RUSSIA'S HYBRID WAR: THE NORTHERN FRONT

Editors: Minna Ålander and Patrik Oksanen
Authors: Dr. Ieva Bērziņa, Karen-Anna Eggen, Bjarni Bragi Kjartansson, Marek Kohv, Dr. Aleksander Olech, Adam Roževič, Dr. Jeanette Serritzlev and Dr. Frank Umbach

Contents

ISBN: 978-91-988500-3-1
Publisher: Frivärld, 2025

Foreword from Konrad-Adenauer-Stiftung

Christine Leuchtenmüller, Resident Representative to the Nordic Countries

The Nordics—Denmark (including Greenland and the Faroe Islands), Finland, Iceland, Norway and Sweden—are playing a prominent role in security policy, both in the Arctic and the Baltic Sea region. Together with the Baltic states—Estonia, Latvia and Lithuania— they are pivotal actors in multilateral cooperation and in shaping Europe's peace and security architecture. For Germany, these countries are indispensable strategic partners.

The Konrad-Adenauer-Stiftung, through its Office for the Baltic States based in Riga and its Regional Programme for the Nordic Countries based in Stockholm, closely observes security developments in the region. This study seeks to contribute to a greater understanding of the growing challenges and risks arising from Russian hybrid aggression.

Our aim is to make these findings accessible to a wide audience and to raise awareness of the destabilising impact of hybrid warfare, which fosters not only societal uncertainty but also erodes the foundations of liberal democracy. Russia's hybrid tactics are designed to erode trust in democratic processes, media, and governance partly by exploiting democratic rights and strengths such as openness, pluralism, and legal protections for speech and association.

This publication has been produced in cooperation with Stockholm Free World Forum (Frivärld). We extend our sincere thanks for their constructive collaboration and to all contributing authors for their dedication to this project.

Stockholm, August 2025

A Letter from the Shadow War's Northern Front

Patrik Oksanen and Minna Ålander

> "Sweden is not at war, but there is no peace either."[1]

When Prime Minister Ulf Kristersson held his speech at Sweden's largest annual security conference in Sälen, it was a clear acknowledgement of the situation in 2025. Spoken not from the battlefield, but from an idyllic ski resort bordering Norway, these words capture the unsettling reality facing NATO and the EU's northern front.

> "Real peace means freedom and no serious conflicts between countries," the prime minister continued. "We and our neighbouring countries are subjected to hybrid attacks that are not carried out with missiles and soldiers but with computers, money, disinformation, and threats of sabotage."[2]

Seen from Northern European capitals, the view is clear: We are not at peace. The battle is real and far more dangerous than the broader public has grasped. Engineered ambiguity has allowed Russia to strike while denying responsibility. To escalate while avoiding retaliation and to place itself in a favorable position should the Kremlin choose to wage a conventional war. The weapon of choice is what we in the West have called hybrid warfare, targeting our institutions, our infrastructure, our alliances, and our minds.

In this war, there are no frontlines. Attack vectors shift by the day, exploiting weaknesses, vulnerabilities, and opportunities. To provide an overview of how this war is waged, each chapter in this book will cover various examples from the Baltic Sea and Nordic region, written by experts from each country:

- **Denmark**: Cyberattacks against airports, railways and hospitals. Anonymous Sudan claims credit, but were they really Sudanese and so anonymous?
- **Estonia**: The interior minister's car is smashed, only one incident of several in the Baltics where Russian intelligence recruits petty criminals to sow fear.

