

NEW POLISH NATIONAL STRATEGY PRIORITIZES CYBERSECURITY AND INFORMATION SECURITY

The latest National Security Strategy of Republic of Poland published recently describes and gives strategic aims in two particularly important areas of security: cybersecurity and information security. Including both is important and it proves that the authorities of the countries noticed its strategic significance and coming potential threat for the security of the state.

Who is our opponent?

The strategy characterizes Polish security environment accurately pointing out the Russian activities under the war threshold as the main threat. Russia used a variety of nonmilitary tools such as cyberattacks and disinformation. However, this characterization is not sufficient and omits the fact that disinformation is just one of the tools in Kremlin information arsenal, which should be characterized as the modern diversion to cover all Russian activities in the grey area under the war threshold. The strategic opponent who can use the nonmilitary actions is in strategy limited to Russia. There are no mentions about China, despite its rising interest in the Central Eastern Europe, and neither remarks about Iran and North Korea, countries which in the past conducted successive cyberattacks against targets in Poland. The intelligence and counterintelligence of other countries in the neighborhood warned about the cyber threat from the above countries.

Technology as a spur of economic development

Strategy rightly identifies the role and significance of digital technology and the opportunities they rise. 5G network, the Internet of Things, cloud computing, quantum computes are particularly important for the development of Poland. They may create new chances but also bring novel risks. The strategy stressed that the proper way of new technology development may create opportunities for Poland to join the club of countries with the most effective and advanced digital economies. This aim is ambitious and rightful but considering the fact that Polish economy is currently aimed at increasing social spending and offers literally no initiative for creative hardworking men and women, it could only stay at designing phase. In addition, the research and development expenditure are one of the smallest in the EU. It is a pity that strategy does not stress a particular role of these technologies for the national security and strengthening the armed forces.

Cybersecurity

Cybersecurity was put under the first pillar of National Security Strategy of Republic of Poland: Security of States and Citizens. The strategy stressed the necessity to increase the resilience to the cyber threats and recommend increasing the data protection and educational activities promoting cyber hygiene.

The security is complementary with the main pillar of cybersecurity in Poland, which is the domestic

cybersecurity system bill. The reference to it is relevant and underscores the continuity of cybersecurity system in Poland. Strategy also stressed the military aspect of operations in cyberspace by pointing on necessity to gain a capability to conduct a full spectrum of military operation in cyberspace, which means the ability to conduct CNE (Computer Network Exploitation), CNA (Computer Network Attacks), CND (Computer Network Defense) operations. These operations should be realized by the Polish Cyberspace Defense Army (Wojska Obrony Cyberprzestrzeni), which should be fully operational till 2023.

Strategy also points out a basic cybersecurity requirement such as developing own capabilities to test and certificate products. Not only does strategy require it but also the EU 5G Tool Box. The certification process will be used in securing implementation of 5G technology, so it is important for developing cybersecurity policy. Strategy also mentions the importance of enhancing knowledge and skills within public administration.

Cybersecurity is based on innovation and advanced research and development and these elements are also included in strategy. Poland plans to develop own capabilities and create Polish cybersecurity solutions and open research project led by country authorities with the active participation from Polish Universities and other research institutes. Particularly important should be increasing cryptology capabilities by producing homemade devices. It is a consequence of international spy affair with Swiss cryptology manufacturer Crypto AG, which was controlled by American and German intelligence. This scandal proves the necessity to develop own cryptology solutions. However, achieving these ambitious aims would be very difficult if not impossible without structural reforms. Polish universities in international rankings are far away from the top and occupy positions between 400- 500. The salaries of researchers are low and the professional career at the university is no longer an attractive option for young people. There is also a long-term problem with transforming research projects into the commercial product. Without solving this daunting problem, the ambitious plans drafted in the strategy will be never realized.

To sum up, cybersecurity in Polish National Security Strategy is presented in an appropriate way and includes the most important points such documents should have. However, the problem of strategic documents in Poland is a lack of implementation and realization of strategic aims. Hopefully, this time the situation will change.

Information space

Polish National Security Strategy mentions separately not only cybersecurity but also the information space, which is classified as the first pillar likewise the cybersecurity. Information space consists of three layers: virtual, physical, and cognitive and therefore it is necessary to build up capabilities on strategic level to protect information sphere. Information space and cybersecurity are interlinked and security of former one could not be considered without the latter one. It is very promising that strategy notices this interdependence.

Another good idea of this document is to create, comprehensive and unified strategic communication system. Currently, the responsibilities are divided between Ministry of Defense, Ministry of Foreign Affairs and Ministry of Digital Affairs and these institutions could not agree even how to define strategic communication. The one institution could solve these problems and increase effectiveness and cooperation.

Strategy also stressed the principles of fighting with the threats in information sphere such as disinformation. Education, rising society awareness and effective cooperation with media and NGOs are the next vital elements necessary to develop information sphere protection. Nonetheless, it could not happen without changing the attitude of state authorities and publication institutions to work with

journalists and NGOs. Currently, Poland position World Press Freedom Index dropped significantly from 47 in 2016 to 62 in 2020.

The last recommendation in information space touches the issues of improving the national security management through integration of widely distributed tools and solutions. And it is a correct direction, but strategy does not deliver details about it and it's not clear if this idea includes the cybersecurity and information sphere.

Separation of cybersecurity and information sphere security in National Security Strategy 2020 is a positive and promising aspect, that Polish government noticed the growing significance of these two security areas. Currently, pundits agree that any armed conflict will start in these domains. Including them in the most important document for Polish national security gives them strategic priority they really need. The aims of cybersecurity and information sphere security in strategy are clear, ambitious and cover majority of the most important aspects of them on strategic level. Finding out that two areas are interdependent and should be developed altogether is also very enriching aspect of this strategy and proves that authors followed the latest trend in security studies. The main problem lies not with the strategy but with the process of operationalizing it. Too long in Poland various strategies were just a piece of paper, now it is time to change this trend and make National Security Strategy really work in practice.