IISS

The Scale of Russian Sabotage Operations on Europe

Charlie Edwards
Senior Fellow for Strategy and National Security

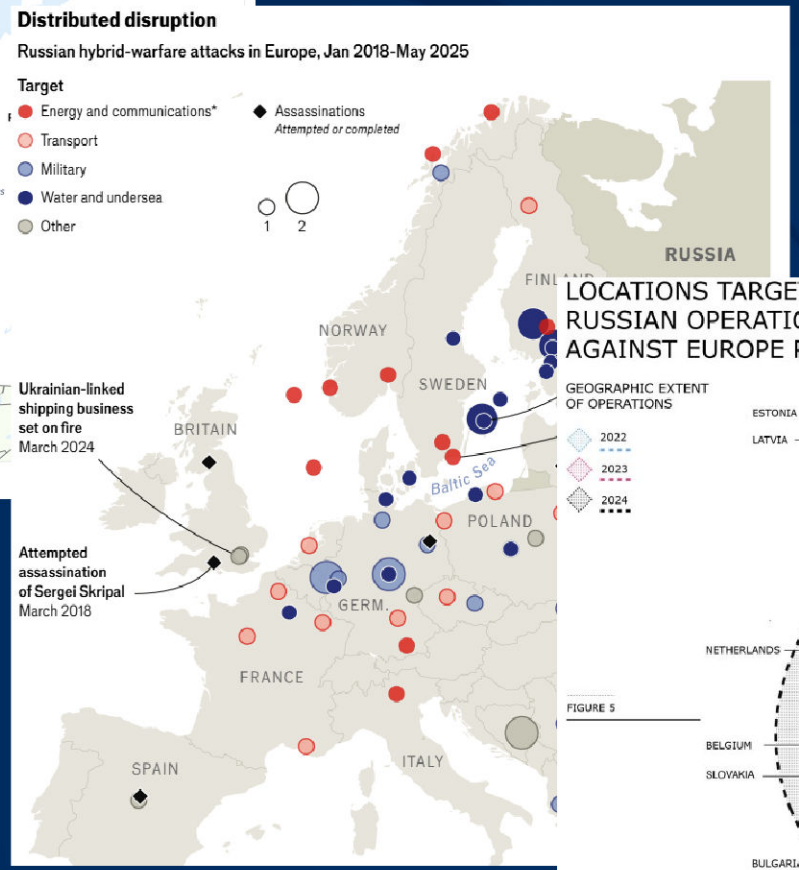
Europe is experiencing the most intense era of sabotage since the Cold War

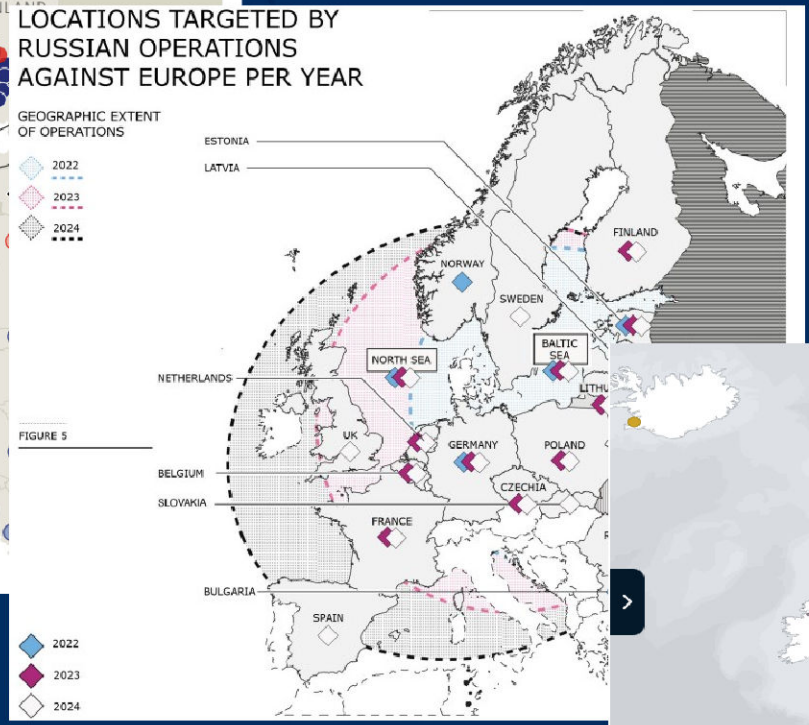
Sabotage: 'Activity conducted for, on behalf of, or for the benefit of a foreign power, resulting in **damage to property, sites and data affecting a country's interests**, and national security. This can be done through, but is not limited to, the use of cyber actions and **physical damage**.'

