PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 111 (1807), 8 JUNE 2021 © PISM

BULLETIN

Online Warfare:
Russian Policy on International Information Security

Agnieszka Legucka

Russia in April this year updated its policy on international information security (IIS). Compared to the previous version of the document from 2013, Russia points to the possibility of an inter-state conflict as a result of activities in cyberspace. Russia also promotes the concept of "sovereign internet" and aims to increase its influence in the field of global regulations concerning the development of the network. The publication of the document confirms the priority for information security in the national security strategy and in the foreign policy of the Russian Federation.

Russia's Goals and Interests. Russia emphasises the political and social nature of the global confrontation in the information sphere. It considers the struggle in cyberspace to be part of an information war waged against it by Western countries. This distinguishes the Russian perception of information security from the Western discourse, which is dominated by concerns about the security of personal data and protection against cyberattacks (e.g., on critical infrastructure).

According to President Vladimir Putin's Executive Order on the "Principles of State Policy of the Russian Federation on International Information Security", approved on 12 April, Russia is striving to strengthen the role of government entities in the information space. In domestic politics, this is dictated by the need to restrict Russian citizens' access to independent content in order to prevent social unrest and internal destabilisation. In the international dimension, Russia has announced that it will try to ensure global peace, security, and stability while seeking to gain influence over regulation of the information sphere. It also means a change in the Russian definition of IIS compared to 2013 when the importance of protecting the rights of individuals, societies, and states in the information sphere was emphasised.

Russia's new declared goal of policy in the field of IIS is to prevent and regulate inter-state conflicts in the information sphere. According to the previous version of the document, Russia wanted only an increase in its impact on regulating the information security system. The Russian authorities still want to strengthen control over internet traffic (the "sovereign internet" concept) and media content, and to introduce a code of conduct for states in cyberspace. Russia is active in multilateral forums, including the United Nations, devoted to information-security issues, and aspires to become a creator of standards in this area.

The assumptions of Russia's information security policy comprise a strategic planning document. It fits in with its ideas to date in the information sphere. In the Military Doctrine of 2014, the National Security Strategy of 2015, and the Doctrine of Information Security of 2016, Russia included information in the defensive and offensive catalogue of the Russian military capabilities.

Challenges and Threats for Russia. The threats identified in the field of IIS mainly relate to the use of technology in the information space, such as disruptions to storing and delivering information or attacks on software and hardware. However, the catalogue of threats and challenges in the field of IIS clearly contrasts with Russia's activity in the internet. Hacker attacks also were identified as one of the threats. Although the Russian government admitted that last year there were more intrusions into Russian federal agencies, it is the Russian authorities that are most often responsible for organising cyberattacks around the world. The largest one took place in December last year when many U.S. government agencies, including the Treasury and Defense departments, were attacked. Thousands of users allowed a virus onto their computers through updates to SolarWinds software. At the same time, Russia emphasises that the technological dominance of other countries (i.e., the U.S.) remains a challenge for it, although Russian spending on research and development is at a low level (around 1% of GDP, compared to the EU, which allocates around 3%).

Other threats indicated in the document include the use of technology for terrorist, criminal, and extremist purposes. However, the laws dealing with these threats often become a pretext for the Russian authorities to control their own citizens. Due to the popularity of opposition activist Alexei Navalny on the internet (a film he published about President Putin had 116 million views on YouTube in April this year), his Anti-Corruption Foundation has been accused of extremism and is likely to be banned as a result.

The International Dimension of Russia's Policy. One of the IIS regulatory instruments is the Russian proposal to adopt a thematic convention within the UN framework on information security. So far, the Russian ideas have not gained wider international support. Although it managed to win the majority of votes in December 2018 for two resolutions in the General Assembly, they are non-binding.

The first of the resolutions called for increased powers of states in the management of cyberspace and also stipulates that any accusations by a state(s) of illegal online activities against another state must be justified and take into account all relevant information, including technological possibilities, as well as the consequences that may result from such accusations. The effect is to blur the responsibility of the attacking party. In the resolution, Russia also proposed extending the Group of Governmental Experts (GGE) to all interested UN states, which prepares the rules of conduct of states in cyberspace. This would enable Russia to push through the "sovereign internet" concept and adopt a binding convention in the future.

The second Russian resolution concerned the fight against cybercrime. Russia wants to transfer the coordination of cooperation between states from the level of the Council of Europe to the United Nations, as it has not ratified the Council's 2001 Convention on Combating Cybercrime. Russia rejected the possibility of the services of other countries carrying out cyber operations on its territory because, according to the Russian authorities, doing so would violate Russia's sovereignty.

In the field of international regulation of the information sphere, Russia finds supporters among third countries, including members of the Shanghai Cooperation Organisation (SCO), the Collective Security Treaty Organisation (CSTO), as well as ASEAN and BRICS. They support Russia both at the UN and in combating threats at the regional level. On 1 April 2019, the "Agreement on cooperation in the field of information security between Member States of the CSTO" entered into force.

Conclusions. The updated principles of Russia's IIS policy confirm that, unlike in Western countries, the Russian authorities do not see the need to protect individual rights in cyberspace. Instead, Russia insists on sovereignty in the information space, and more state control of network traffic and media broadcasts. This will of course strengthen the political regime in Russia by restricting access to independent content for its citizens.

With the strengthening of authoritarian regimes in the world, it is becoming more and more likely that the "sovereign internet" concept will be implemented, both at the global (UN) and regional (CSTO, SCO) levels. Although Russia is gaining the support of some UN members, African and Asian countries, including China, to increase regulation at the intergovernmental level, it has so far failed to push through a binding IIS convention.

Russia perceives the information sphere as an area of international confrontation in which a conflict may break out between states. Despite Russia's declarations on peace and preventing cyberattacks, Russia will improve its technological capabilities in the area of communication and information and use them for military-political purposes. Since its annexation of Crimea in 2014, Russia has pursued coordinated hybrid actions against Ukraine. It is also acting against EU countries. They have become the target of attacks aimed at undermining public confidence in their governments, which is particularly important in the context of the upcoming elections in Germany (2021) and France (2022).

The prospect of network fragmentation, such as erecting barriers to internet traffic, may have negative consequences for Western countries, including Poland. It will hinder communication with the societies of Eastern Europe (particularly in Russia and Belarus). Therefore, Polish diplomacy can support initiatives aimed at increasing cybersecurity and strengthening international regulations on the protection of personal data and the fight against cybercrime, without prejudice to the protection of individual rights online.