

BALTIC SEA HYBRID THREATS

Since Russia’s full-scale invasion of Ukraine in 2022, the Baltic Sea region has become one of the main arenas of strategic competition between NATO allies and Russia. The region’s strategic importance, advanced digital infrastructure, dense energy and transportation networks, and proximity to Russia make it vulnerable to hybrid threats targeting critical infrastructure, democratic institutions, and societal resilience.

HYBRID WARFARE

Hybrid warfare is a **combination** of overt and covert activities designed to achieve **strategic objectives** below the threshold of conflict. These activities ranges from cyberattacks, influence operations, political and economic coercion, to active sabotage and overt military provocation, such as airspace violations.
Source: NATO

MAIN TOOLS OF HYBRID THREATS

CYBERATTACKS

Cyber operations target digital systems to disrupt services, steal information, or create strategic pressure. The **2007 cyberattacks against Estonia** demonstrated the potential impact of large-scale cyber disruption, as **vital government infrastructure** was rendered **offline for nearly two weeks**.

DISINFORMATION & INFLUENCE OPERATIONS

Disinformation campaigns aim to **manipulate** public opinion, **weaken trust** in institutions, **amplify** societal **divisions**, and influence political decision-making. These operations often exploit existing social tensions and target democratic processes.

CRITICAL INFRASTRUCTURE SABOTAGE

Energy networks, telecommunications systems, pipelines, railways, and undersea cables have become key targets due to their strategic importance. Recent incidents in the Baltic Sea, including damage to the Balticconnector gas pipeline and telecommunications cables in 2023 and the Estlink 2 electricity cable in 2024, have highlighted **vulnerabilities** in underwater **infrastructure** and raised concerns about **maritime security**.

ECONOMIC COERCION

Economic pressure is used to **influence** state **behavior** by **exploiting dependencies** in areas such as energy, trade, or supply chains. Russia’s use of energy exports as political leverage in Europe is a prominent example.

BORDER & AIRSPACE VIOLATIONS

Violations of territorial borders, airspace, and maritime boundaries can be used as tools of **intimidation**, **testing responses**, and **creating uncertainty** among targeted states. Examples include repeated Russian military aircraft activities near NATO airspace and the use of migration as a tool of political pressure. In 2021, Belarus facilitated the movement of migrants toward the EU’s eastern borders, creating a security crisis for Poland, Lithuania, and Latvia.

FROM ENIGMATIC ACTIONS TO BRAZEN PROVOCATIONS?

Timeline 2022-26: Major Trends

February 2022

RUSSIAN GPS JAMMING

Following the February invasion of 2022, Russia increased GPS signal jamming across the Baltic Sea. The disruptions affected civilian aviation, maritime navigation, and military activities, particularly in areas close to Russia’s borders. Electronic interference became an increasingly visible tool of pressure and disruption in the region.

UNDERSEA INFRASTRUCTRE SABOTAGE

From autumn 2023 onward, a series of incidents affecting critical undersea infrastructure increased concerns about sabotage in the Baltic Sea region. Damaged pipelines and telecommunications cables highlighted vulnerabilities in the infrastructure connecting Nordic and Baltic countries to European energy and communication networks.

Fall 2023-2025

Spring 2025

AGGRESSIVE CYBERATTACKS

Russian hacker groups, often connected to Russian intelligence services were noted to shift from Denial-of-Service attacks (DDoS) to more sophisticated and destructive cyberattacks through infiltration and malware.

12 MINUTE AIRSPACE VIOLATION

Three Russian MiG-31 fighter jets flew over Estonian airspace for approximately twelve minutes, shortly after the conclusion of the Zapad-2025 exercise. Estonia requested NATO consultations under Article 4, highlighting concerns over assertive Russian military behavior and the potential use of conventional forces alongside hybrid pressure.

September 2025

August 2026

EUROPE-WIDE SABOTAGE CAMPAIGN

August 2026 saw numerous sabotage attempts targeting locations vital to Europe’s defense industrial sector and its support for Ukraine, including Leipzig Airport and railways spread across Europe.