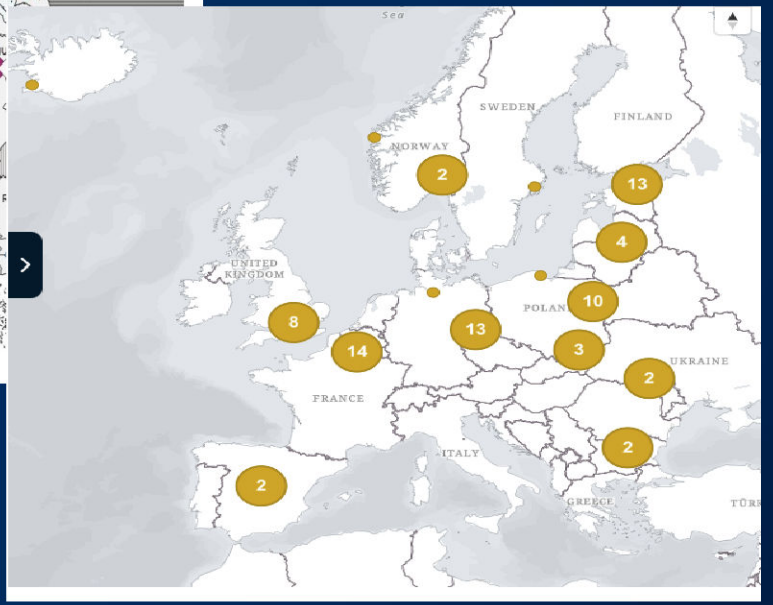
(UK definition but no European definition of sabotage or CNI exists).

Ukraine sabotage on a Russian railway roughly 100 miles southeast of Moscow (November 2023)

Russian sabotage on a French railway 150km to the south-west of Paris (July 2024)







ACLED *The Economist* *Leiden University* *AP News*

Russia's unconventional war on Europe

- **Focus on CNI:** Communications, energy, government, health, industry, military, transport, undersea cables, water;
- **MO** (arson, explosives, anchor-drag, vandalism, UAV ISR, electronic attack, assassination/attempt, weaponised migration).
- **Plausible Deniability:** actor/method/sponsorship Almost certain / Highly likely / Likely / Realistic possibility
- We used **multi-source corroboration.** Treating actions by third-country nationals or contractors as state-linked when there is evidence of tasking, financing, logistics, or alignment with RIS campaigns.
- Example: *PM Tusk in May 2024: 'It is likely that Russia was involved' and PM Tusk in May 2025: 'Poland knows for sure Russia was involved'*

European critical infrastructure is vulnerable

- **Aging infrastructure and lack of investment:** 60% of the EU's total grid investment must be directed toward basic distribution grid upgrades.
- **Europe's rail** still relies on GSM-R (2G) and is only now migrating to FRMCS (4G/5G), requiring years of risky co-existence
- **Hospitals** run long-lived clinical systems/medical devices that can't easily be patched or replaced
- **Legacy and compromised digital systems:** Lithuania continues to use Russia's KLUB-U railway locomotive control system.
- **Vulnerability of naval and water systems:** The Netherlands' hydraulic water management, for example, has been found to be seriously outdated, relying on old computer systems connected to digital networks
- **Seabed & offshore assets are exposed and hard to defend:** Russian vessels and "research" ships have repeatedly surveyed this infrastructure.
- **Detection & attribution gaps create a deterrence problem:** Governments still struggle to attribute beyond reasonable doubt. NATO and the EU have set up coordination cells but legal constraints (eg: in international waters persist).
- **Repair capacity and spares are limited so outages last:** Europe has limited sovereign cable-repair capacity and very few specialised ships worldwide.
- **RIS repeatedly target energy operators' IT/OpTech:** eg: the cloud/identity layer used by those operators.
- **Uneven regulation & fragmented governance across borders:** NIS2 and the CER Directive raise the bar, but transposition/implementation is patchy.

