The Big Read Russia

Russian technology: can the Kremlin control the internet?

Moscow is developing a ‘sovereign’ web that critics say will enhance official power to silence dissent

Max Seddon and Henry Foy in Moscow 6 HOURS AGO

Thousands of protesters had gathered outside government headquarters in Magas, the capital of the heavily Muslim republic of Ingushetia in Russia’s north Caucasus. They were there to oppose concessions in a years’-long bitter border dispute with neighbouring Chechnya, but when they tried to share information about the protest on WhatsApp they found the internet was down on all three major Russian mobile providers across Ingushetia.

The October outage began late at night before the protest was scheduled to start, and lasted until it died down more than two weeks later. When protests sparked up again, the internet suddenly went out of action once more.

It amounted to a virtual blackout: locals’ fondness for voice messages has made WhatsApp the main form of communication in the north Caucasus.

No official explanation was given until spring, when the FSB security service — the successor to the KGB — admitted in court that it had shut down the internet because of “terrorist threats”. All but one of the supposed threats coincided with the dates of the protests, says Andrei Sabinin, who filed a lawsuit against the FSB and the interior ministry over the outages.

"They want to take down platforms for spreading information online," the human rights lawyer says. "No WhatsApp means no communication in the Caucasus. As soon as you go into Ingushetia, it's a black hole."

Protests in Ingushetia over land swaps with Chechnya in October 2018, when WhatsApp was shut down in the republic to curb discussion about the issue

Activists fear Ingushetia's blackouts could be repeated across Russia thanks to a law signed by President Vladimir Putin in May. The measure ostensibly aims to create a "sovereign internet" — effectively a parallel web run entirely on Russian servers — that would allow Moscow to keep the internet operating in the event of a foreign cyber attack aimed at disabling it.

To do so, internet providers will be required to install equipment, which Russia could use to separate itself from the worldwide web at the flick of a "kill" switch. The technology, known as deep packet inspection, or DPI, is meant to reroute all external traffic through Russian-controlled nodes while creating a back-up domain name system to help the country's internet function independently.

Russia's dependence on foreign systems would be vastly reduced, hastening a global Balkanisation of the internet where the west's influence is fragmented. Using DPI would simultaneously centralise filtration powers in the hands of Russian censors, who have previously relied on internet providers to block access to banned content.

"It's framed as a precaution, but it's actually a means of control," says Sergey Sanovich, a political scientist at Stanford University who specialises in Russian online censorship. "For the most part this is about making sure the Russian government can, when necessary, have more direct access to control of information space."

Russia let its internet grow largely untrammeled until 2012, when Mr Putin's return to the presidency met with mass street protests organised via social media. The Kremlin responded with an aggressive crackdown on online dissent: opposition pages were put on a list of banned websites, dozens of people went to prison for "liking" and reposting material, and independent news websites were brought to heel. But this ad hoc system was seen as inefficient.

In 2014, Mr Putin declared the internet a "CIA project" able to weaken Russia's sovereignty. Officials blamed the US for using it to start the Arab spring and Ukraine's Maidan revolution in 2013-14. Some pro-Kremlin figures spoke of emulating China's Great Firewall — a mix of technologies and laws designed to regulate the internet domestically, whose architects were invited to Moscow to share advice.

