PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 79 (2198), 22 JUNE 2023 © PISM

BULLETIN

EU and NATO Countries Strengthen the Protection of Critical Infrastructure

Filip Bryjka, Tomasz Zając

New EU regulations on critical infrastructure could strengthen the resilience of the Member States to hybrid threats from Russia and China. The main challenge, however, will be to develop and implement precise standards for the protection of such infrastructure jointly with NATO. It will be necessary to exchange experience in this regard among states and on the state-private sector line. This may provoke resistance among some Member States reluctant to share sensitive information.

Russia's invasion of Ukraine has increased the risk of Russian hybrid actions, including cyberattacks, acts of sabotage and subversion targeting critical infrastructure (CI) in EU and NATO countries. The explosion of the Nord Stream 1 and 2 pipelines has demonstrated the vulnerability of seabed infrastructure to such threats. Since the beginning of 2023, the intelligence services of Norway, Denmark, and the Netherlands have reported increased Russian activity aimed at reconnaissance of seaports, pipelines, fibre-optic cables, oil platforms, and wind farms. Russia conducts these activities using warships (including submarines), unmanned aerial and surface vehicles, research vessels, and special forces. Russia's increased intelligence activity may indicate preparations for sabotage attacks, the purpose of which may be, for example, to disrupt the transportation of energy resources or data transmission in order to undermine the economies of EU and NATO countries and influence their stance on supporting Ukraine. Indirect threats to CI are also posed by Chinese investments in the ICT sector (5G network), or Chinese takeover of ports and marine terminals. There is a risk that such infrastructure could be used to conduct mass digital surveillance, or block supply chains.

Changes in the EU's Approach to Protecting CI. Although the management of CI is mainly the responsibility of Member States, at the EU level there is also a number of standards aimed at protecting it. These are contained in the 2008 CI Directive, the 2014 EU Strategy for Maritime Security, and the 2019 Regulation establishing a framework for monitoring foreign direct investment, among others. Additional rules were introduced after the Russian full-scale invasion of Ukraine, for example, the tenth package of sanctions against Russia prohibits Russian citizens from sitting on the governing bodies of CI-related companies.

The European Commission (EC) has decided to replace a key 2008 directive on CI protection with a new piece of legislation that better meets current security challenges. Member States will have to implement it into their legal orders by October 2024. Its provisions will now cover 11 sectors (including digital infrastructure and banking), a significant expansion of its scope compared to the 2008 directive, which listed only two such areas (energy and transport). The approach to the subject of CI protection itself has also changed. The earlier directive emphasised prevention—the most important goal was to prevent an unwanted CI event such as a terrorist attack. While the current act still places considerable emphasis on protecting such infrastructure from unwanted incidents, since it may be difficult to prevent them, it is equally important to prepare the process associated with their occurrence and remediation (e.g., preparing alternative supply chains in advance). The directive also provides for the possibility of sharing best practices among the Member States, to be facilitated by a specially created Critical Entity Resilience Group, which will include representatives from EU countries and the EC.

Another sign of the EU's greater commitment to protecting CI is the Commission proposal in March of this year to revise its maritime security strategy. Additional areas will now be monitored as part of the EU's coordinated maritime presence, in order to prevent events such as the explosion of the NS 1 and 2 pipelines.

EU-NATO Cooperation. The new EU CI directive is part of the implementation of the objectives of the 2022 Strategic Compass adopted in March. Strategic Compass, which sets out the EU's security and defence policy objectives. The document primarily emphasises the need to strengthen CI protection against cyberattacks, secure communication lines and supply chains. The Union intends to achieve these goals in cooperation with NATO. In January this year, the organisations signed a third declaration of cooperation and established *NATO-EU Task Force on Resilience of Critical Infrastructure*. It was created to share information and good practices on CI protection, and develop guidelines to strengthen CI resilience in four sectors: energy, transportation, digital infrastructure, and space**.**

Cooperation between the EU and NATO on CI protection is crucial, among others, because of the non-overlapping memberships in the two organisations of countries such as the UK, Norway, and Sweden, which is waiting to join the Alliance. The territorial waters of these countries contain elements of undersea critical infrastructure crucial to transatlantic security. The Allies have pledged to protect CI as part of strengthening resiliency. The Alliance has significant institutional experience in this area dating back to the 1950s when the Civil Emergency Planning Committee was established in NATO. In 2022, it was transformed into the Resilience Committee, which reports directly to the North Atlantic Council and sets the main directions for the Member States' strategies and policies in the area of strengthening resilience. The Committee reports to six specialised planning groups and the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), which is responsible for supporting the Member States and partners in emergencies caused by natural disasters. A special Critical Undersea Infrastructure Coordination Cell was also established within the Alliance in 2023. It is a platform for the exchange of experiences and practices between member states, civilian and military institutions, as well as the private sector (especially in the use of innovative technologies to protect CI). The Maritime Centre for the Security of Critical Undersea, established at the Allied Maritime Command in Northwood, will be responsible for the protection of underwater CI in operational terms. In response to Russia's increasing intelligence activity at sea, NATO has increased the number of warships and aircrafts patrolling areas around key elements of maritime CI**.**

Conclusions and Outlook. The EU's decision to gradually become less dependent on import of energy from Russia, as well as Russia's increased intelligence activity significantly increase the risk of Russian sabotage attacks on CI. A potential target could be gas supplies from Norway, which has become the largest supplier of this resource to EU countries. Poland's diversification of energy resources relies heavily on supplies by sea, therefore a potential target for Russian hybrid attacks could be infrastructure in the Baltic. Russia may be willing to do so in order to have a negative impact on the economic situation of EU and NATO countries, and thus discourage their societies from supporting Ukraine.

The severity of the CI threats and their transnational nature call for strengthened regulation at the EU level and coordination between NATO and the EU. The decisions so far rightly change the Union's overall approach to CI, shifting the focus from its protection to resilience. This means that in their actions, countries not only try to prevent damage to CI but must also prepare plans for the entire process associated with potential damage in order to minimise negative consequences.

To counter hostile hybrid actions against CI, the EU, and NATO should make a joint assessment of the vulnerabilities of sectors crucial to their energy and cybersecurity and propose additional solutions to increase its level of protection (such as a system for sharing CI-related experiences). In addition, they should prepare common transnational standards for assessing CI resilience. A major challenge and constraint to cooperation between NATO and the EU may be the reluctance of individual Member States to share sensitive information on their own vulnerabilities, as well as cooperation with the private sector, on which additional reporting obligations will be imposed (such as the need to conduct risk assessments on a cyclical basis). Also key to the Commission's new plans will be the question of what financial resources member states will be willing to devote to actually committing to protecting CI in the EU.