Key points

- Russia's summer offensive failed.
- NATO 2035 and the 5%: The Kremlin can prevail only by stopping European capitals turn latent strength into usable superiority and by sapping their resolve.
- The Kremlin's aim is to impose costs, disrupt resilience, and erode support for Ukraine via sabotage, espionage, and covert action.
- Sabotage activity surged post-2022 and keeps testing European thresholds below open war.
- Confirmed sabotage of critical infrastructure **almost quadrupled from 2023 to 2024**; continued incidents into 2025 including drones, explosive devices, and targeting of CNI (rail network).

War in Ukraine + Add to myFT

Russian hackers target Polish hospitals and city water supply

Warsaw increases cyber security budget as Moscow makes up to 50 sabotage attempts a day, says minister

Polish hospitals have been targeted by Russian hackers, leading to operations being suspended and data stolen © Getty Images

Raphael Minder in Warsaw

Published SEP 16 2025

102

Proxies, low-tech, and deniability

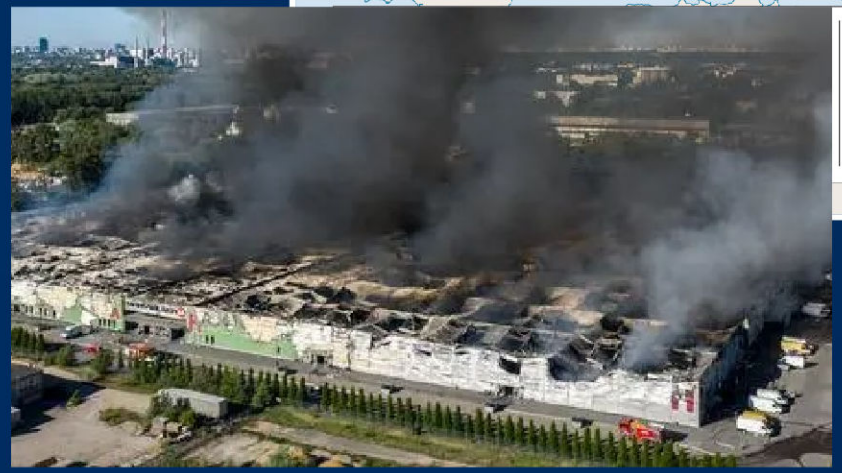
- **After mass expulsions (~ 400 RIS in 2022):** GRU shift to a "**gig-economy**" model—remote tasking of third-country nationals via Telegram

Proxies, low-tech, and deniability

- **After mass expulsions (~ 400 RIS in 2022):** GRU shift to a "**gig-economy**" model—remote tasking of third-country nationals via Telegram
- **GRU Unit 29155** leads physical ops; mix of arson, vandalism, and simple sabotage against single points of failure in ECI