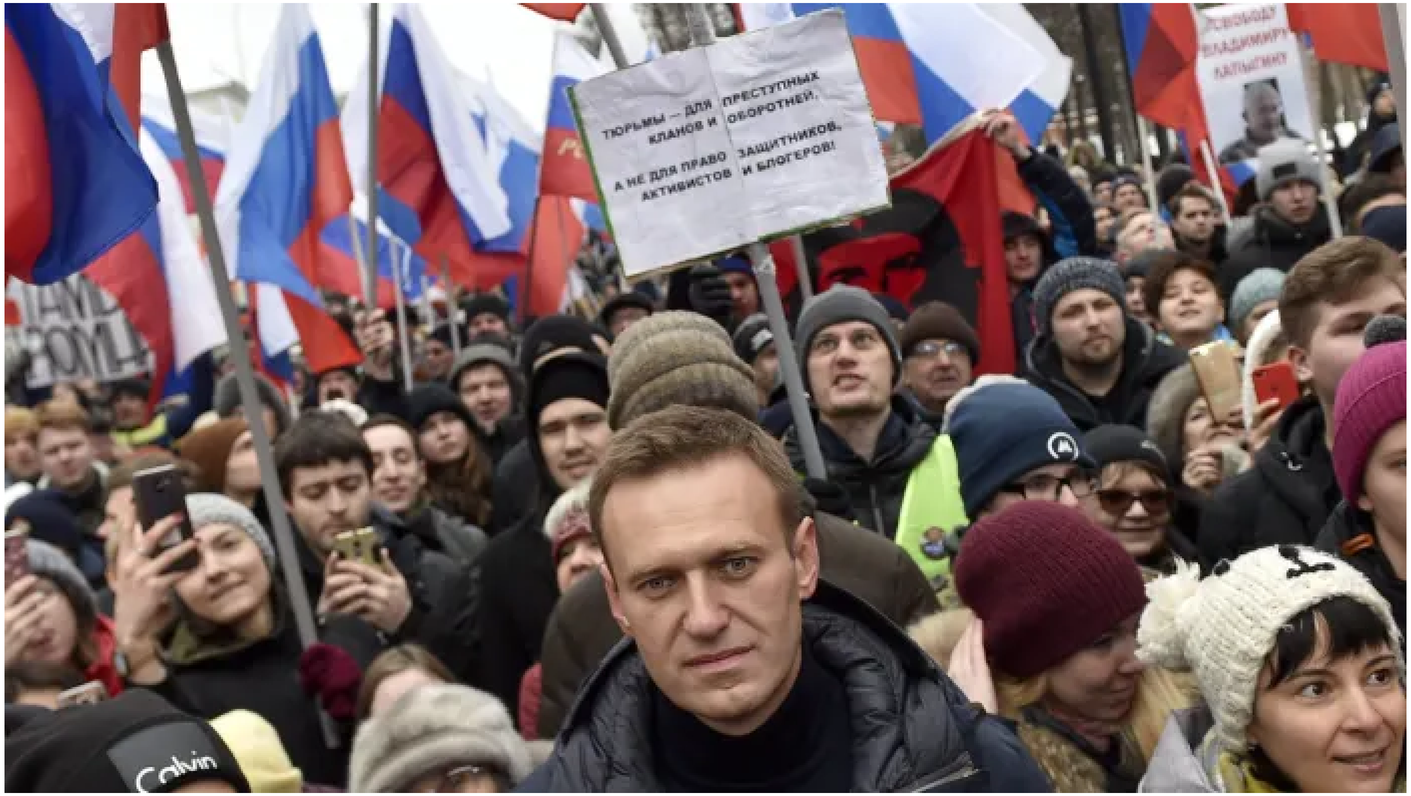
The crackdown intensified after 2017, when opposition leader Alexei Navalny aired a video of an anti-corruption investigation — which racked up more than 20m views on YouTube — to help spark the largest nationwide protests since the Soviet Union collapsed. In 2018, Russia restricted access to almost 650,000 websites— a nearly fivefold increase on the year before, according to human rights group Agora.

Yet Russia's late start meant it lacked both the infrastructure and the human resources to control the internet as effectively as Beijing. China boasts its own hugely popular messaging services, such as WeChat, and has a reported 2m people who police public opinion online. By contrast, Roskomnadzor — the communications ministry's watchdog — has just over 3,000 employees.

"The Chinese have been blocking things since day one," says a person close to Russia's communications ministry. "We can't do that."

Roskomnadzor made its most ambitious effort to ban Telegram, the messaging service, last year, accusing it of not complying with FSB requests to share user data. The attempt to block the app was a disastrous failure. Pavel Durov, Telegram's Russian founder, rerouted its traffic through cloud hosting services, forcing censors into a game of whack-a-mole that saw them temporarily take down more than 16m IP addresses, including their own website, while having little effect on Telegram.