- **Finland**: A suspicious amount of real estate in strategic areas is owned by Russians. Finland moves to legally prevent Russian nationals from buying property.
- **Germany**: With pipelines and cables regularly damaged in the Baltic Sea, a giant that overslept awakens to a reality it can no longer ignore.
- **Iceland**: Typically outside Russia's crosshairs, the European Council's meeting in Reykjavik draws public institutions under fire from cyberattacks.
- **Latvia**: Two Russian comedians prank call a staggering number of Latvian and Western leaders, receiving a state medal for their efforts.
- **Lithuania**: The "gig-economy of sabotage" and efforts to reshape Lithuania's historical memory and national identity sow societal discord.
- **Norway**: The Svalbard archipelago and northern mainland Norway have witnessed several Russian paramilitary incidents, accompanied by disinformation campaigns and challenges to Norway's sovereignty over Svalbard.
- **Poland**: A primary conduit for aid to Ukraine, Russia has unleashed an onslaught of sabotage attempts, assaults, and other hostile actions, but the hybrid siege of Poland pre-dates Russia's wars against its neighbors.
- **Sweden**: A "dual-use" Russian Orthodox Church, financed by Russia's State Atomic Energy Corporation Rosatom, is built by a strategic airport and the priest receives a medal from the Russian Foreign Intelligence Service (SRV).

These are not isolated incidents. When a strategy works well, Russia adapts it to a new context for reuse. The incidents are meant to test our resilience, measure our response, exploit our openness, and try to exhaust our capacity and will to resist—and our will to support Ukraine.

The Foreign Minister of Czechia, Jan Lipavsky told reporters in the spring of 2025 that there were "500 suspicious incidents in Europe last year, 100 of which were attributed to the Russian Federation." These activities were described as continuing and intensifying.[3] A group of public service journalists within the European Broadcasting Union looked at some 80 incidents in Europe since the beginning of 2024: In more than 60 cases, Russian links were suspected or confirmed.[4]

These numbers underline the key element of hybrid warfare, plausible deniability: the uncertainty about the perpetrator and suspicions of a hostile actor

when there is none. Both cases benefit Russia. Hybrid attacks are intensifying as a resurgent ideology of the Russian Empire is challenging a Europe built on the rule of law and sovereign states, with the number of hybrid attacks tripling between 2023 and 2024 alone.[5] Russia has targeted transportation, government, critical infrastructure, and industry, and the weapons have included explosives.

More is likely to come. Europe is now in a situation that could be described as total psychological war. There are no limits or restraint to Russia's behavior, so long as it stays under the threshold of armed conflict and NATO's article 5.[6] Russia will only stop once we make it.

Resilience is necessary—but not sufficient—to win the hybrid war. To establish deterrence, we must demonstrate both the capability and the will to impose significant costs on the adversary. The Northern Flank offers a potential blueprint for hybrid deterrence: countries in the region are already investing in national capabilities and enhancing cross-border cooperation to detect and respond to hybrid threats.

Stockholm, September 2025

References

1 The Local, "Sweden 'not at war, but not at peace either', says PM," *The Local*, January 12, 2025, https://www.thelocal.se/20250112/sweden-not-at-war-but-not-at-peace-either-says-pm.

2 Ibid.

3 Matīss Arnicāns, "Journalists track Russia's hybrid hooliganism across Europe," *Latvian Public Media*, March 12, 2025, https://eng.lsm.lv/article/society/crime/12.03.2025-journalists-track-russias-hybrid-hooliganism-across-europe.a591301/.

4 Eurovision News, "Playing With Fire: Are Russia's hybrid attacks the new European war?" *Eurovision News*, March 12, 2025, https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/.

5 Seth G. Jones, "Russia's Shadow War Against the West," *Center for Strategic and International Studies*, March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west.

6 Patrik Oksanen, *Rysslands hemliga krig mot Sverige* (Volante, 2025). P. 30.

Introduction: Tracking Russia's Hybrid Warfare

By Patrik Oksanen, Minna Ålander

Russia's 2014 illegal annexation of Crimea and war in eastern Ukraine sparked substantial debate on hybrid activities as part of Russian thinking about and approach to modern warfare. A key notion was the idea echoing ancient military thinkers like Sun Tzu, that the supreme art of war is to subdue the enemy without fighting.[1] Although Russia has fought a kinetic war against Ukraine since 2014, its wider hybrid war against the West involves tactics that resemble Sun Tzu's strategic thinking.

