Netoscope: A New Black Box Through Which the Russian Government Controls Content Dissemination?

Sivetc, Liudmila

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Sivetc, L. (2022). Netoscope: A New Black Box Through Which the Russian Government Controls Content Dissemination? *Russian Analytical Digest*, 281, 15-18. https://doi.org/10.3929/ethz-b-000539633

demands and has sometimes supported aggrieved citizens, has fallen completely in line and is currently too busy demonstrating its loyalty to be a force for protest. For a while, therefore, the regime's treatment of protest and opposition as similarly threatening will suppress both, thereby continuing developments that began years ago.

Long-Term Scenario

In the medium to long term, however, the coming economic crisis may well shake these established patterns. Mounting grievances—resulting from rising food prices, unpaid wages, and unemployment—may push new groups of people onto the streets, people who have never protested before and have thus never experienced repression. Moreover, as stability erodes, and with it an important part of Putin's claims to legitimacy, the war's consequences might turn larger swathes of people against him personally. And although systemic opposition forces themselves will likely not call for protest, strong independent mobilization could make the parties' elites (most notably the KPRF) rethink the bargain with the Kremlin that has secured them a place in the system in exchange for loyalty. Protest, it therefore seems, could not only re-emerge, but also usher in a new phase of political opposition. This scenario is unlikely but cannot be ruled out. If it becomes reality, the Kremlin will need to decide to what extent it is willing to escalate repression against the unemployed and hungry—people who are quite difficult to paint as "national traitors."

Conclusion

Given the regime's clearly signaled readiness to quell any form of resistance, the coming weeks and months are unlikely to see much protest. Changing socio-economic conditions, however, have the potential to reshuffle the protest landscape and generate incentives among elites to address social grievances, perhaps even giving new life to the loyal opposition. That said, even if the systemic parties try to exploit potential social protest politically, it is far from guaranteed that this will bring an end to the war. If the regime's response to social mobilization includes costly concessions like higher social payments, however, this might put further strain on the state's finances, which will increase the pressure on the regime more broadly. In this scenario, volatile times lie ahead.

About the Author

Dr *Jan Matti Dollbaum* is a post-doctoral researcher at the University of Bremen. His research interests include protest and social movements in democratic and authoritarian regimes. Together with Morvan Lallouet and Ben Noble, he recently published the first book-length study on Aleksei Navalny.

ANALYSIS

Netoscope: A New Black Box Through Which the Russian Government Controls Content Dissemination?

By Liudmila Sivetc (Turku University) and Mariëlle Wijermars (Maastricht University)

DOI: 10.3929/ethz-b-000539633

Abstract

Russia has increasingly adopted policies that leverage the power of private infrastructure owners, including algorithmic gatekeepers, to achieve more effective, but less easily perceptible, control over online content dissemination. This article analyzes the Netoscope project, which has compiled a database of Russian domain names suspected of malware, botnet or phishing activities. Within the framework of this project, federal censor Roskomnadzor cooperates with Yandex (which downgrades listed domains in its search results), Kaspersky, and foreign partners. The article concludes that non-transparency creates possibilities for misuse of the project.

History and Functionality of the Netoscope Project

Over the last decade, Russia has increasingly adopted policies to leverage the power of private infrastructure owners, including algorithmic gatekeepers, to achieve more effective, but less easily perceptible, control over online content dissemination (Sivetc 2020, 2021; Wijermars, 2021). One example of this kind of coopera-

tion is the Netoscope Project, launched in 2012 by the Coordination Center for top-level domains .ru and .рф.[1] As stated on the official website of the project, www.netoscope.ru, the project "aims at making the Russian domain space safer for users." A representative of the Coordination Center who is directly involved in the functioning of Netoscope explains that the project was not intended to regulate the Russian internet. Rather, the project was necessary to improve the reputation of the Russian top-level domains, which fell outside the ranks of the safest domains in 2009–2011. In light of this, the Coordination Center proposed the Netoscope Project as a platform for cooperation with experts from the cybersecurity field.

Cybersecurity experts, in turn, needed to cooperate with the Coordination Center because only this organization is able to terminate the delegation of domain names to resources involved in the "epidemic" dissemination of, for example, malware. Domain name delegation means connecting a registered domain name with the corresponding address of the server hosting the relevant website. The termination of domain delegation does not cancel the registration of this domain name. Rather, it terminates the connectivity between the domain name and the corresponding address, making the relevant website inaccessible until the delegation is restored. Cybersecurity experts can detect malware being spread by such resources and can identify which domain names serve as coordinating command points. However, experts cannot disable the resources behind malware attacks because the termination of the delegation of the involved domain names is not in their power. Netoscope has provided the necessary mechanisms for doing so. Now, expert partners send information on malicious domain names to the project to enable the Coordination Center to expeditiously react to cyber threats. The aforementioned representative of the Coordination Center indicates that cooperation within the framework of the Netoscope project has led to a decline in the number of malicious activities in the .ru domain, thereby improving its reputation. If in the beginning Netoscope flagged 100,000 malicious domains per year, the representative indicated that by 2020 the figures had decreased significantly and the domain had become "cleaner."