The ban became a running joke among officials. At a ministry party last year, Roskomnadzor chief Alexander Zharov was taking photographs of a picturesque sunset on his phone when guests joked that he should share them on the app, prompting a foul-mouthed tirade, according to one guest.


ТЮРЬМЫ — ДЛЯ ПРЕСТУПНЫХ КЛАНОВ И ОБОРОТНЕЙ,
А НЕ ДЛЯ ПРАВОЗАЩИТНИКОВ, АКТИВИСТОВ И БЛОГЕРОВ!
Calvin

The crackdown intensified after 2017 when opposition leader Alexei Navalny posted a video of an anti-corruption investigation, garnering over 20m views © AP

"He's a hostage to the situation," says the person close to the ministry. "He knows you can't block it. We have no control over the process. The guys with epaulettes [in the FSB] bring bills to [lawmakers] and we have to implement them, [but] we look like idiots."

Part of the problem, experts say, is that Russia's security bureaucracy rarely takes its own technical limitations into account.

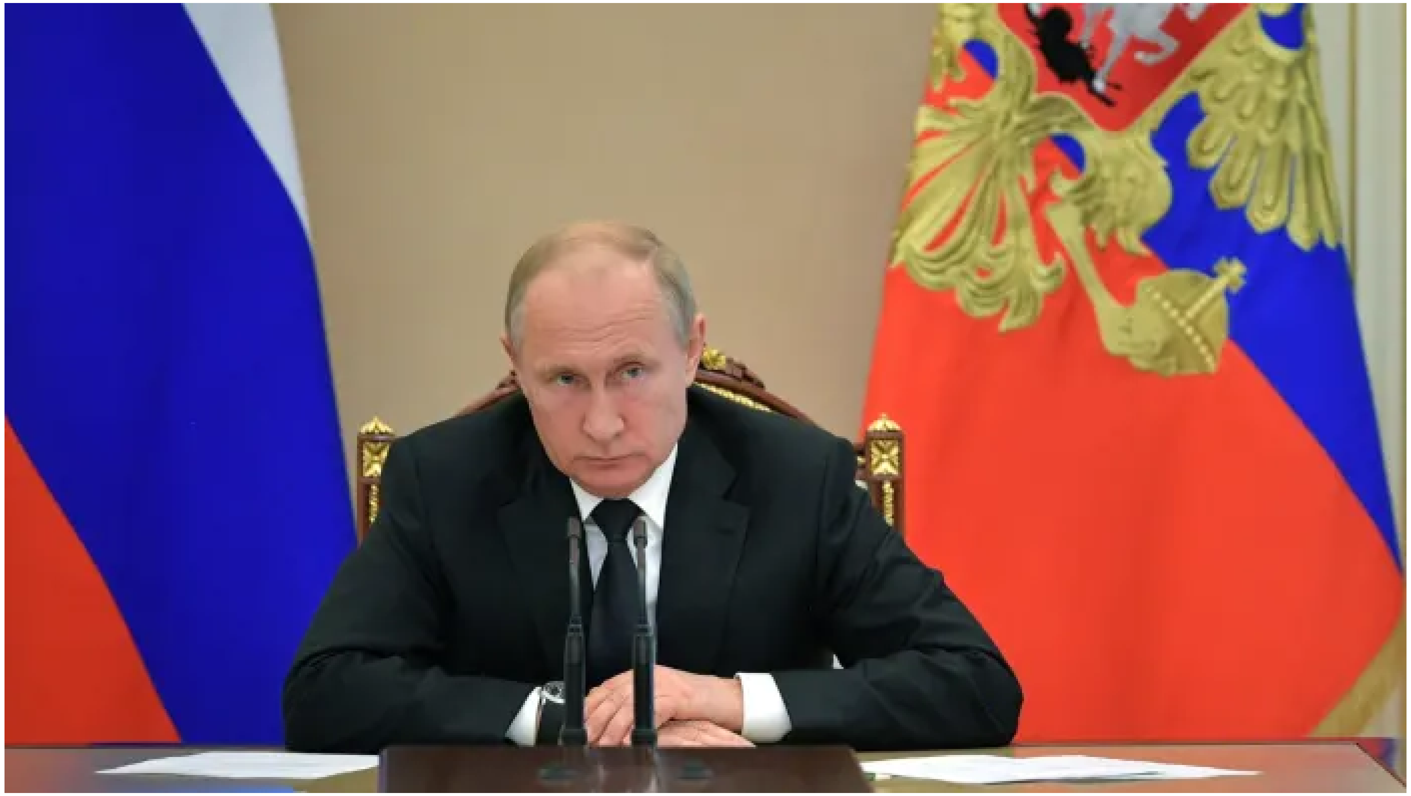
"Attempts to implement Russia's notion of information security on the internet have been distinguished by mishaps because they don't really understand how the internet works," says Keir Giles, a senior fellow of the Russia and Eurasia programme at Chatham House. "If you prevent free flow of information across national borders you'll break the internet."