The European Centre of Excellence for Countering Hybrid Threats defines hybrid threats as "harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined."[2] These activities are conducted with the aim to serve strategic objectives and are usually deliberately kept below the threshold of armed conflict in order to, in Russia's case, avoid activating (but preferably undermining) NATO's Article 5.[3] As made evident by the collection of cases investigated in this book, the activities are part of a comprehensive approach to malign influence—economic, legal, diplomatic, information, religious, military, intelligence, and other tools are used if deemed effective.

The aim of this book is twofold. The first is to provide a comprehensive overview of the sub-threshold, or hybrid, activity in Northern Europe. The second is to categorize the examples of Russian activity to help academics and practitioners alike better understand the scope and scale of Russian approaches. Examining the region as a whole is of importance as Russian military exercises indicate that Russia views the High North and the Baltic Sea region as one continuous area.[4] Scholarly and news articles from the region also point to increased Russian activity, especially after 2014.[5]

In May 2024, NATO stated that it was deeply concerned about recent Russian hybrid attacks affecting half a dozen member states, among them Estonia,

Latvia and Lithuania: "These incidents are part of an intensifying campaign of activities which Russia continues to carry out across the Euro-Atlantic area, including on Alliance territory and through proxies. This includes sabotage, acts of violence, cyber and electronic interference, disinformation campaigns, and other hybrid operations."[6]

A couple of days later, the Financial Times cited several European intelligence services collectively warning of Russian preparation and planning for sabotage and other attacks on European soil.[7] The Swedish Prime Minister Ulf Kristersson confirmed that Swedish intelligence shared this threat assessment, as did the head of Finland's secret and intelligence service (SUPO).[8]

The nature of Russian hybrid activity, utilising the realms below the threshold of armed conflict, has created ambiguity and uncertainty over how to respond to such attacks. Part of the challenge lies in the inherent difficulty of attributing hybrid attacks, but also the lack of Western willingness to name perpetrators—either to avoid revealing intelligence capabilities to Russia or out of concern that attribution might "provoke" a response and escalate tensions—or a combination thereof.

But even if such attributions can be made with confidence, the next question is how to calibrate a response; democratic countries that value the rule of law cannot resort to illegal or grey zone methods. This creates a discrepancy in what tools are available to the target country and the adversary, with the latter enjoying freedom of manoeuvre with impunity or few consequences, and the former being left with ineffective responses.

Hybrid Tools: A Preliminary Overview

In this book, we identify two main categories of tools: *non-military* and *military*. Each category is further divided into two subcategories. Non-military tools are divided into *non-physical* and *physical*, while military tools are divided into *conventional* and *nuclear* (or other weapons of mass destruction, WMDs). The typology is designed to provide a pedagogical framework for illustrating and describing different hybrid cases and the variety of tools employed in hybrid activities.

Non-military		Military	
Non-physical	Physical	Conventional	Nuclear (or other WMDs)
Hostile information*	Real estate	GPS-jamming/EW	Indirect threat of nuclear weapons
Diplomacy	Strategic location	NOTAMS	Direct threat
Official statement	Coercive migration	Cyber attack (military target)	Exercise
Cyber attack (civilian target)	Critical infrastructure	Blockade	Deployment
Harassment (non physical)	Harassment/ assault (physical)	Violation of sea territory	Space
History / memory	Abduction, detainment and/or disappearance	Violation of land territory	Other
Compatriots	Assassination	Violation of airspace	
Religion	Vandalism / sabotage	Exercise	
Front organisation	Nuclear** or other WMDs	New military structure	
Espionage	Criminals / mercenaries / private contractors***	Mercenaries / private contractors / paramilitary	
Economic fraud / money laundering	Incident in the air / close flying	Incident in the air /close flying	
Infiltration / influence or take over 3rd party	Incident on the sea / close manoeuvring	Incident on the sea / close manoeuvring	
Corruption	Space	Mobilisation	
IP theft	Other	Sabotage	
Sanctions/Economic coercion		Kinetic military violence	
Democratic Institution		Special military operation	
Deception (including deepfake)		Space	
Lawfare		Other	
Other			

