot T.** Public networked discourses in the Ukraine-Russia conflict: 'Patriotic hackers' and digital populism. *Irish Studies in International Affairs*. 2017; 28(1): 99–116. DOI: https://doi.org/10.1353/isia.2017.0011
5. **Nakashima E.** US government officially accuses Russia of hacking campaign to interfere with elections. Washington Post. 2016 Oct; p. 7.
6. **Freelon D, Lokot T.** Russian Twitter disinformation campaigns reach across the American political spectrum. *Misinformation Review*; 2020 Jan 6.
7. **Gehlbach S, Lokot T, Shirikov A.** The Russian media. In: Wengle S (ed.), *Russian politics today: Stability and fragility*. Cambridge: Cambridge University Press. 2022; 390–407. DOI: https://doi.org/10.1017/9781009165921.021
8. **Lokot T.** Telegram: What's in an app? *PONARS Eurasia*; 2018 Nov 26 [cited 2023 Mar 1]. www.ponarseurasia.org/point-counter/telegram-whats-app
9. **Daucé F, Musiani F.** Infrastructure-embedded control, circumvention and sovereignty in the Russian internet: An introduction. *First Monday*. 2021 May 1; 26(5). DOI: https://doi.org/10.5210/fm.v26i5.11685
10. **Epifanova A, Dietrich P.** Russia's quest for digital sovereignty: Ambitions, realities, and its place in the world. *German Council on Foreign Relations*; 2022 Feb 21 [cited 2023 Mar 1]. https://dgap.org/sites/default/files/article_pdfs/DGAP-Analyse-2022-01-EN_0.pdf.
11. **Lokot T.** Unfreedom monitor: Russia country report. Advox, Global Voices; 2022 Aug 25 [cited 2023 Mar 1]. https://globalvoices.org/wp-content/uploads/2022/08/Unfreedom_Monitor_Russia_Country_Report_2022.pdf.
12. **Greenberg A.** The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. 2018 Aug 22; 22.
13. **Lin H.** Russian cyber operations in the invasion of Ukraine. *Cyber Defense Review*. 2022 Oct 1; 7(4): 31–46.
14. **Ermoshina K.** 'Voices from the island': Informational annexation of Crimea and transformations of journalistic practices. *Journalism*; 2023 Jan 16. DOI: https://doi.org/10.1177/14648849231152359
15. **Boichak O, Lokot T.** Billionaires won't save Ukraine's internet. *Foreign Policy*; 2022 Nov 20 [cited 2023 Mar 1]. https://foreignpolicy.com/2022/11/20/ukraine-russia-war-internet-musk-starlink-space-x/.
16. **Boichak O.** Digital war: Mediatized conflicts in sociological perspective. In: Rohlinger DA, Sobieraj S (eds.), *The Oxford handbook of sociology and digital media*. Oxford: Oxford University Press. 2020; 511–527. DOI: https://doi.org/10.1093/oxfordhb/9780197510636.013.31
17. **Boichak O, Hoskins A.** My war: Participation in warfare. *Digital War*. 2022 Dec 2; 1–8. DOI: https://doi.org/10.1057/s42984-022-00060-7
18. **Merrin W.** *Digital war: A critical introduction*. London and New York: Routledge; 2018. DOI: https://doi.org/10.4324/9781315707624
19. **Sherman J.** Cord-cutting, Russian style: Could the Kremlin sever global internet cables? *Atlantic Council*; 2022 Jan 31 [cited 2023 Mar 1]. https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/.
20. **Bergengruen V.** The battle for control over Ukraine's internet. *Time*; 2022 Oct 18 [cited 2023 Mar 1]. https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/.
21. **Netblocks.** Internet disruptions registered as Russia moves in on Ukraine. *Netblocks*; 2022 Feb 24 [cited 2023 Mar 1]. https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.
22. **Vallance C.** Ukraine war: Major internet provider suffers cyber-attack. *BBC News*. 2022 Mar 28 [cited 2023 Mar 1]. https://www.bbc.com/news/60854881.
23. **Beketova E.** Behind the lines: Russia's occupation forces move to crush dissent. *Center for European Policy Analysis*; 2023 Mar 9 [cited 2023 Mar 1]. https://cepa.org/article/behind-the-lines-russias-occupation-forces-move-to-crush-dissent/.

24. **Reporters Without Borders.** In Ukraine's occupied zones, 'the Russians let us choose between collaboration, prison or death'. *Reporters Without Borders*; 2022 Aug 22 [cited 2023 Mar 1]. https://rsf.org/en/ukraine-s-occupied-zones-russians-let-us-choose-between-collaboration-prison-or-death
25. **Smith B.** Defending Ukraine: Early lessons from the cyber war. *Microsoft*; 2022 Jun 22 [cited 2023 Mar 1]. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
26. **Schectman J, Bing C, Pearson J.** Ukrainian cyber resistance group targets Russian power grid, railways. *Reuters*; 2022 Mar 1 [cited 2023 Mar 1]. https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/.
27. **Schechner S.** Cyberattacks don't appear to have increased in Ukraine war, EU says. *Wall Street Journal*; 2022 Mar 9 [cited 2023 Mar 1]. https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-09/card/cyberattacks-don-t-appear-to-have-increased-so-far-in-ukraine-war-eu-says-mHV8L58ppVwINzQoQzpX.
28. **Fedorov M.** The village of Ivankiv, Kyiv region, right after RU occupation. *Twitter*; 2022 Apr 7 [cited 2023 Mar 1]. https://twitter.com/FedorovMykhailo/status/1512157048133275651.
29. **European Commission.** Supporting Ukraine through digital. *European Commission*. [cited 2023 Mar 1]. https://digital-strategy.ec.europa.eu/en/policies/support-ukraine.
30. **Mitchell R.** How Amazon put Ukraine's 'government in a box' – and saved its economy from Russia. *Los Angeles Times*; 2022 Dec 15 [cited 2023 Mar 1]. https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.
31. **SSSCIP.** Ukraine has signed an agreement on accession to the NATO Cooperative Cyber Defence Centre of Excellence. *State Service of Special Communications and Information Protection of Ukraine*; 2023 Jan 19 [cited 2023 Mar 1]. https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-z-kiberoboroni-nato.

TO CITE THIS ARTICLE:
Lokot T. Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience. *LSE Public Policy Review*. 2023; 3(1): 7, pp. 1–8. DOI: https://doi.org/10.31389/lseppr.85

Submitted: 06 April 2023
Accepted: 18 May 2023
Published: 08 September 2023

LSE Public Policy Review is a peer-reviewed open access journal published by LSE Press.