Advocates for greater controls frame it as a way to ensure Russia's independence from hostile powers. "A great deal of sectors of the real economy — power stations, transport infrastructure — depend very closely on the internet. It's an issue of state security," says Andrei Klishas, a member of the upper house of parliament, who co-authored the law.

Mr Klishas cites the latest US cyber security strategy, with its emphasis on making countries like Russia pay "costs likely to deter future cyber aggression," as the impetus for Moscow to act. President Donald Trump added to those fears last month, when he admitted that the US carried out a cyber attack against a Kremlin-backed "troll farm" in St Petersburg during the 2018 US midterm elections in apparent retaliation for Russia's online meddling in the 2016 presidential campaign.

Experts say Russia's justifications for shutting the country off from the global internet are too vague to support such sweeping action. These scenarios include a threat to network "integrity" that would prevent it from securing user communications; anything that would affect its ability to function such as a natural disaster; and "deliberate destabilising informational pressure from outside or within".

"There needs to be a way to react to the threats," says Irina Levova, head of a government working group on internet issues. "[But] you can't just say let's go to Mars tomorrow and have everyone go without having the technology to do so."



Russian president Vladimir Putin aims to create a 'sovereign internet' — effectively a parallel web run entirely on domestic servers © AP

Officials successfully tested the DPI system in a “fairly large region with a population of several thousand” — not Ingushetia — several months ago, says Mr Klishas, and plan to do a nationwide test later this year. But serious doubts remain about whether the law’s aims are even realisable.

According to Ms Levova, maintaining the DPI equipment alone may cost as much as Rbs134bn ($2bn) a year— seven times Mr Klishas’ estimate — while many of the law’s technical provisions have yet to be clarified. Roskomnadzor reportedly hired RDP.RU, a company partly owned by state-run Rostelecom, to supply the DPI equipment before the bill was even passed.

There is scepticism in the industry about whether Russia can produce the required technology. It has yet to undergo a full-scale test. And attempts to separate Russia from global technology value chains have failed: 96 per cent of state institutions still use unapproved foreign software despite an attempt to move them on to domestically produced alternatives, according to the audit chamber, which monitors the spending of government departments. Russia's government bought Rbs82bn in foreign hardware compared to just Rbs18bn of domestically-produced equipment, according to state defence conglomerate Rostec.

"Right now it's totally impossible," says a senior executive at a major Russian tech company. "There's no capacity to produce really productive, powerful chips. It would take years to develop that industry and in that time Apple will have gone much further. We could buy everything from China, they've done it all themselves, but that would raise national security questions."

Centralising control over Russia's internet — in a bid to make it more secure — could actually make it more vulnerable to foreign attacks, says Artem Kozlyuk, head of privacy rights group Roskomsvoboda. "Where the internet is more centralised and there is one state provider, then there is more risk of external meddling," he says.

The Russian web

1,156,480

Internet protocol addresses banned in Russia, according to Roskomsvoboda, the privacy rights group

650,000

Websites were added to Roskomnadzor ‘s banned list last year, up from just 9,021 in 2015

7.2m

Subscribers to Telegram in 2017. It rose to 9.3m after a bungled effort to ban the messaging service last year

Russia might also be trying to safeguard itself from the consequences of its own cyber operations, Mr Giles says. The WannaCry and NotPetya attacks — which ravaged businesses globally with ransomware and were blamed on Moscow — did considerable damage in Russia, taking some state-owned companies' systems offline. "Massive disruption has blowback," he says. "[These measures] make sure that you don't suffer damage by cutting yourself off."