** Hostile information covers disinformation and propaganda. These are distinct but related categories. The former can be information that is outright false or partly true, but taken out of context or proportion to do harm. The latter share similar traits but are used to amplify messages, often to the benefit of Russia. This may take place in traditional, digital and social media.*

*** Nuclear here includes activities that could for example be drones over nuclear power plants, Russian nuclear producer and atomic energy company Rosatom or other non military means that could be associated with nuclear activities.*

**** May also be MC-clubs, fight clubs, cyber criminals.*

Northern Europe: The Baltic Sea and Arctic in a Strategic Context

NATO's northern flank is more of a hot spot now than it was during the Cold War. The reasons are many, and the inclusion of Finland and Sweden in NATO marked a major security policy turning point for the region.

Russian imperialism views many of its neighbouring countries as part of the Russian world, or at least within its sphere of interest, especially the Baltic States. In order to succeed in its endeavour to re-establish the empire, Russia needs NATO and the EU to fail in defending the countries in the region. To achieve this, and to avoid a direct confrontation with NATO, hybrid tools are of great value for Russia, for example by delaying decision-making processes and achieving reflexive control over Western decision-makers through fuelling fears of escalation.[9] The Kremlin views the West as an enemy seeking to keep Russia weak and aiming to topple Putin's regime. This perception has fostered a hyperfocus on securing the domestic information environment, casting the West as an enemy to galvanize patriotism and maintain internal cohesion as Russian losses in Ukraine mount. On the flip side, it has created an active, all-encompassing Kremlin-led system set on imposing its will upon Russia's self-proclaimed sphere of influence in particular, but also conducting intimidation and influence operations abroad in general. In Russian zero-sum thinking, Russian loss of influence is someone else's (often Western) gain.

The Arctic has been called a "zone of national and strategic interest" by Russian officials.[10] Climate change is opening up previously year-round frozen sea lanes and brings with it new opportunities for exploitation of natural resources. Russia claims control over the Northern Sea Route (NSR) to use it exclusively for its energy exports to Asia, as Western markets are now largely closed due to sanctions (apart from gas and LNG, which are only to be phased out by 2027).[11] [12] China has ambitions in the region too and shows an increasing interest in the NSR.[13]

To assert its interests in the Arctic, Russia has also heavily militarized parts of the region, including the harbors that serve its strategic submarines—crucial to its nuclear second-strike capability—in the Northern Fleet Military District on the Kola Peninsula. What happens in the Arctic has consequences in the Baltic Sea and vice versa. Therefore, the whole region, including the European parts of the Arctic, must be viewed from a strategically holistic perspective.

Four Legally Vulnerable Islands

The Nordic-Baltic region has a unique geography with strategically important islands, two with special legal status: Faroe Islands and Greenland (Denmark), Svalbard (Norway), and Åland (Finland). This creates vulnerabilities that could be exploited by malign actors. In its annual report in 2023, the Danish security police (PET) drew attention to the threat against the self-governed islands of Greenland and Faroe Islands from Russia (and China) and the "interest in information that could be used for influence activities such as potential internal disagreements within the Danish Realm."[14] The Trump administration, with concerning statements about Greenland, could arguably be added to this list of actors using information operations against Denmark. Svalbard is Norwegian but regulated under the Svalbard Treaty with all signatory states having the right to pursue economic activities in the archipelago. Of the 46 parties of the treaty, Russia is the only foreign signatory currently present in Svalbard, operating a coal mine in Barentsburg since 1932. China has a research station on the island, established in 2004. The Åland islands are an autonomous part of Finland and, under the Åland convention from 1856 and 1921, demilitarised in peacetime but also neutral in wartime, with a responsibility for Finland to defend the neutrality of the islands.[15]

References

1 Sun Tzu was an ancient Chinese military strategist and philosopher who wrote *The Art of War*, a seminal text on military tactics and strategy. He lived in the 5th century B.C. in China, a time of significant military conflict and political turmoil. His teachings stress the importance of intelligence, strategic planning, and adaptability in warfare.

