ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

December 2016

FIIA COMMENT 26/2016

Katri Pynnöniemi & Martti J. Kari
Finnish Institute of International Affairs

Russia's New Information Security Doctrine: Guarding a besieged cyber fortress

Russia´s new Information Security Doctrine follows the line adopted in previous strategic documents whereby Russia is perceived as a besieged fortress. The doctrine identifies a number of external threats to Russia's information space and calls for intensified monitoring of the Russian segment of the internet, Runet.

On 5 December 2016, President Vladimir Putin signed a new Information Security Doctrine of the Russian Federation, replacing the Information Security Doctrine published in 2000. The Doctrine is one of the strategic planning documents and, as such, it expresses the official view about the management of national security in the information sphere. Rhetorically, the text resembles the National Security Strategy, adopted in December 2015, which signalled a heightened sense of threat towards Russia, and underlined the importance of maintaining strategic stability. Consequently, the spirit of the new Doctrine is sharper, almost bellicose in tone, and the threats are described in more concrete terms.

The information sphere is defined in a broader sense than in the previous doctrine. The key term in this regard is "informatization", which refers to social, economic and technical processes for adopting and expanding information technology in society and the country as a whole, and for securing access to information resources. This change indicates recognition of the role of the information sphere in technological development but, most importantly, regards it as a tool to change the fabric of society. The Doctrine describes how this tool is used in the interests of Russia's national security, and calls for an increased role for internet and information security management and the domestic production of information technology.

The overall change in the Doctrine stems from a sharper and more nuanced view of threats to information security. The increased cyber-attack capabilities of (unidentified) foreign countries for military purposes is identified as a major negative factor. Furthermore, it is stated that cyber espionage has intensified towards Russian state agencies, scientific institutions and the defence industry. According to the Doctrine, the scale of information-psychological influence is increasing, as is the number of cyber crimes in the banking and financing sectors.

The Doctrine views Russia's national interests in the information sphere through the prism of "strategic balance". The use of this concept indicates both where the problem lies from Russia's viewpoint, and how the country seeks to manage it.

Russia has not managed to reduce the lead held by Western countries in technology development. For example, the lack of Russian supercomputers has been on the Russian political agenda for years. This topic was mentioned in the draft Doctrine published in June 2016, but removed from the final version. An insufficient level of development in domestically produced information technology and services and production capabilities leads to a dependence on foreign information technology. This, in turn, makes Russia's social and economic development dependent on the geopolitical interests of foreign countries, as the problem is described in the Doctrine. To mitigate these risks, the domestic production of hardware and software should become a priority.

However, an improvement in domestic technology production would take years and may not produce the desired results. Hence, the Doctrine includes a blueprint for how to diminish the impact of Russia's technological inferiority, as befits the country's great power status. The idea is that by building a new international information security system, namely rewriting the international legal norms regulating the international information domain, Russia may prevent the use of information technology from disturbing the strategic balance between the great powers. It seems unlikely that this plan will succeed, at least on the scale that Russia envisages, or then it will take a long time.

Hence, Russia has started with the less time-consuming issue: strengthening the walls around Runet. The new Doctrine identifies the protection of people's rights and freedoms in the information sphere, including access to information and

Finnish Institute of International Affairs
Kruunuvuorenkatu 4
POB 400
00161 Helsinki

Telephone
+358 (0)9 432 7000

Fax
+358 (0)9 432 7799

www.fiia.fi

the use of information as issues of national interest. At the same time, it is suggested that a balance should be struck between citizens' rights to the free exchange of information and the limitations caused by the need for national security in the information sphere. The text also highlights the need for the continuous monitoring of information security threats. This indicates the increasing control over the Russian segment of the internet exerted by the security authorities as a part of the response to the internal and external threats in the information sphere.

As a legal measure for information security management, in July 2016 President Putin signed amendments to the Federal Law "On Counteracting Terrorism" and to the Criminal Code. These amendments, dubbed the "Yarovaya Laws", require mobile network operators and internet service providers to retain and store data on users, user activity and user communications on Russian territory for one year. They are also required to retain and store the content of user communications on Russian territory for up to six months as of July 2018, and to enable Russian security agencies to decrypt such correspondence.

To sum up, the Information Security Doctrine adopts the view taken in previous strategic documents, namely by portraying Russia as a besieged cyber fortress. At stake is the strategic balance, which refers to Russia's aspiration to maintain its great power status. The Doctrine prioritizes the development of Russia's own information technology, including research and development activity. Its goal is to rewrite the international legal norms to alleviate dangers to Russia's national interests posed by its own underdevelopment, and to increase the monitoring of the information sphere inside Russia.