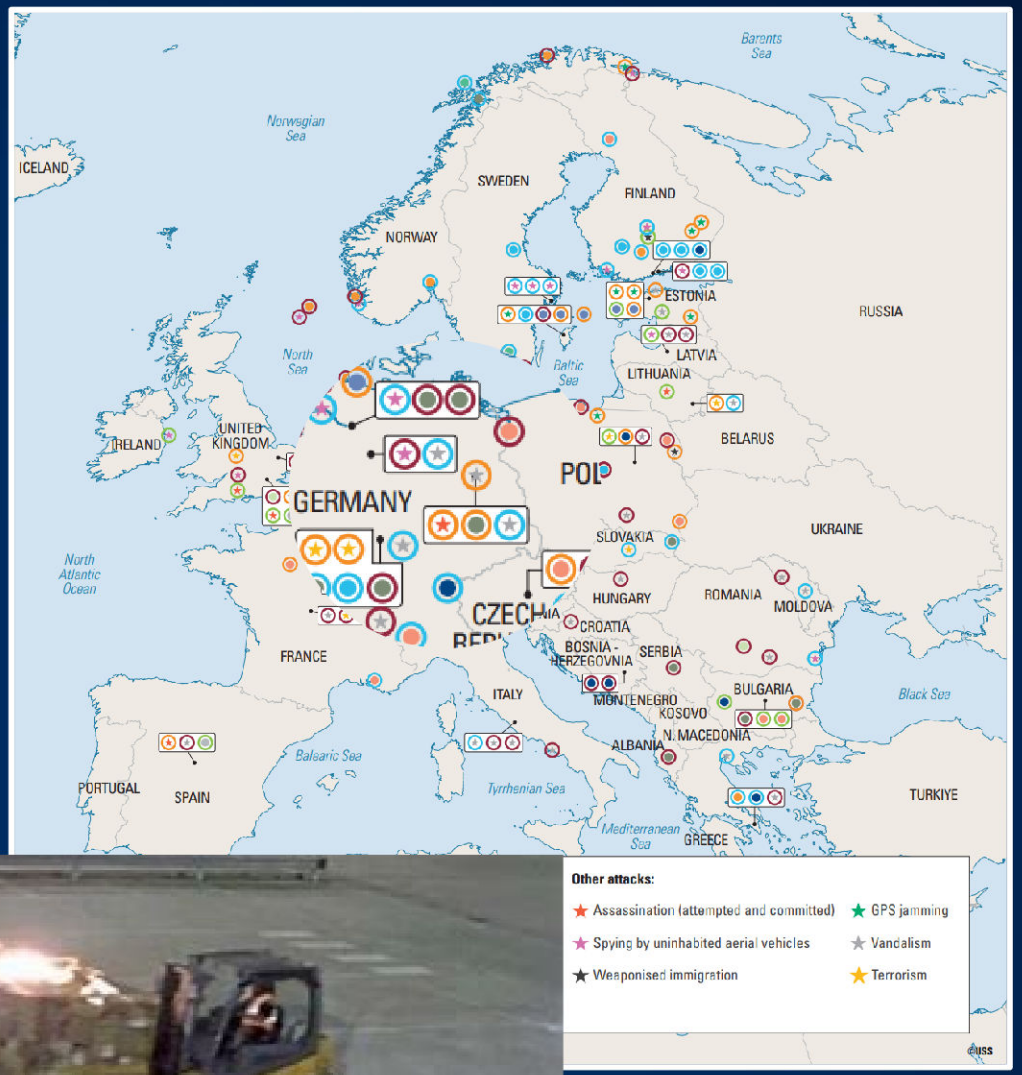
Proxies, low-tech, and deniability

- **After mass expulsions (~ 400 RIS in 2022):** shift to a "**gig-economy**" model—remote tasking of third-country nationals via Telegram
- **GRU Unit 29155** leads physical ops; mix of arson, vandalism, and simple sabotage against single points of failure
  - 12 May 2024: Arson attack on Marywilska 44 shopping centre
  - Terrorism: DHL "massager-bomb" tests



Proxies, low-tech, and deniability

- **After mass expulsions (~ 400 RIS in 2022):** shift to a "**gig-economy**" model—remote tasking of third-country nationals via Telegram
- **GRU Unit 29155** leads physical ops; mix of arson, vandalism, and simple sabotage against single points of failure
  - Arson: 'Marywilska shopping centre'
  - 22nd July 2024: DHL "massager-bomb" tests at logistics hubs



Proxies, low-tech, and deniability

- **After mass expulsions (~ 400 RIS in 2022):** shift to a "**gig-economy**" model—remote tasking of third-country nationals via Telegram
- **GRU Unit 29155** leads physical ops; mix of arson, vandalism, and simple sabotage against single points of failure
  - Arson: 'Marywilska shopping centre'
  - Terrorism: DHL "massager-bomb" tests at logistics hubs
  - 25th December 2024: Anchor-dragging damaging Baltic cables (Eagle S)

Thank you