When Russian troops seized Crimea in 2014, they quickly took over the peninsula's main internet exchange point and cable connections to the mainland. "That was the gold standard to achieve total information dominance — the only things the target population is receiving are yours," says Mr Giles.

Activists fear the internet isolation plan will do the same to Russian citizens. "It'll be a totally different internet. It won't be as quick or secure as it is now," Mr Kozlyuk says. "Blocking will be totally non-transparent. It might take months until someone finds out there was some sort of internal order [to block a site]."

Mr Klishas says the system will simply help Roskomnadzor enforce existing law, which is ostensibly aimed at preventing terrorism and child pornography but is often redirected to suppress dissent. "When states started fighting money laundering, the system was ineffective for a long time, especially [against] problems like drug trafficking and international terrorism. People always found ways to finance this unlawful activity. Then new procedures appeared to close these legal loopholes," he says.

Undeterred by the Telegram ban, the FSB recently made a similar demand to Yandex, Russia's largest tech company. Yandex, which already shares some data with authorities, said on Tuesday it would push back against the FSB's requests to decrypt all user communications.

Despite sweeping requirements on data storage and censorship compliance — which saw LinkedIn banned in 2016 — Roskomnadzor has made little progress in bending Facebook and Google to its demands. In December Russia fined Google Rbs500,000 for failing to sign up to a government system for sharing information with the security services. Google continues to defy the law, but there has been an escalation in Moscow's attempts to pressure western companies, Mr Sanovich says.

“The irony is that Putin, who is conducting all these information operations abroad, also makes Google or Facebook enforce censorship at home,” he adds. “If they comply they risk making the regime stronger and compromising the integrity of their platform, but it’s much more significant if they are blocked. The media environment in Russia is now so heavily government-controlled that these providers play a vital role in giving Russians access to unfiltered information.”

Roskomnadzor is doubling down on that by making it more difficult to avoid its bans. Though virtual private networks remain widely accessible, several have recently abandoned their Russian servers after the watchdog ordered them to share user traffic information with the Kremlin.

Mr Kozlyuk expects it to use DPI to enforce the ban by filtering individual VPN traffic and fining those using them. “It’s the logical extension,” he says, “first you control the content, then the infrastructure, then the users.”

The ‘doomsday’ effort at online independence

Half of Russia’s internet traffic passes through an unassuming 19-storey high rise in southwestern Moscow that houses MSK-IX, the largest of the country’s internet exchange points. The data centre is the physical point of contact for over 500 providers, linking traffic in western Russia with the world.

Under Russia’s new internet “sovereignty” law, providers are required to install black boxes at every stage of the process using deep packet inspection, a technology that can inspect, filter and reroute web traffic. A new internet monitoring centre will use DPI to give the Kremlin a closer look at all information going in and out of Russia.

“We have no idea whatsoever about the communications networks installed in Russia and cross-border connections . . . who owns them, how they are used, what information is carried along them,” MP Andrei Lugovoi, who co-authored the bill, said in February. “The centre we are creating will see it all online.”

Russia's censors say DPI will help create a parallel domain server to function as a domestically-run, back-up internet in the event of a cyber attack. It will also give the Kremlin far greater control over the web within its borders by placing censorship directly in the state's hands. Russia can refine its censorship by blocking individual pages rather than whole servers. Should that fail, it can be used to reduce internet speed for targeted groups.

"The more sovereignty we have, including in the digital field the better. This is a very important area," Mr Putin said.

"It's a doomsday device — if you want to turn your country into North Korea, you can," says Sergey Sanovich, a political scientist at Stanford University. But unlike China, which began censoring its internet decades ago, Russia's internet is built into the global web — carrying a large risk of collateral damage. "It would be such a heavy blow to the [Russian] economy and the state: they all depend on IT services," says Mr Sanovich.