THREAT OVERVIEW

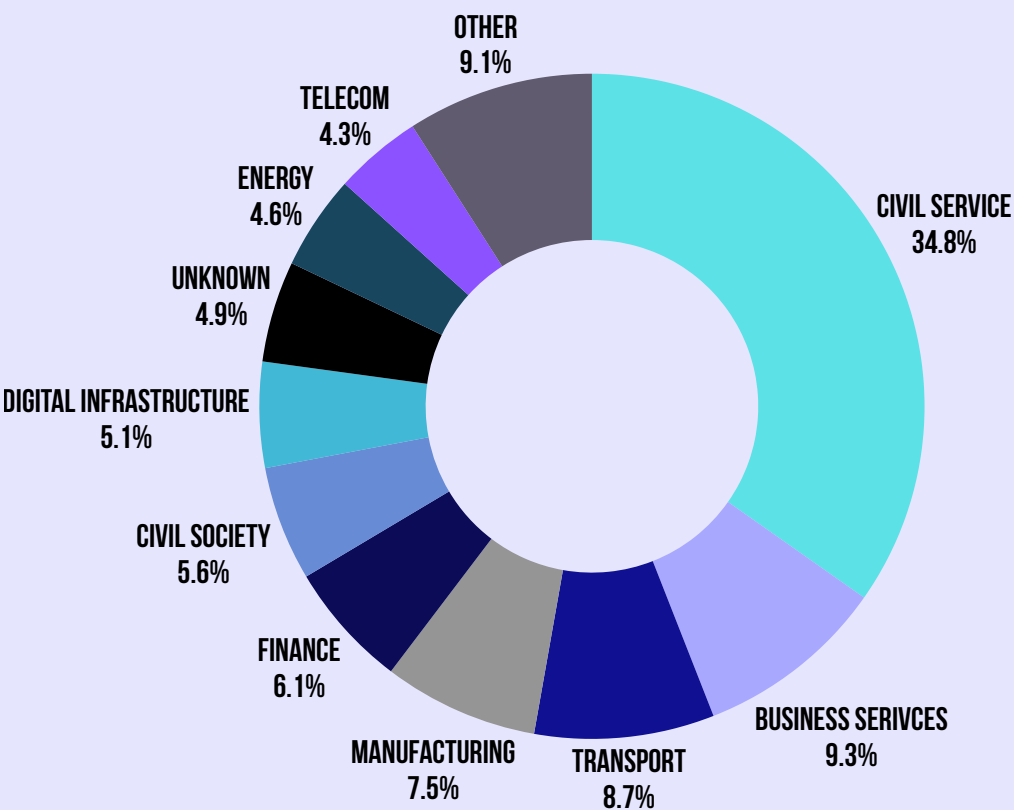
The Baltic Sea region is one of Europe’s most economically significant maritime regions. The combined nominal GDP of the NB8 countries exceeded \$2.21 trillion in 2025. Its extensive land- and sea-based infrastructure supports trade, energy, transportation, and communications, but also presents a wide range of potential targets for adversaries seeking to inflict political, military, and economic harm on NATO allies through acts of sabotage.

Source: World Bank: World Development Indicators

CYBER THREATS

The high rate of **digitalization** among countries of the Baltic Sea region has made government more effective. However, it has also made **cyber operations** the main way to **disrupt government functions** and daily life for ordinary citizens as vital online services are disrupted.

OVERVIEW OF EUROPEAN SECTORS TARGETED BY CYBERATTACKS



SOURCE: ENISA THREAT LANDSCAPE 2026

INFRASTRUCTURE SABOTAGE

Sabotage against critical infrastructure have become an ongoing threat for the wider Baltic Sea region due to the extensive damage they can cause. Suspected Russian sabotage attacks are estimated to have caused hundreds of millions of euros in physical damage across Europe in 2022-25.

In recent months, critical infrastructure attacks have become widespread in the region.