2 The European Centre of Excellence for Countering Hybrid Threats, "Frequently Asked Questions on Hybrid Threats" (Helsinki, 2024), https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf.

3 NATO, "The North Atlantic Treaty," *NATO Newsroom*, April 4, 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

4 Etterretningstjenesten, "Focus 2024: Russia's Permanent Break with the West" (Oslo, 2024), https://www.etterretningstjenesten.no/publikasjoner/focus/Focus24_contents/Focus24_chapter_2.

5 Karen-Anna Eggen, "Russia's Strategy towards the Nordic Region: Tracing Continuity and Change," *Journal of Strategic Studies* 45, no. 3 (2021): 1–42, https://doi.org/10.1080/01402390.2021.1873781; Ivo Juurvee et al., "Russia's Footprint in the Nordic-Baltic Information Environment 2019/2020" (Riga: NATO Strategic Communications Centre of Excellence, 2020), https://stratcomcoe.org/publications/russias-footprint-in-the-nordic-baltic-information-environment-20192020/24.

6 NATO, "Statement by the North Atlantic Council on Recent Russian Hybrid Activities," *NATO Newsroom*, May 2, 2024, https://www.nato.int/cps/en/natohq/official_texts_225230.htm#:~:text=These%20incidents%20are%20part%20of,campaigns%2C%20and%20other%20hybrid%20operations.

7 Sam Jones, John Paul Rathbone, and Richard Milne, "Russia Plotting Sabotage across Europe, Intelligence Agencies Warn," *Financial Times*, May 5, 2024, https://www.ft.com/content/c88509f9-c9bd-46f4-8a5c-9b2bdd3c3dd3.

8 Patrik Dahlin, "Kristersson: Uppgifter Om Ryska Angrepp Är Korrekta," *Omni*, May 5, 2024, https://omni.se/kristersson-uppgifterna-om-ryska-angrepp-ar-korrekta/a/jQP5KA.; Samuli Niinivuo, "Suojelupoliisi: Sabotaasin Uhka on Tiedossa, Eikä Venäjä Välitä Tekojensa Seurauksista," *Helsingin Sanomat*, May 5, 2024, https://www.hs.fi/maailma/art-2000010405744.html. Among earlier confirmed Russian sabotage are the blowing up of two munitions depots in the Czech republic in 2014.

9 A simple definition of reflexive control is manipulating an opponent to one's advantage. For a more detailed introduction to the Russian concept, see: Timothy L. Thomas, "Russian Military Thought: Concepts and Elements" (The MITRE Corporation, August 2019), Chapter 4, p. 1-11, https://www.mitre.org/sites/default/files/2021-11/prs-19-1004-russian-military-thought-concepts-elements.pdf.

10 Mikhail Komin & Joanna Hosa, "The bear beneath the ice: Russia's Arctic Ambitions," *European Council on Foreign Relations*, May 27, 2025, https://ecfr.eu/publication/the-bear-beneath-the-ice-russias-ambitions-in-the-arctic/.

11 European Commission, "Commission proposes a plan to phase out Russian gas and oil imports", June 17, 2025, https://commission.europa.eu/news-and-media/news/commission-proposes-plan-phase-out-russian-gas-and-oil-imports-2025-06-17_en.

12 Trym Eiterjord, "Amid Ukraine War, Russia's Northern Sea Route Turns East," *The Diplomat*, December 13, 2022, https://thediplomat.com/2022/12/amid-ukraine-war-russias-northern-sea-route-turns-east/.

13 Malte Humpert, "China Pushes Northern Sea Route Transit Cargo to New Record," *High North News*, December 18, 2023, https://www.highnorthnews.com/en/china-pushes-northern-sea-route-transit-cargo-new-record.

