AMERICAN FOREIGN
POLICY COUNCIL

RUSSIA REFORM MONITOR

The American Foreign Policy Council's Review of
Russian Goverment Actions and U.S. Policy

Russia Reform Monitor No. 2506

January 18, 2022 **Ilan I. Berman**

Related Categories: Cybersecurity and Cyberwarfare; Russia; Ukraine

THE NUTS AND BOLTS OF RUNET
Russia's sovereign internet project - commonly referred to as RUNET - is now a decade old. And while few details have emerged to date regarding what might be the Kremlin's most ambitious social engineering experiment, a new expose by agentura.ru has detailed the vital components of the Kremlin's efforts to create a national internet insulated from the larger World-Wide Web. RUNET, the investigative website details, consists of several overlapping components: a control center in Moscow dedicated to the "monitoring and management of the public communication network"; a dedicated Internet Registry, to de-link Russian domains from Internet registrars abroad; a national domain name system, "to replace the functions of the global DNS (Domain Name System)"; and technical devices (provided by foreign firms such as China's Huawei) designed to give authorities the ability to monitor and - if necessary - disrupt threats.

After years of concerted investments, RUNET is far more ubiquitous than commonly understood. "At the end of 2021, the Sovereign Internet system controlled 73% of Internet traffic and 100% of mobile traffic" within Russia, the Agentura study notes. This percentage, moreover, is projected to expand as more and more devices, components and capabilities associated with RUNET are installed by Russian authorities. (agentura.ru, December 31, 2021)

NO PROGRESS IN UKRAINE TALKS...
Diplomatic talks intended to diffuse tensions between Russia and the West over Ukraine have hit what officials are calling a "dead end." Days of talks between Russian and Western officials have concluded without a substantive breakthrough, and policymakers are now bracing for the possibility of conflict. "The threat of military invasion is high," White House National Security Advisor Jake Sullivan has said. "There are no dates set for any more talks. We have to consult with allies and partners first."

The impasse stems from NATO's refusal to accede to Russia's demand that Ukraine be categorically denied the possibility of joining the Alliance in the future, as well as to the Kremlin's insistence that the bloc pare back its presence in Eastern Europe. Western officials have called the demands "non-starters." (Reuters, January 13, 2022)

...AS CONGRESS AIMS TO DETER MOSCOW...
Lawmakers in Congress have put together a biting new package of sanctions that could be leveled against the Kremlin if Russia does indeed invade Ukraine. The new measures are contained in the Defending Ukraine Sovereignty Act, which is being spearheaded by Congressional Democrats. They include direct sanctions against Russian President Vladimir Putin and other officials, as well as a number of Russian financial institutions. The Act also proffers an additional $500 million, above and beyond what has been allocated by the Biden administration so far, to Ukraine in military aid. "We are coming together to send a clear message — Putin need not collapse his entire economy nor does he need to sacrifice the lives of his own people in a futile attempt to rewrite the map of Europe," Senator Bob Menendez (D-NJ), who chairs the Senate Foreign Relations Committee, has stated. (Agence France Presse, January 13, 2022)

...AND THE KREMLIN DRAWS (ANOTHER) RED LINE
If the United States slaps personal sanctions on Russian President Vladimir Putin over the Kremlin's aggression against Ukraine, it would mark an "extreme" step that would herald the complete collapse of relations between Moscow and Washington, Russian officials have warned. The proposed step has been floated by Congress as part of a package of punitive measures designed to deter Moscow from moving ahead militarily in its current conflict with Ukraine. "Introducing sanctions against the head of the government or the head of Russia is an extreme measure which is comparable to a breakdown in relations," Kremlin spokesman Dmitry Peskov has told reporters. (*The Moscow Times*, January 13, 2022)

THE FSB TAKES AIM AT HACKERS
In a rare episode of U.S.-Russian cooperation, Russia's main security service, the FSB, has successfully dismantled REvil, a prominent criminal hacker group, at Washington's request. The collective had previously launched a series of ransomware attacks against foreign individuals and businesses, emerging as one of the world's most notorious cyber crime gangs. The FSB operation reportedly resulted in the seizure of some 426 million rubles-worth ($5.5 million) of ill-gotten currency, the detention of multiple REvil members, and the confiscation of twenty luxury automobiles.

The BBC had described the operation as a "monumental moment" in cyber-cooperation between the U.S. and Russia. "For years, Russia has ignored and denied accusations that Russian ransomware hackers are allowed safe harbour in the country to attack western targets," it notes. "In their Geneva Summit last summer, Russia's President Putin and US President Biden agreed to open discussions about how to combat the scourge of ransomware, but even the most optimistic experts had given up on seeing the talks bear fruit." And while Russia and the West remain at loggerheads over security in Eastern Europe, the operation "may point to a thawing of relations, which is already being widely celebrated in the cyber-security world." (Lenta.ru, January 14, 2022; *BBC*, January 14, 2022)

© 2024 - American Foreign Policy Council