Poland first chaired the Council of the European Union in the second half of 2011. Shortly after the beginning of the Presidency, on 22 July, there were terrorist attacks in Oslo and on the Norwegian island of Utoya. They represent one of the most tragic pages in the history of terrorism in Europe. The perpetrator attacked in open public spaces. Since then, protecting such places from the effects of terrorist activity has been a priority, both in the EU Member States and in the EU institutions.

The second Presidency of the Republic of Poland in the Council of the EU began in January 2025. Poland assumed the Presidency at a time of global unrest, when the most important task is to ensure the security of the EU's external borders and the continuity of key services in EU Member States. This is reflected in the slogan of this Presidency: 'Security, Europe!'. For the Internal Security Agency and the Government Centre for Security in Poland, it is a time to undertake initiatives both at home and abroad to support the building of resilience to hybrid threats, with particular emphasis on the protection of critical infrastructure (CI) facilities, national and European (#OchronaIK).

With regard to CI, the leading theme of the Polish Presidency was shaped by:

- the war in Ukraine and the associated increase in the number of hybrid actions, including sabotage by Russian actors against CI facilities in the energy, transport, telecommunications, water supply sectors, as well as under the influence of the support provided to Ukraine by EU and NATO states;

- the implementation of the CER Directive of the European Parliament and the EU Council on the resilience of critical entities, which changes the concept of their protection in Member States and gives their governments a new impetus for action in this strategic area.

The special issue of the scientific journal "Terrorism – Studies, Analyses, Prevention" (T-SAP), prepared under the aegis of the Internal Security Agency and the Government Centre for Security, is a thematic issue. We have collected analyses and case studies on the current challenges of protecting CI on land and sea and in the cyberspace of EU countries. The authors of the articles are civilian and military experts representing academia, think tanks and specialised news portals, as well as government and law enforcement officials. They present CI security issues from different perspectives, taking into account their competences and experiences.

The publication opens with an article discussing the use of CI in hybrid conflicts and providing a comparative analysis of the solutions for building the resilience of this infrastructure arising from the CER and NIS 2 Directives of the European Parliament and the EU Council. The CER Directive is expected to bring about a sea change in building the resilience of CI to terrorist and sabotage activities. In Poland, the basis of the proposed CI protection system will be, inter alia, the idea of standardising the physical security of protected facilities, as discussed in detail in one of the analyses.

An article on past terrorist and sabotage attacks on CI may help to better understand the evolution of threats and how to neutralise them. Instead, data from Europol's annual TE-SAT (*EU Terrorism Situation & Trend Report*) from 2021–2024 provides a contribution to showing the contemporary landscape of terrorist threats in the EU. The results of the 2025 terrorism and sabotage threat perception survey may also add to this knowledge. Respondents were advisors on building resilience to terrorist threats working within the EU Protective Security Advisors initiative. European experts assessed the current challenges in this area and identified opportunities to enhance prevention and protection efforts. The EU

perspective on hybrid threats, especially in Central and Eastern Europe, is presented in an article devoted to the analysis of reports produced by the European Centre of Excellence for Countering Hybrid Threats in Helsinki.

One of the domains where conflict can take place is the maritime domain. In the special issue, we present the specificity of the hybrid threats in the Baltic Sea, which are intensifying from 2022 onwards, and the possibilities for NATO to counter them. In the article, the author pays particular attention to the threats posed by modern maritime autonomous systems. As the country holding the Presidency of the Council of the EU, we would like to share our experience in building capabilities to protect strategic facilities from unmanned aerial vehicles. We present this issue with legal and technical aspects.

In the special issue, we also address Ukraine's experience in countering and combating Russian hybrid and conventional attacks on CI facilities. Related to the Russian-Ukrainian war is the issue of sanctions. In an article, we discuss the national individual restrictive measures implemented in Poland against economic entities supporting the actions of the Russian Federation and Belarus.

The largest number of hybrid actions against EU countries' CI facilities are undertaken in cyberspace. We present specific cyber security incidents in selected European countries caused by state-sponsored, hacktivist and cybercriminal groups. We also describe the different reporting strategies adopted by the services and teams responsible for the cyber security of EU and NATO countries, giving an overview of the cyber threats currently facing Europe.

An important support in shaping national and EU initiatives to increase CI's resilience to hybrid threats, including terrorism and sabotage, are research projects implemented with EU funds. Therefore, we have decided that it is worth discussing selected topics implemented under Horizon Europe, which is one of the EU's flagship initiatives in this area.

During the Presidency, Poland supports activities strengthening European security in all its dimensions:

external, internal, information, economic, energy, food and health. The special issue of T-SAP fits in with these objectives by showing the multidimensionality of CI protection, which is the common denominator of all these dimensions. We hope that the material presented here will contribute to the knowledge of contemporary threats to CI facilities and effective ways of countering these dangers, and will inspire not only further research and analysis, but also EU initiatives in the area of security under successive presidencies of the Council of the EU.

Karolina Wojtasik, PhD

Government Centre for Security

Damian Szlachter, PhD

Internal Security Agency