Digital sovereignty: can the Russian Internet cut itself off from the rest of the world?

October 29 2019, by Francesca Musiani, Benjamin Loveluck, Françoise Daucé and Ksenia Ermoshina

What digital border controls should be used in Russia? Credit: Wikimedia

The Internet infrastructure is based on the principle of the internationalisation of equipment and data and information flows. Elements of the Internet with a geographic location in national territories need physical and information resources hosted in other territories to be able to function. However, in this globalised context, Russia has been working since 2012 to gradually increase national controls on

information flows and infrastructure, in an atmosphere of growing political mistrust toward protest movements within the country and its international partners abroad. Several laws have already been passed in this regard, such as the one in force since 2016 requiring companies processing data from Russian citizens to store them on national territory, or the one regulating the use of virtual private networks (VPNs), proxies and anonymisation tools in force since 2017.

In February 2019, a bill titled "On the isolation of the Russian segment of the Internet" was adopted at first reading in the State Duma (334 votes for and 47 against) on the initiative of Senators Klichas and Bokova and Deputy Lugovoi. The accompanying memo of intent states that the text is a response to the "aggressive nature of the United States National Cybersecurity Strategy" adopted in September 2018. The project focuses on two main areas: domain name system control (DNS, the Internet addressing system) and traffic routing, the mechanism that selects paths in the Internet network for data to be sent from a sender to one or more recipients.

Russia wants to free itself from foreign constraints

The recommendations notably include two key measures. The first is the creation by Russia of its own version of the DNS in order to be able to operate if links to servers located abroad are broken, since none of the twelve entities currently responsible for the DNS root servers are located on Russian territory. The second is for Internet Service Providers (ISPs) to demonstrate that they are able to direct information flows exclusively to government-controlled routing points, which should filter traffic so that only data exchanged between Russians reaches its destination.

This legislation is the cornerstone of the Russian government's efforts to promote their "digital sovereignty". According to Russian legislators, the goal is to develop a way of isolating the Russian Internet on demand,

making it possible to respond to the actions of foreign powers with self-sufficiency and to guarantee continued functioning. On the other hand, this type of configuration would also facilitate the possibility of blocking all or part of communications.

The Russian state is obviously not the only one aiming for better control of the network. Iran has been trying to do the same thing for years, as has China with the famous Great Firewall of China. Many states are seeking to reinforce their authority over "their" Internet, to the point of partially or totally cutting off the network (measures known as "shutdowns" or "kill switches") in some cases. This was the case in Egypt during the 2011 revolution as well as more recently in Congo during the elections. It is also regularly the case in some parts of India.

In connection with these legislative projects, a recent initiative, published on February 12 by the Russian news agency Tass, has attracted particular attention. Under the impetus of the Russian State, a group uniting the main public and private telecommunications operators (led by Natalya Kasperskaya, co-founder of the well-known security company Kaspersky), has decided to conduct a test in order to temporarily cut off the Russian Internet from the rest of the globalised network and in particular the World Wide Web. This will in principle happen before April 1, the deadline for amendments to the draft law, requiring Russian Internet providers to be able to guarantee their ability to operate autonomously from the rest of the network.

Technical, economic and political implications

However, beyond the symbolic significance of empowerment through the disconnection of such a major country, there are many technical, economic, social and political reasons why such attempts should not be made, for the sake of the Internet on both an international and national scale.

From a technical point of view, even if Russia tries to prepare as much as possible for this disconnection, there will inevitably be unanticipated effects if it seeks to separate itself from the rest of the global network, due to the degree of interdependence of the latter across national borders and at all protocol levels. It should be noted that, unlike China which has designed its network with a very specific project of centralised internal governance, Russia has more than 3,000 ISPs and a complex branched-out infrastructure with multiple physical and economic connections with foreign countries. In this context, it is very difficult for ISPs and other Internet operators to know exactly how and to what extent they depend on other infrastructure components (traffic exchange points, content distribution networks, data centres etc.) located beyond their borders. This could lead to serious problems, not only for Russia itself but also for the rest of the world.

In particular, the test could pose difficulties for other countries that route traffic through Russia and its infrastructure, something which is difficult to define. The effects of the test will certainly be sufficiently studied and anticipated to prevent the occurrence of a real disaster like a long-term compromise of the functioning of major infrastructures such as transport. More likely consequences are the malfunctioning or slowdown of websites frequently used by the average user. Most of these websites operate from multiple servers located across the globe. *Wired* magazine gives the example of a news site that depends on "an Amazon Web Services cloud server, Google tracking software and a Facebook plug-in for leaving comments", all three operating outside Russia.

Economically speaking, due to the complex infrastructure of the Russian Internet and its strong connections with the rest of the world, such a test would be difficult and costly to implement. In February 2019 the Accounts Chamber of Russia opposed this legislation on the grounds that it would lead to an increase in public expenditure to help operators implement technology and to hire additional staff at Roskomnadzor, the

communications monitoring agency, which will open a centre for the supervision and administration of the communication network. The Russian Ministry of Finance is also concerned about the costs associated with this project. Implementing the law could be costly for companies and encourage corruption.

Lastly, from the point of view of political freedoms, the new initiative is provoking the mobilisation of citizen movements. "Sovereignty" carries even greater risks of censorship. The system would be supervised and coordinated by the state communications monitoring agency, Roskomnadzor, which already centralises the blocking of thousands of websites, including major information websites. The implementation of this project would broaden the possibilities for traffic inspection and censorship in Russia, says the Roskomsvoboda association. As mentioned above, it could facilitate the possibility of shutting down the Internet or controlling some of its applications, such as Telegram (which the Russian government tried to block unsuccessfully in spring 2018). A similar attempt at a cut or "Internet blackout" was made in the Republic of Ingushetia as part of a mass mobilisation in October 2018, when the government succeeded in cutting off traffic almost completely. A demonstration "against the isolation of the Runet" united 15,000 people in Moscow on March 10, 2019 at the initiative of multiple online freedom movements and parties, reflecting concerns expressed in society.

Is it possible to break away from the global Internet today, and what are the consequences? It is difficult to anticipate all the implications of such major changes on the global architecture of the Internet. During the discussion on the draft law in the State Duma, Deputy Oleg Nilov, from the Fair Russia party, described the initiative as a "digital Brexit" from which ordinary users in Russia will be the first to suffer. As has been seen (and studied) on several occasions in the recent past, information and communication network infrastructures have become decisive levers

in the exercise of power, on which governments intend to exert their full weight. But, as elsewhere, the Russian digital space is increasingly complex, and the results of ongoing isolationist experiments are more unpredictable than ever.