In February 2021, the project's website listed 17 Netoscope partners: Roskomnadzor (a government agency responsible for controlling the Russian Internet), Group IB, Kaspersky, Mail.Ru, Rostelecom, TCI (Technical Center "Internet"), Yandex, BI.ZONE (a daughter company of Sberbank), RU-CERT, IThreat, the Association of MasterCard Participants, SkyDNS, SURF, FIFA, National Computer Incident Response and Coordination Center, and Dr. Web. The list of partners thus includes the two key players on the Russian Internet: Yandex, the Russian counterpart and competitor of Google, is the leading Internet browser, search engine, and news aggregator, while Mail.ru Group is the owner of Russia's most popular social networks (among many other activities).

Roskomnadzor, according to the Coordination Center's 2016 Report (2017, p. 12), joined Netoscope on 19 April 2016. The federal agency and Netoscope agreed on cooperation aimed, *inter alia*, at "the joint investigation of content, types, and features of unlawful online information and the development of means of precluding it from dissemination on the Internet." Despite only becoming an official partner in 2016, Roskomnadzor, as the representative of the Coordination Center clarifies, has been involved in Netoscope since the outset. The agency was an active participant before 2016 and has continued to cooperate actively since signing the agreement.

Experts contribute to Netoscope by sending information on domain names involved in phishing, malware, and botnet activities to a database that accumulates the information and stores all suspected domain names. This means that once a domain name is included in the Netoscope database, it will never again be excluded from it. In other words, the flagged domain name will not be excluded even when it no longer hosts the malicious content. Even if the domain name ceases to exist—namely, if its registration in one of the Russian top-level domains is discontinued—this fact does not affect the information stored in the database. The principle of forever storage, as the representative of the Coordination Center explains, is based on the presumption that a domain name that has been used for malicious activities in the past preserves its dangerous potential and is likely to be used again. The Netoscope database serves as the basis for the "Domain Checker" available on the Netoscope website. Any Internet user can use it to find out whether a domain name registered to the .ru, .su, and .рф domains has been flagged by Netoscope.

According to the project's website, the Netoscope database contains approximately 4.7 million domain names (December 2020). As the representative of the Coordination Center explains, this figure should not be understood as an indicator of a high level of malicious activities: only a small number of these domain

1 This article draws on an article by L. Sivetc and M. Wijermars, "The Vulnerabilities of Trusted Notifier-Models in Russia: The Case of Netoscope," *Media & Communication* 9, no. 4 (2021): Media Control Revisited: Challenges, Bottom-Up Resistance and Agency in the Digital Age, https://doi.org/10.17645/mac.v9i4.4237.

names (around 5,000) are currently flagged as malicious. Instead, a site's appearance in the database should signal to users that the relevant website is safe to access—even if the fact that it was previously flagged by Netoscope raises questions regarding the website's safety. For example, according to the representative of the Coordination Center, companies that are involved in the domain name business decide not to buy a certain domain name if it has been flagged by Netoscope as being involved in malicious activities in the past. They refer to this practice as an "indirect effect" of the Netoscope project.

Netoscope has yet another effect, but this one is direct and planned: according to the Coordination Center's 2014 report (2015, p. 11), Yandex has been using the Netoscope database since 2014 to exclude optimization links to websites corresponding to flagged domain names from its search results (see also Kudriavtseva, 2020). The representative of the Coordination Center confirms that Yandex can use the Netoscope database to adjust how its algorithms decide which websites are to be prioritized in search results lists. At the same time, Yandex also contributes to the database. The representative cites the Yandex Safe Browsing database as a source that Netoscope has been using to enrich and refine its data about domain names included in the Netoscope database. However, they point out that the Netoscope database is just one of many resources that Yandex uses as an input source for its algorithms.

Embedded Vulnerability

The representative of the Coordination Center highlights a unique feature of Netoscope: the project provides a platform for collaboration among competitors. As partners in Netoscope, they are willing to share information with the Coordination Center and contribute to the Netoscope database

Andrei Yarnykh from Kaspersky mentions market competition among Netoscope partners as the reason why there is only unilateral communication between Netoscope and the company. Information submitted to Netoscope by partners is available only to the project, not to its partners.

As the representative explains, cooperation around the Netoscope database occurs as follows. The Netoscope database is located at the Coordination Center. Each partner sends information on those domain names that it identifies as being involved in malicious activities to the Netoscope database. The representative stresses that the partner decides whether to flag a domain name in accordance with its expertise. According to Andrei Yarnykh, Netoscope aggregates information sent by the partners and issues reports on the level of malicious activities like malware, spam, and phishing. These reports are purposely designed not to reveal the size and content of each partner's contribution to the project. As Andrei Yarnykh says, reports provide "statistics rather than analytics." Netoscope does not enable Kaspersky to see which partner flagged a certain domain name.

