PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 115 (1811), 14 JUNE 2021 © PISM

BULLETIN

Strengthening the EU's Role in Cybersecurity

Aleksandra Kozioł

The ongoing pandemic has increased the use of digital technologies and intensified the threats they pose. Therefore, the EU faces the need to strengthen its ability to detect and respond to hostile cyber activities. New initiatives should, above all, improve the cooperation of EU institutions with Member States and private entities. However, their effectiveness will be limited by low and dispersed financing.

Strategy for the Digital Decade. In December 2020, the European Commission and the High Representative for Foreign Affairs unveiled a new cybersecurity strategy that aims to strengthen collective resilience against cyberthreats and ensure the protection of digital services and tools in the EU. Its implementation is also intended to ensure the Union a leading role in setting international norms and standards in cyberspace.

Together with the strategy, two legislative proposals were published. They include the so-called NIS 2 Directive, which concerns increasing the cyber resilience of the Union, and the directive on the resilience of critical entities. The new regulations are to improve cooperation and information exchange at national and EU levels, they also expand the catalogue of sectors important for cybersecurity by digital services, health and space, among others. Their advantage is a comprehensive approach, combining protection against cyberattacks with the prevention of traditional threats such as crime and natural disasters.

Growing Threat. The functioning of ICT systems increasingly affects EU economies, institutions and external actions. The reliance on digital technologies has become especially visible during the pandemic, as 40% of EU workers switched to remote work, and an increase in web traffic by up to 60% exacerbated attacks on users. Such attacks affect not only the security of systems and information but also lead to severe financial losses—it is estimated that the cost of attacks on a global scale in 2020 amounted to €5.5 trillion.

Providing open access to the internet and ensuring the security of digital technologies requires international cooperation, which is hindered by authoritarian states' actions. They often support the activities of hacker groups or engage their own special military units online. In December 2020, for example, the European Medicines Agency was attacked, from which hackers—possibly connected to Russia and China—stole data on vaccines against COVID-19. Difficulties in identifying the perpetrators, however, make it difficult to react, which is why the EU has imposed sanctions for cyberattacks only twice, in those instances covering several entities from Russia, China, and North Korea.

New Cooperation Initiatives. The effectiveness of the fight against cyberthreats is based primarily on the ability for early detection and response before damage occurs. Member States, recognising the benefits of cooperation, initiated several PESCO projects in this area, such as cyber rapid-response teams. Defence against attacks in cyberspace, however, requires coordinated actions on a larger scale, which is to be served by the creation of a network of Security Operations Centres across the EU. They will be supported by artificial intelligence technologies, improving the detection and accelerating the analysis of incidents. Better anticipation is also to be ensured by the establishment of a cyber-intelligence working group at the EU Intelligence and Situation Centre. Overcoming Member States' scepticism about delegating national competences will, however, require a precise definition of the group's role in the Union's system, for

example, taking into account the European Cybercrime Centre's tasks at Europol.

The scale of cyber incidents means that an increasing number of entities from Member States and the EU is involved in combatting them. This raises difficulties in the exchange of collected information, as well as establishing cooperation at the operational and technical levels. The Joint Cyber Unit will contribute to the improvement of crisis response and recovery capacity. Its tasks are not precisely defined yet, which raises concerns about duplicating existing competences, for example, of Union bodies—the EU Agency for Cybersecurity (ENISA) or the Computer Emergency Response Team (CERT-EU).

Building an International Position. Cybersecurity is an important element of the Union's external action. Cyberspace as an operational sphere influences the conduct of EU missions and operations and is also important for security in the global dimension. The main goals and tasks are to be set out in the "EU External Cyber Capacity Building Agenda", which will be supported by the EU Cyber Capacity Building Board. The Union is also considering setting up an informal Cyber Diplomacy Network to promote a secure cyberspace. Activities will focus on deepening cooperation with partners, including NATO, and the promotion of security standards in cyberspace in the framework of international organisations, such as the United Nations and the Council of Europe.

Ensuring a leading role in cybersecurity will require the EU to improve its innovation and technological competitiveness in the global marketplace. For this purpose, in April 2021, the Council authorised the establishment of a Cybersecurity Industrial, Technology and Research Competence Centre. It aims to connect public and private centres dealing with cybersecurity issues at the EU level, and to ensure cooperation with a network of specially established Coordination Centres at the national level.

A major challenge to the coherence and effectiveness of Union cybersecurity efforts will be, however, overcoming funding constraints. First of all, funds allocated to this area are too low in relation to the needs—for the years 2021-2027, they will amount to about €2 billion at the EU level and about €2 billion annually at the Member State level, while the U.S. alone spent about $17 billion in 2020. In addition, Union funding is provided under several different instruments, which makes it difficult to plan investments in this area.

Conclusions. Improving situational awareness and information exchange between Member States and EU bodies is imperative given the scale of the threats in cyberspace. Increasing the EU's resilience to cyberattack requires, among others, securing infrastructure and methods of communication. The proposals for new instruments partially meet these needs. Member States, however, should ensure a precise division of tasks and actively contribute to improving cooperation, as well as increasing funding. For the EU as a leader in cybersecurity, investment in research and development and the creation of initiatives to attract and retain experts in the EU labour market will be required. Currently, the industry is experiencing large staff shortages, which also proves the lack of adequate education in the field of cybersecurity and low public awareness of cyberthreats.

In view of the growing vulnerability to attacks, it will be crucial to quickly adopt regulations on information security and common cybersecurity rules to be applied by EU bodies (their implementation is to be supported by enhanced CERT-EU). More attention should also be paid to the coordination of civil, defence and space aspects of cybersecurity. Separate projects are currently under development in the EU, such as the secure governmental satellite communications system (GOVSATCOM).

Safe operation of ICT systems and open access to the internet will require increased diplomatic efforts to promote responsible state behaviour in cyberspace. These are particularly important due to the aggressive actions of states such as Russia and China, which challenge international standards in this regard. Due to the global scale of cyberthreats, combatting them effectively will foster closer cooperation with partners, such as the UK and the U.S., which have offensive capabilities in cyberspace.

Vulnerability to hybrid actions, such as cyberattacks and disinformation in the closest neighbourhood of the EU, spread by, for example, Russia, negatively affects security within the EU. Poland can therefore play an active role in the process of developing the EU's cyber resilience by proposing special programmes for the associated countries of the Eastern Partnership and the Western Balkans. An important element also will be maintaining Polish involvement in the development of the space surveillance and tracking (SST) project, which will ensure safe and stable operation of technologies based on satellite data.