Risks

Last updated on 20.11.2025

Table of contents

Infrastructure sabotage **3**

Infrastructure sabotage

Threat assessment: Deliberate sabotage of critical infrastructure within the next two years is unlikely, but incidents involving damage to undersea connections during this period are considered likely. It is therefore important to accelerate planning for their protection and to implement the necessary regulatory adjustments and additional protective mechanisms.

Since the continuation of Western support and assistance is the key precondition for Russia to subdue Ukraine, the Kremlin has decided to raise the stakes and has launched a deliberate sabotage campaign against Western states, including Estonia. According to Moscow's calculations, the campaign directed by Russian intelligence services is intended to sow fear and confusion and to push Western states decisively away from supporting Ukraine. Another direct goal of the Kremlin is to disrupt and break the supply chains for military and civilian support destined for Ukraine.

Throughout 2024, Europe witnessed arson attacks, acts of vandalism, sabotage, and attempted sabotage carried out under the instruction of Russia's military intelligence service, the GRU. Through hybrid operations, Russia is attempting to destabilize Europe and undermine collective resolve to support Ukraine.

Although it is unlikely that the Kremlin will be able to turn its ongoing sabotage campaign into success in its confrontation with Ukraine and the West, neither the Western political community nor the wider public can ignore Russia's intensified hostile activities. The risks of miscalculation and the inherently violent nature of the campaign carry too great a possibility of serious consequences, including civilian casualties. For this reason, it is critical for the West to develop adequate countermeasures to deter Moscow's covert freedom of action and prevent further escalation into even riskier hostile behaviour.

THREATS

- While most sabotage attempts remain unattributed and some turn out to be accidents, Western states have observed an increase in Russian sabotage attempts. According to the think tank CSIS, the number of Russian attacks nearly tripled between 2023 and 2024. In the case of undersea connections, a cable or pipeline is only one part of the whole system: vulnerable points also include the terrestrial landing sites and control systems. Both China and Russia have the capability to cut undersea cables quickly and cheaply, but so far deliberate sabotage has not been proven in investigations. Russia's shadow fleet consists of old vessels that under normal conditions would have been scrapped. Their crews are poorly trained, inexperienced, and often negligent. In addition

- to damaging infrastructure, the shadow fleet also poses the risk of potential environmental disasters.

- Damage to undersea cables in our waters will remain a possibility in the future. All Baltic Sea states are actively cooperating to monitor shipping and vessel activity, to respond quickly and decisively to possible incidents, to collect evidence of criminal intent, and to hold perpetrators accountable.

- As the aggressor, Russia has demonstrated that energy infrastructure is a target for attacks aimed at lowering societal resilience and morale. Cyberattacks are also a common component of such strategies. By hacking into network management systems used by private companies to control data traffic across cables, cyberattacks can significantly disrupt data flows.

- Operators of critical infrastructure must maintain and strengthen both physical and digital resilience. A significant number of employees working for providers of essential services still regularly travel to the Russian Federation, despite the Estonian state's recommendation to avoid this entirely.

ACTIONS

- On 8 February 2025, a historic step was taken to strengthen energy security – a cornerstone of economic security – when the Baltic states disconnected from the Russian and Belarusian electricity grid and successfully synchronized with the Continental European power system.

- Crisis preparedness must be maintained and constantly practiced, as the threat of hybrid attacks on infrastructure coordinated by the aggressor state continues to exist. Operators of critical infrastructure must preserve and enhance both physical and digital resilience.

- Essential service providers must plan for service continuity, assess risks, and prepare recovery plans. They are also required to check the criminal records of employees performing critical tasks. In addition, essential service providers are obliged to notify the competent authority responsible for essential services of any unplanned disruption, interruption, or threat to continuity.

- In addition to its usual activities, the Estonian Internal Security Service (KAPO) has worked with essential service providers to raise awareness of their vulnerabilities, including those related to supply chains, insufficient adherence to security standards, weak cyber hygiene, or insider threats posed by employees.

- The European Union and NATO have intensified cooperation on the protection of critical infrastructure, including undersea infrastructure, since the start of Russia's full-scale aggression against Ukraine. A NATO Maritime Centre for the Security of Critical Undersea Infrastructure has

- been established in the United Kingdom under NATO's Allied Maritime Command (MARCOM). NATO and the EU have also set up a joint working group on critical infrastructure resilience and other cooperation formats. As this area of cooperation is still relatively new, concrete capabilities will need to be developed over the coming years to make it fully operational.

Expand all

Read more

Annual Review 2024–2025 – Internal Security Service

International Security and Estonia 2025 – Foreign Intelligence Service

Last updated on 11.11.2025