Importantly, according to the representative of the Coordination Center, Netoscope relies on the partners' expertise and does not verify inputs into the database. They explain that such verification is outside the scope of the Coordination Center's tasks. The Coordination Center does not employ experts to check whether, for instance, a domain name flagged by a Netoscope partner as being involved in phishing is indeed connected to such activities. If a Netoscope partner "says that this domain name is connected with phishing at this moment, it means that the partner answers for [the accuracy of] its words."

The Domain Checker available on the Netoscope website warns users about any malicious activity the checked domain name is/was involved in based on Netoscope partners' assessments. In line with the restricted disclosure and anonymized aggregation discussed above, the results received from the Domain Checker do not show which partner flagged the domain name in question nor when this occurred. As the representative of the Coordination Center explains, making information non-traceable was "the main condition at the start of the project." This means that although the Coordination Center has access to these details, information about partners' involvement is not disclosed.

The lack of transparency extends to all partners in the project. As Andrei Yarnykh explains, Kaspersky sends information "like an email" and is not able to trace how it is subsequently processed by Netoscope. This means that Roskomnadzor can also send unchecked "emails" to the Netoscope database, which can trigger re-indexing of the allegedly malicious domain names and positioning them further down Yandex's list of search results. Thus, the functioning of Netoscope resembles a black box that filters out allegedly harmful domain names without accountability or safeguards against abuse.

About the Authors

Dr. *Liudmila Sivetc* is a lawyer and a former doctoral candidate at the Faculty of Law, University of Turku.

Dr. *Mariëlle Wijermars* is an assistant professor in cybersecurity and politics at Maastricht University.

References

- Coordination Center (2015). *Otchet Direktora ANO "Koordinatsionnyi tsentr national'nogo domena seti Internet" A.A. Vorob'eva*. https://cctld.ru/upload/files/dir_year_report_2014.pdf

- Coordination Center (2017). *Otchet Direktora ANO "Koordinatsionnyi tsentr national'nogo domena seti Internet" A.A. Vorob'eva*. https://cctld.ru/upload/files/dir_year_report_2016.pdf
- Kudriavtseva, V. (2020, February 26). Kak ne popast' v ceti internet-moshennikov? Telekanal Kul'tura. Accessed via INTEGRUM Profi database.
- Sivetc, L. (2020). The blacklisting mechanism: New-school regulation of online expression and its technological challenges. In M. Wijermars & K. Lehtisaari (Eds.), *Freedom of Expression in Russia's New Mediashere* (pp. 39–56). Routledge
- Sivetc, L. (2021). Controlling free expression "by infrastructure" in the Russian Internet: The consequences of RuNet sovereignization. *First Monday*, 26(5). https://doi.org/10.5210/fm.v26i5.11698
- Wijermars, M. (2021). Russia's law 'On news aggregators': Control the news feed, control the news? *Journalism*. https://doi.org/10.1177/1464884921990917

ANALYSIS

Russian Academia and the Ukraine War

By Dmitry Dubrovskiy (Center for Independent Social Research / Central and East European Law Initiative)

DOI: 10.3929/ethz-b-000539633

Abstract

Before Russia launched its war on Ukraine, the Kremlin sought to demonstrate the strength of Russian universities and researchers in international rankings. Now, Western anti-war sanctions are working to isolate Russian scientists. In response, those parts of the Russian academy that historically opposed collaboration with the West are seeking to impose nationally defined metrics. Russia is likely to pursue a new form of academic internationalization, turning its attention to China, India, and Iran rather than the West.

Situation Before the War

Russian officials frequently emphasize the importance of developing Russia's higher education potential and seek to position the country at the forefront of technical innovation. President Putin himself constantly states that "Russia should expect to play a leading role in science and technology."

The Kremlin identified science as one of its top priorities by making it one of the national projects focused on achieving the strategic goals Russia set for itself during the period 2018–2024. The Russian government wants the country to be among the top five countries engaged in research and development in the specific areas that it identified. For this purpose, it established science mega-projects as a way to promote the active development of science under conditions of limited resources. Among the six such projects developed, the primary emphasis was on nuclear and laser physics. These projects were designed in collaboration with the European Union's Horizon 2020 program. In addition, Russia invested about 1.5 billion euros in 2017–2020 in nuclear physics projects abroad. In total, there were 115 scientific projects with international participation by 2020; the European Union was Russia's main partner on these projects, with 22 projects, while the CIS countries ranked second, with 17 projects.

In the field of higher education, the main task was improving the position of Russian universities in international rankings. Thus, the program 5-100-2020 sought to get five Russian universities into the top 100 universities worldwide. The universities involved in the program received significant government funding. Although the program did not achieve its main goal, it brought about several notable accomplishments: the emergence of the very category of a research university in Russia; an improvement in the rankings of universities previously unrepresented in the international arena; a noticeable increase in the numbers of international publications; new laboratories and access to new research equipment; increased student and academic exchanges; and intensified participation of Russian scholars in international research projects and conferences.

After Russia annexed Crimea in 2014, the ambitious goal of turning Russian science and education into a flagship of modernization encountered serious limitations, both political and structural. Figure 1 shows that