Analyses OSW

CENTRE FOR EASTERN STUDIES 4.02.2026 www.osw.waw.pl

Germany: new law on the protection of critical infrastructure

Kamil Frymark, Michał Kędzierski

On 29 January, with the votes of the CDU/CSU–SPD coalition and the opposition AfD, the Bundestag adopted a framework law on the protection of critical infrastructure (the KRITIS umbrella law), implementing the EU CER Directive on the resilience of critical entities. The new legislation introduces uniform standards for the physical security of infrastructure in key sectors: energy; transport and communications; finance and insurance; healthcare; drinking water supply; wastewater and municipal waste management; information technology and telecommunications; food supply; space; and public administration. The law applies only to entities, including railways, the banking sector, and power plants, that supply at least 500,000 people. Operators of such facilities are required, among other obligations, to carry out systematic risk analyses at least once every four years, to implement appropriate technical and organisational measures to minimise risks, and to report serious security-related incidents. The federal states may identify additional critical facilities in areas that fall exclusively within their competences. Each federal state is to establish a body responsible for implementing the new provisions. Oversight of the law's implementation will rest with the Federal Office for Civil Protection and Disaster Relief (BBK), which will be empowered to impose fines ranging from €100,000 to €1 million in the event of violations.

The strengthening of critical infrastructure protection is driven not only by EU regulations but also by the growing number of attacks against such infrastructure. Until now, security issues have been regulated mainly through sector-specific legislation and IT security provisions. The new law introduces cross-sector regulations and strengthens the physical protection of key facilities.

Commentary

- **Since 2022, Germany has experienced a steady increase in the number of attacks on critical infrastructure, both physical and cyber.** There have been growing numbers of suspicious drone flights over military, energy, and transport facilities. According to the Federal Criminal Police Office (BKA), more than 1,000 such incidents were recorded last year alone. In addition, assessments by the BKA and the domestic intelligence service (BfV) indicate an increase in acts of sabotage that may be carried out by foreign states. In the first half of 2025, 143 such incidents were observed, including an arson attack at the port of Rostock, from which Ukrainian grain is exported. The number of cyber attacks has also continued to grow. According to data from the Federal Office for Information Security (BSI), more than 720 attacks were recorded between mid-2024 and mid-2025, compared with 490 in the preceding year. These attacks most often targeted the healthcare, energy, and transport sectors. The perpetrators are identified as common

criminals, political extremists, and state actors, primarily Russia, China, Iran, and North Korea.

- **The legislation has faced widespread criticism from experts, representatives of the sectors concerned, local authorities, and the opposition, who argue that it is insufficient in view of existing threats.** Critics point out that implementing regulations, which are intended to define specific minimum requirements for critical infrastructure operators, are not expected to be adopted until 2030, significantly delaying the law's full implementation. The legislation is also criticised for covering only the largest entities. Moreover, the adopted act does not take into account lessons from the January attack by left-wing extremists on Berlin's power grid (see '*Consequences of the Berlin blackout*'), including calls to prohibit the public disclosure of data on the precise location of energy and water networks. The government has announced an additional legislative initiative to this effect. Infrastructure operators have also highlighted the need to regulate the financing of protection measures, as the obligation currently rests solely with the entities concerned. Companies are calling for support, for example from the defence ministry's budget. A further challenge is the fragmentation of competences between federal and regional administrative authorities, which hampers effective coordination and the efficient protection of infrastructure.
- **The adopted regulations form part of a broader set of measures undertaken by Germany to strengthen protection against hybrid threats.** Drones are identified as a particular risk. In December last year, a dedicated Federal Police unit was established for this purpose (Drohnenabwehreinheit der Bundespolizei), and the Joint Drone Defence Centre (Gemeinsames Drohnenabwehrzentrum) was launched to coordinate the activities of the Federal Police, state police forces, and the Bundeswehr. Amendments to the Federal Police Act and to legislation on airspace security are under consideration, aimed at expanding the powers of the security services to counter drone-related threats (see '*Drones over Germany – plugging legislative and technical gaps*'). In addition, a Defence Centre against Hybrid Threats is being established within the Federal Chancellery.