Analyses OSW

CENTRE FOR EASTERN STUDIES 19.04.2019 www.osw.waw.pl

The Runet fortress: the Kremlin's struggle with the 'hostile' internet

Maria Domańska

On 16 April, the Russian State Duma passed a bill on the 'sovereign Internet' with the votes of the 'party of power', United Russia. The declared aim of this bill is to create an infrastructure that will allow the Russian segment of the Internet (the 'Runet') to function in a situation when foreign servers are cut off (those who put the bill forward point out to the risk of hostile moves from the USA). To respond to threats to the Runet's security, a state-administered centralised system for controlling internet traffic in the Russian Federation, including internet traffic exchange points and cross-border data transfer, is to be created.

Internet operators will be obliged to install 'technical measures to counteract the threats' in online traffic, as well as provide designated state authorities with extensive information, including the use of the network infrastructure, network addresses that are supported, data transfer routes, internet traffic exchange points and cross-border links. The operators will be also obliged to co-operate with law enforcement authorities as regards testing internet security in Russia. The bill appeals for the 'cross-border component' in internet communication between Russian users to be minimised. Furthermore, a 'national domain name system' is to be created (by the end of 2020) which will be autonomous of the global DNS system managed by the US-based organisation ICANN. Some regulations of the bill are expected to come into force as early as in November 2019. The discussion over the bill has revealed a difference of opinions inside the Russian government regarding the desirable content of the act (criticism has come not only from expert circles but also from the government and the Accounts Chamber).

Commentary

- The argument that the bill must be passed to ensure protection from external cyber-sabotage has a strong ideological undertone. This is a reflection of growing fear among the key Russian decision-makers, whose origins lie in the secret services, of the threat posed by the United States (they claim that the US wants to bring about regime change in Russia). It also reflects their perception of the virtual sphere as a space of quasi-military confrontation. By signalling the possibility of isolating the Russian internet from the global network (its 'sovereignisation') and centralisation of its administration, Russia demonstrates its great-power ambitions ('sovereignty' is understood here as total independence from the international environment). However, this does not so much offer

a guarantee of protection from cyber attacks as it enables control of the Runet to be maximised. The bill should thus be viewed in the domestic political context above all.

- The document is another manifestation of the Russian government's consistent efforts to tighten control of the virtual sphere that began in 2012. Intensifying control and repression in the case of any manifestations of independent social and political activity (including by the use of the internet and social networks) is treated as an important instrument for counteracting alleged threats to the authoritarian system of government. This fits the paradigm of confrontation with the West which is used as an ideological argument for the Kremlin's tightening its grip in domestic politics. The bill is also a result of the unsuccessful attempts by control and law enforcement agencies to block larger sections of the Runet (including the failed attempt to block the Telegram messenger service in 2018). It reveals a mindset typical of Russian decision-makers, where security prevails over development and the state dominates any spheres of social activity.
- Given the country's economic stagnation, the Western economic sanctions, the deteriorating financial situation of the Russian public and falling public support for the government, we should assume that the Kremlin is concerned about a possible outburst of public protests on a much larger scale than before. These concerns are accompanied by the assumption that the protests will be inspired from the outside (this is how the Kremlin perceived the mechanism of the 'colour revolutions' in the post-Soviet area, the Arab Spring and the political protests in Russia). Since control of the public is viewed as an essential condition to guarantee the elite's security, the bill's overriding goal is to create an effective, centralised system of control of the transfer routes and the content of data, above all in the cross-border aspect. It would offer the opportunity to block selected segments of the Runet, user groups, regional fragments of the network and 'disloyal' content. Collecting data on users and their activity in social networks will also be easier, which is expected to both facilitate repressions and bring about a 'freezing effect', and make users more inclined to employ self-censorship.
- The implementation of the bill's provisions will reinforce the trend visible over the past few years wherein the powers of the secret services (mainly the FSB) are expanded. These powers include harvesting citizens' sensitive data without restriction and without the need to present any legal grounds, and using this data during operational activities. New legislation is usually introduced to legalise methods that have already been in practical use for years.
- The obvious beneficiaries of the bill, apart from the secret services (above all the FSB) will be the Federal Service for Supervision of Communications, Information Technology and Mass Media (*Roskomnadzor*), which is tasked with coordinating the actions envisaged in the bill, as well as the entities selling the necessary equipment and software. In Russian reality, this creates opportunities for enormous financial abuses and the siphoning of significant amounts of money from the state budget. It is unclear what the total cost of implementing the bill will be: it should be assumed that the proposed sum of around 30 billion roubles (less than US$500 million) is many times lower than really needed – and so the additional costs, which are difficult to assess now, may be imposed on internet operators. Along with the procedural requirements, including those resulting from the implementation of the orders from the secret services, this may lead to

ousting smaller Russian operators and foreign entities – even such global firms as Google or Facebook – from the market, and thus to the gradual centralisation and nationalisation of the internet services market (over 5000 Internet operators are currently functioning in Russia, and 70% of the broadband internet is controlled by five entities). This will mean redirecting profits to a small group of selected firms controlled by the state or the Kremlin-linked establishment.

- The wording of the bill is very imprecise, and leaves many doubts as regards the effectiveness of its implementation and the final shape of the technical solutions. The proposal of creating a 'national domain name system' is particularly unclear. It is also an open question what kind of 'technical measures to counteract the threats' will be used on the links (most likely the DPI [deep packet inspection] technique will be employed, which allows the contents of data packets to be analysed), and how they will affect the effective functioning of the internet infrastructure. The most vital questions are only to be determined in a more precise manner in the executive acts. It cannot be ruled out that the interpretation of the adopted regulations will be modified as they are being implemented. The entire implementation process may take years and may ultimately have limited effects, but will still allow selected groups to strengthen their position in the Russian ruling elite.