

Russia-Ukraine Conflict: Russian Internet Infrastructure Updates

ZEROFOX INTELLIGENCE BRIEF

B-2022-03-04a

Classification: TLP White

Criticality: High

Intelligence Requirements: Internet Infrastructure

March 4, 2022

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on March 4, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Executive Summary

Ukraine has asked the Internet Corporation for Assigned Names and Numbers (ICANN) to revoke Russian top-level domains (TLDs) and SSL certificates. However, ICANN, the United States, and its European Union (EU) counterparts have expressed no interest in sanctions that would restrict Russian access to the global internet. The United States is also unlikely to use offensive cyber capabilities against Russian information and physical infrastructure targets, lest it be construed as an act of war.

Key Findings

- On February 28, 2022, Ukraine asked ICANN to revoke Russian TLDs and SSL certificates, but ICANN said it has no sanctions power.
- ICANN could theoretically be pressured to take more aggressive action against Russia, but the United States and its allies currently have no interest in such measures.
- Targeting Russian internet infrastructure could set precedent for both “splintering” global internet infrastructure and manipulating internet regulators.
- Russia is centralizing the control of its information environment through its “Sovereign Internet Law.” War with Ukraine will likely exacerbate this process.
- The United States has offensive cyber capabilities but is unlikely to take action against Russia that could be construed as an act of war.

Analyst Commentary

On February 28, 2022, Ukraine’s ICANN representative, Andrii Nabok, and Prime Minister Myhailo Federov asked ICANN to permanently or temporarily revoke Russian TLDs .ru, .рф, and .su; to aid in revoking SSL certificates for those domains; and to shut down the DNS root servers in St. Petersburg and Moscow. They also noted their intent to request that Réseaux IP Européens Network Coordination

Centre (RIPE NCC) withdraw the right of Russian members of the centre to use all IPv4 and IPv6 addresses and block the DNS root servers that RIPE NCC is operating. The Ukrainian representatives were clear that their requests should be considered sanctions against Russia for its invasion of Ukraine—in essence, making them comparable to financial sanctions levied by the United States and the EU against Russia.¹ Both ICANN and RIPE quickly rejected the request. ICANN responded on March 2, 2022, stating that they have no authority to levy sanctions and that their role requires the operation of the internet to be non-politicized.²

The Ukrainian request was unprecedented and likely represents the most extreme scenario for sanctions against Russia's internet infrastructure. Such a move would cut off Russia from data-routing technology and essentially sever its ties to the global internet. Theoretically, Ukraine could attempt to persuade the U.S. government to pressure ICANN, but U.S. support for such an effort would be very unlikely. Overall, there is no appetite for such measures from the United States or its allies, and sanctions to that effect have not been publicly discussed among leading Western governments.

Revoking Russian top-level domains and SSL certificates does not currently serve Western information interests in the conflict. Western leaders and senior officials want pro-Western and anti-Russian information to be accessible in Russia to support efforts to undermine Russian President Vladimir Putin's regime. U.S. President Joseph Biden's White House has also faced pressure to implement other damaging sanctions, such as an embargo of Russian oil and gas imports, and has resisted internal calls to do so. An attempt to disrupt Russia's access to the internet would have few obvious benefits to the war effort and many possible drawbacks, potentially creating precedence for both a "splintered" global internet infrastructure and future efforts to manipulate the authority of internet regulators. Additionally, experts question whether ICANN has the ability to carry out the Ukrainian request.³

Despite the unlikelihood of such an extreme scenario, Russia has for years taken steps to negate the possibility of U.S. or NATO-led efforts to cut off its access to the internet. A series of November 2019 and January 2021 amendments to existing federal law, often described as the "Sovereign Internet Law," have attempted to protect the Russian internet from threats to international servers. In practice, the amendments have created a framework to centralize the management of Russia's internet and increase state control on the flow of information. This has heightened

¹ <https://eump.org/media/2022/Goran-Marby.pdf>

²

<https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf>

³ <https://www.cnet.com/news/russias-ukraine-war-raises-specter-of-an-online-splinternet/>

surveillance and made the Russian government the primary regulator of internet activity in Russia.

One example of this law in practice is the requirement that all internet service providers (ISP) install deep packet inspection (DPI) technology in their networks, which allows government regulators to filter and reroute traffic. This was used in March 2021 to slow Twitter access after the platform did not respond quickly enough to a request by the Russian government to take down content considered unlawful, and it has since been used to block access to sites accused of hosting content related to imprisoned political dissident Alexey Navalny.⁴ Russia also requires internet companies to record and store the personal data of Russian citizens on servers physically located in Russia and telecommunication companies to store the content of text and phone conversations and their metadata on domestic servers.⁵

Russian efforts to create the so-called “RuNet” have had mixed results and have mostly been used to pressure news organizations and U.S.-based technology companies to comply with Russian laws and to suppress political activism. The Russian state still maintains less centralized control over its network infrastructure than, for example, China. However, the centralization of the Russian internet is a long-term project favored by President Putin that the war with Ukraine will only hasten. Moves by Western companies to restrict Russian news outlets and alleged propaganda networks, like RT and Sputnik, and decisions by individual technology companies, such as Apple, to withdraw from the country will accelerate Russia’s internet isolation and intensify President Putin’s control of the domestic information environment.

The United States could take measures to disrupt Russia’s internet infrastructure through cyber warfare. On February 24, 2022, President Biden said that the United States was prepared to respond to Russian cyberattacks on U.S. critical infrastructure. It is unclear, however, what form such attacks would take. NBC News and other outlets reported that the U.S. president was presented with options for potential cyberattacks on Russia that included moves to disrupt Russian internet connectivity and target its electrical grid or railway systems. The White House denied the reporting, but the United States has used cyber weaponry in the past. Stuxnet malware, identified in 2010 and unofficially attributed to the United States and Israel, caused severe disruption to the Iranian nuclear program.⁶

⁴ <https://www.rferl.org/a/russia-internet-crackdown-redoubles/31626590.html>

⁵ <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>

⁶ <https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558>

However, the United States and its allies are not likely to pursue offensive, or even highly damaging, cyberattacks on Russian targets as both sides would probably consider such activity tantamount to NATO military action against Russia.