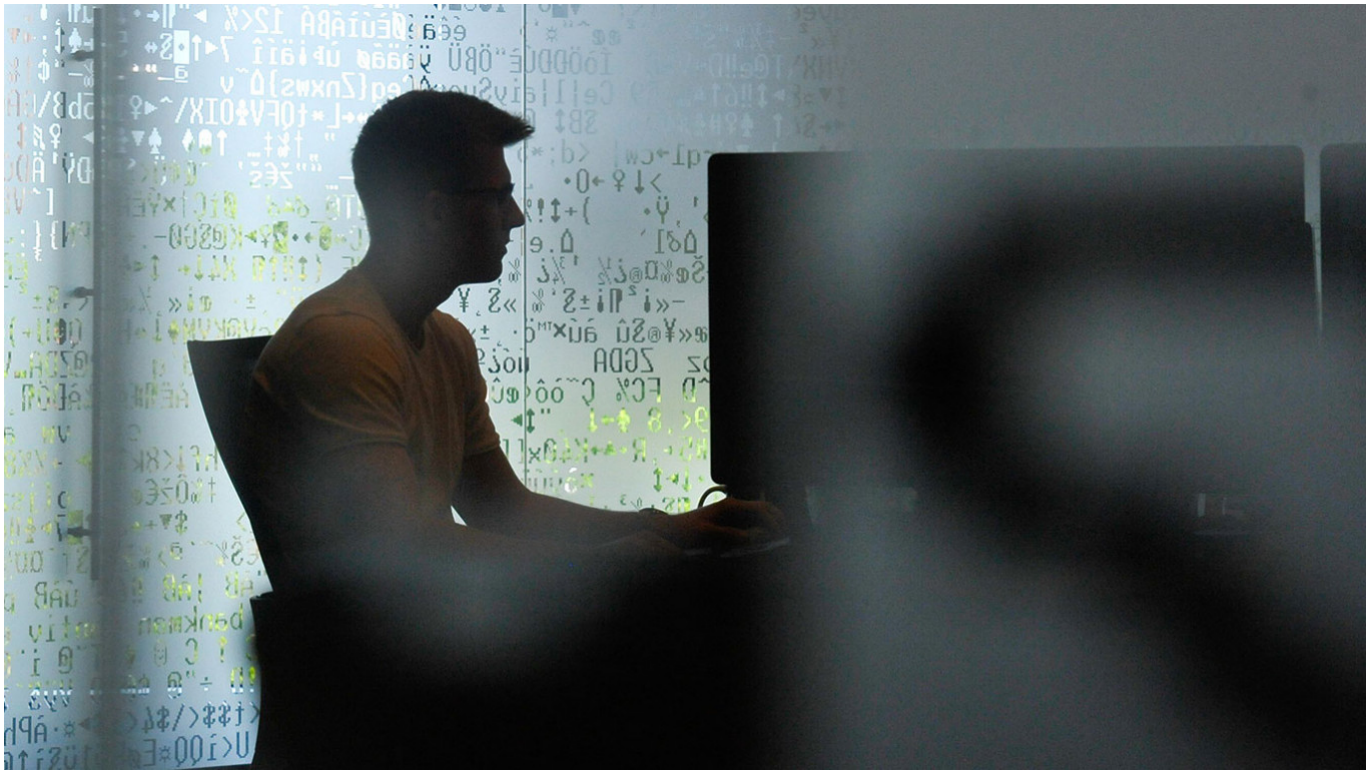
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Why the Kremlin Blocking TOR Is a Big Deal

By Andrei Soldatov

December 07, 2021



Alexander Avilov / Moskva News Agency

Like many significant political developments of late, the decision to block TOR came almost unannounced by the Russian authorities. TOR — an acronym for "The Onion Router" — is encryption software that allows users to stealthily surf the Internet and bypass locally imposed web restrictions.

Russian internet users spotted the blocking of TOR, and it was only after their numerous complaints that activists and journalists spotted the threat Roskomnadzor had published three days before about "the introduction of centralized management in relation to the means of circumventing the restriction of information prohibited by law," an announcement not easy to decipher even to those well-versed in Russian bureaucratic speak.

And now it is clear — Russian censors have finally found a way to block the most famous online censorship circumvention tool.

Related article: Russia's Sovereign Internet Law Comes Into Force

Throughout 2021, Russia's Internet censors mounted a systematic attack on technologies that could be used by the country's users to bypass censorship.

In the summer, Roskomnadzor blocked the first two VPNs, then the popular browser Opera killed support for its VPN. In September, eight more popular VPNs were blocked. And then Apple turned off its Private Relay service in Russia. Private Relay was designed to encrypt all the traffic leaving the user's device so no one can intercept it. Apple has already been forced to turn it off in China, Belarus, Colombia, Egypt, Kazakhstan, Saudi Arabia, South Africa, Turkmenistan, Uganda and the Philippines, citing 'regulatory requirements' in those countries. Now it is Russia's turn.

TOR was Russia's next natural target because the software allows users to access websites and pages blocked by the authorities. But the significance of this development is much bigger.

Many technologies the users use today to avoid censorship were developed as commercial tools. VPNs, or virtual private networks, were developed when companies understood they needed a secure way to share data between different offices, and to allow employees to access sensitive files remotely and safely.

However, TOR was political from the beginning. It was developed in the mid 1990s in the U.S. Naval Research Laboratory to protect American intelligence communications online — essentially to give U.S. spies a way to communicate with their assets securely using the Internet, and doing it by hiding their traffic in millions of other people's traffic.

In the mid-2000s, the U.S. military released the code for TOR, and the Electronic Frontier Foundation (EFF) started to fund TOR developers to continue the project. From then on, the TOR Project, now a nonprofit, was largely seen as a technology developed and maintained by democratic countries to help activists in dictatorships bypass censorship in their countries.

In other words, TOR became the latest addition to the long tradition started by radio sets supplied by the British and Americans to the resistance in Nazi-occupied Europe, and copying machines smuggled beyond the Iron Curtain. The TOR project was supported financially by the U.S. Bureau of Democracy, Human Rights, and Labor, the International Broadcasting Bureau — which supports Voice of America and Radio Free Europe/Radio Liberty — Internews and Human Rights Watch.

It was a scheme in which technically advanced democracies helped technically backward authoritarian regimes withstand repression by supplying technology to activists, not least to help them provide access to content produced by democracies.

It all went well, and TOR seemed unbeatable for years, even in Russia. Moscow challenged TOR unsuccessfully in 2014, two years after Internet censorship was introduced in the country. Back then Russia's interior ministry offered 3.9 million rubles ($86,000) for research on cracking TOR, but was forced to cancel the project due to the lack of any breakthrough.

Changing picture

And then the picture got a bit blurry.

First, it became increasingly evident that the TOR project enabled the Dark Web, populated with hackers, drug and gun dealers, and this picture was very far from the bright and shiny community of activists fighting dictators.

And second, the dictators found a way to block TOR, also using technology developed in democracies. Deep Packet Inspection was initially developed for commercial use, but many authoritarian countries use it in their censorship and surveillance systems, including the Russian Sovereign Internet.

It was probably very nice to have both the moral and technical high ground in dealing with brutal but backward dictators. That time has come to an end. The dictators remain brutal, but not backward, and they have learned well how to adapt to the new circumstances, including adapting commercial technologies to their political needs.

The question is, are democracies also capable of adapting?

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2021/12/07/why-the-kremlin-blocking-tor-is-a-big-deal-a75751