Source: S&P Global, Sascha Ostanina, 2025

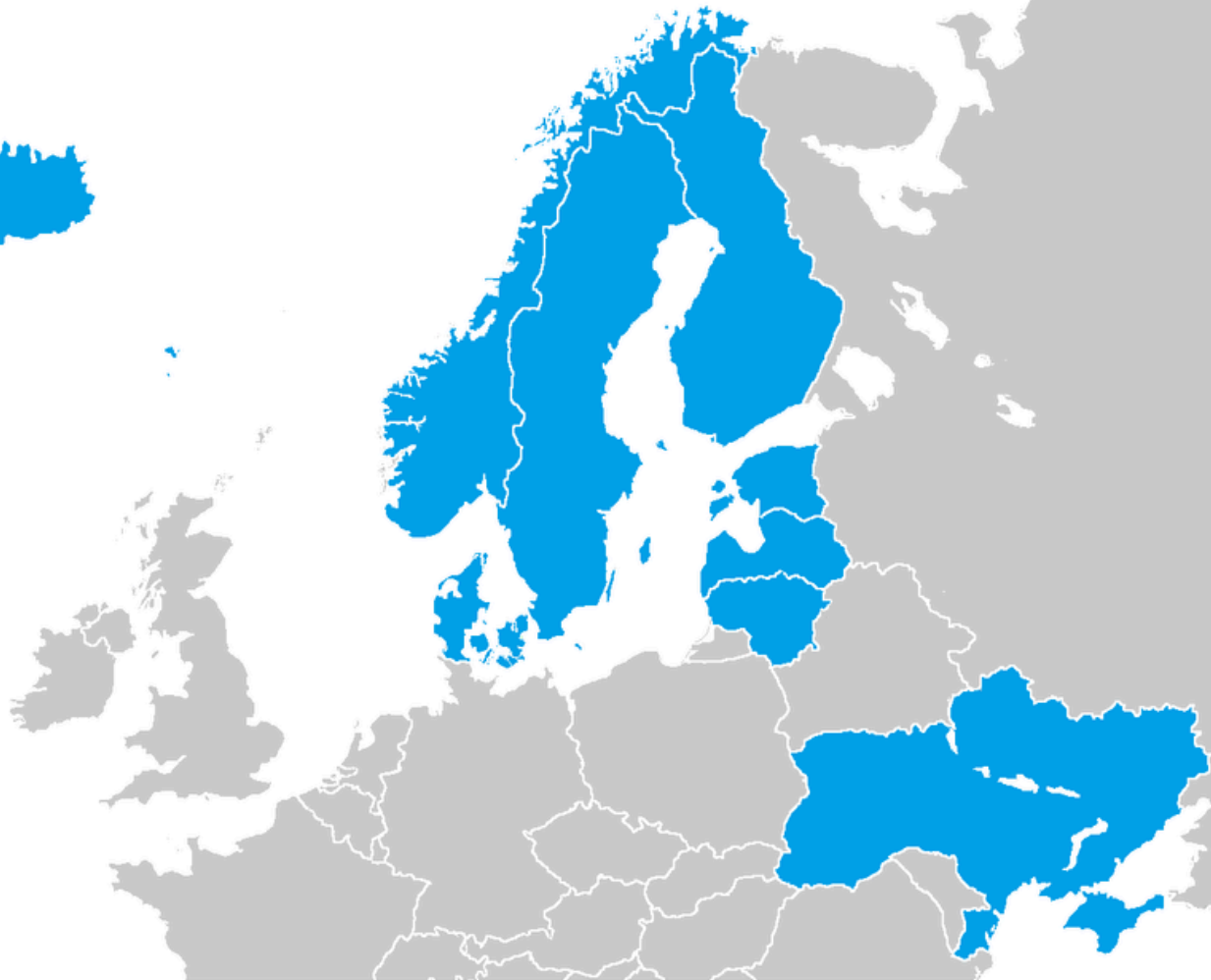
MARITIME SECURITY

Maritime trade remains an important pillar of the economy of the Baltic Sea region, with +2,000 ships navigating the sea at any given second. This includes Russia who uses the Baltic sea as its main region for the export of hydrocarbons through its shadow fleet, and maintains a large naval presence in the region.

The Increased risk of deliberate sabotage or environmental disasters occuring has become a regional issue for the NB8.



Image Credit: GN.Studio, Shutterstock.com



REGIONAL RESPONSES

In response to sustained hybrid attacks, the NB8 countries have developed comprehensive **Whole-of-Society** security frameworks to strengthen preparedness, innovation, and resilience against hybrid threats.

These measures include establishing ministries and other dedicated institutions responsible for enhancing societal preparedness, as well as monitoring and countering active influence operations.

