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

NO. 106 (2225), 7 AUGUST 2023 © PISM

BULLETIN

EU Still Limited in Cyberdefence Capabilities

Aleksandra Kozioł

The EU has developed a new cyberdefence policy after Russia's invasion of Ukraine increased the level of threats in the digital space. The policy guidelines emphasise defending against cyberattacks, as well as the development of military capabilities and coordination with the civilian sphere. However, the high fragmentation between actors responsible for cybersecurity at the EU level and lack of incentives for Member States make it difficult to achieve the intended results.

The EU Policy on Cyber Defence, presented by the European Commission and the High Representative in November 2022, is being implemented with difficulty. The policy envisages increasing the capacity to defend against cyberattacks in the EU and improve the state of the European digital sector, thus implementing the Strategic Compass and the EU's Cybersecurity Strategy from 2020, which set targets to protect against cyberattacks and improve the security of digital services. Additionally, in the EU the so-called Cyber Resilience Act to set out the cybersecurity requirements for products and two regulations to enhance digital and information security in EU institutions are still under review.

Cybersecurity Challenges. Russian troops in February 2022 entered Ukraine backed by, among others, a cyberattack on one of the satellite networks operating in Europe. This confirmed that the digital space is a domain of warfare and that defence against cyberattacks must include actors and services from the military and civilian spheres. Cyberattacks are usually considered acts below the threshold of war, even though in the case of critical infrastructure such as electricity grids or satellite networks, these attacks can not only paralyse them but also cause physical damage. According to the EU Agency for Cybersecurity's (ENISA) "Threat Landscape 2022", both the number and the impact of cyberattacks, digital surveillance, and disinformation campaigns are increasing in the EU. They are also more often used by states in support of political objectives.

The growing interconnections in the digital space requires mechanisms for joint deterrence and building of capabilities not only to protect against cyberattacks but also to defend when attacked. Currently, these areas are mainly the responsibility of the Member States, although their capabilities vary, while the EU supports them, however only to a limited extent, mainly in the civilian sphere. Given the cross-cutting nature of cyberthreats, at the EU level four actors are responsible for supporting the states: ENISA, the Computer Emergency Response Team (CERT-EU), the European Cybercrime Centre (EC3) at Europol, and the European Defence Agency (EDA). These entities signed a cooperation agreement in 2018, but the EU's capacity to defend against cyberattacks remains insufficient, while cooperation—particularly on military issues—is limited. A greater role in this context is played by NATO.

Cyberdefence in the EU. Implementation of the policy is based on building capabilities and deepening cooperation between the Member States because military action in the digital space is within their competences. The EU plays a supporting and coordinating role, with cooperation between military and civilian actors as the basis for a comprehensive approach. The latter is particularly important given the increasing level of interdependence between the armed forces and the civilian sector.

The main policy goal—building joint capabilities to defend against cyberattacks—was to be achieved by the establishment of new cyberdefence units at the EU level and their integration into the existing civilian cybersecurity system. The leading role in the new cyberdefence system was tasked to the EU Cyber Defence Coordination Centre (EUCDCC) in order to provide situational awareness for the Member States and EU missions and operations. In addition, the EDA is to support operations of the networks for military Computer Emergency Response Teams (MICNET) and the EU Cyber Commanders Conference, meant to be a platform for discussion on cyber incidents in the armed forces. Cyberdefence capabilities in practice were to improve through the CyDef-X joint exercise project and the cyber reserve, established with services from trusted private providers. The creation of so many new units along with the relevant competences has proved difficult to implement in practice. In February 2023, the EDA belatedly created the MICNET proposed in the Policy on Cyber Defence, and it was only joined by 18 out of 27 EU countries.

Other policy guidelines intended to improve European industry through Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF), among others, require rapid strategic assessment of emerging and disruptive technologies (EDTs) applicable to the digital sector. The policy, however, did not identify the essential investments the Member States would be required to undertake, while, for example, independence from third countries in critical cyber technologies and increasing the attractiveness of the cyberdefence sector for skilled experts is currently lacking in the European market, though it is necessary to strengthen the EU's international position.

Prospects for Cooperation. The publication of the Policy on Cyber Defence did not significantly increase the awareness of the states about the importance of cooperation in the light of current cyberthreats, nor did it translate into an increase in their commitment to building joint cyberdefence capabilities, as evidenced by the nature of PESCO projects, among other things. The Cyber and Information Domain Coordination Centre (CIDCC), on which the Cyber Defence Coordination Centre is to be based, has so far involved only four countries (France, Germany, Hungary, and the Netherlands), and the largest project, the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT), comprises only eight countries (Belgium, Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania, and Slovenia). Although two new PESCO cyber projects were established by the Member States in May 2023, three and four countries, respectively, are participating in them. Cooperation on cyberdefence is limited especially in comparison to the development of conventional military capabilities in Europe. For example, under the PESCO project Military Mobility (MM), 25 EU countries (apart from Denmark and Malta), as well as four global partners—Canada, Norway, the United States, and the United Kingdom—cooperate.

The EU's ambitions for cybersecurity at the international level have increased since the start of the Russian full-scale aggression against Ukraine. Sharing experience and supporting the capabilities of Eastern Partnership and Western Balkans countries most vulnerable to cyberattacks became a key objective. Through the European Peace Facility (EPF), for example, the Union funded software and hardware for the Ukrainian Armed Forces, enabling a cyberdefence training centre to open in Kyiv in December 2022. Under the guidelines of the new policy, further support will be available in particular to candidate countries that align themselves with the EU's Common Security and Defence Policy. The EU is also consistently addressing the topic of cybersecurity in bilateral relations, holding in 2022, among others, the eighth dialogue with the United States and the second with Ukraine. However, establishing a permanent information-sharing mechanism remains a challenge in U.S.-EU relations, despite the fact that, for example, in 2016, the EU's CERT-EU and NATO's NCIRC concluded a technical agreement enabling information-sharing on cyberdefence matters, and the two organisations have been cooperating on cybersecurity issues since 2010.

Conclusions. The cross-border nature and impact of cyberattacks has increased the need for joint action, to which the EU Policy on Cyber Defence responds. However, institutional fragmentation and the unclear division of competences between military and civilian units hinders cooperation and reduces the commitment of Member States, although the document refers to the mutual assistance clause in Article 42(7) TEU, which operates similarly to Article 5 in NATO. Currently, cooperation within the framework of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)—due to recognised experience—is more attractive, with countries outside the Alliance gradually joining it, including South Korea in 2022 and Ukraine in 2023.

The development of military capabilities to defend against cyberattacks at the EU level should respond to current hybrid threats, including from Russia. Therefore, the implementation of the Policy on Cyber Defence that separates the activities of military and civilian entities should be assessed as the wrong approach in this context. MICNET, for example, will only begin to cooperate with CERT-EU once its capabilities are formed. Terminology standardisation or exchange of experience in operational techniques would be more beneficial if conducted in parallel to the creation of a new unit. Poland, which has three separate response teams at the national level—governmental, military, and research—will not only be able to easily join the work at the EU level but also to offer its own experience in their operation procedures. At the same time, considering the growing threats from Russia and Belarus, it would be worthwhile for Poland to increase investments in the cyberdefence sector with EU funds, among others, EDF and Digital Europe.