14 Politiets Efterretningstjeneste, "Assessment of the Espionage Threat to Denmark, the Faroe Islands and Greenland," May, 2023, https://pet.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vurdering-af-spionagetruslen-mod-danmark-2023_uk_web.pdf.

15 Ministry for Foreign Affairs of Finland, "Government Report on Changes in the Security Environment" (Helsinki: Finnish Government, 2022), https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164002/VN_2022_20.pdf.

Nordic and Baltic Sea Region: Everyday Intimidation and Interference

Patrik Oksanen and Minna Ålander

Incident on the sea / close manoeuvring (non-military)

Incident in the air / close manoeuvring (military)

Violation of airspace

GPS jamming (GPS-jamming/EW)

Lawfare

In the Nordic and Baltic Sea region, Russian hybrid activities often take place in international airspace and waters, but can also occur on sovereign territory or in maritime exclusive economic zones.

Increased GPS jamming of maritime and aerial traffic in the Baltic Sea has attracted substantial international media attention.[1] In March 2024, for example, Finnair announced a new destination: Tartu, Estonia. The new route was initially short-lived. Two Finnair flights had to turn back to Helsinki airport, unable to land at Tartu airport due to extensive GPS jamming in the Gulf of Finland.[2] As a consequence, Finnair suspended flights[3] until the Estonian Air Navigation Services were able to solve the problem by installing an alternative to GPS navigation, the distance measuring equipment solution (DME).[4]

However, GPS jamming is far from a new phenomenon, nor is it restricted to the Baltic Sea. In 2018, the Fintraffic Air Navigation Services gave out a warning due to large-scale GPS jamming in Finnish Lapland, reaching all the way to Norway's Arctic coast.[5] In 2019, Norway said it had electronic proof that Russia was behind extensive GPS jamming during NATO exercises.[6] The Russian full-scale invasion of Ukraine on February 24, 2022 marked an uptick in GPS jamming in the whole Nordic-Baltic region. In Northern Norway,

close to the Russian border, GPS was jammed for several days at a time in 2022, and the frequency increased to "almost daily" by 2024.[7]

An increasingly common interference activity is spoofing. Instead of jamming the signal, this method deceives a receiver about a ship's or an airplane's real location.[8] In late April 2025 Swedish authorities reported an increase in GPS spoofing in the central Baltic Sea, and just before Midsummer festivities Swedish authorities warned holiday sailors to take caution against GPS-disturbances.[9] The Swedish Maritime Association noted that spoofing occurrences have been more frequent in southern parts of the Baltic Sea.[10]

With spoofing, ships that were in reality nowhere near Russia suddenly appeared to be in Russian waters. In 2021, Swedish naval ships seemed to be aggressively sailing near Russian waters outside of Kaliningrad on MarineTraffic and other real time applications. But in reality, they were anchored in a port or even in a dockyard. The Swedish Navy stated that they saw a clear pattern in the incidents.[11]

Intimidation Is In the Air

Another frequently applied Russian tool of interference towards its Nordic and Baltic neighbours are combinations of unsafe maneuvers, buzzing borders, airspace violations, and flying without transponders. Here too have the numbers of violations spiked since Russia's full-scale invasion. In 2023 alone, NATO Air Policing intercepted Russian aircraft more than 300 times.[12] NATO has not disclosed the numbers for 2024.

But even prior to the full-scale invasion of Ukraine, the incidents were frequent. The Lithuanian Ministry of Defence regularly publishes data on interceptions of aircraft near the Baltic States' borders. One example from a single week in May 2021 counted NATO Air Policing jets scrambling "three times to identify and escort military aircraft of the Russian Federation in the international airspace over the Baltic Sea."[13] The same pattern has persisted. In April 2025, the British Royal Air Force intercepted an IL-20M (NATO code name Coot-A) reconnaissance aircraft from a base in Poland on the 15th and an unknown aircraft leaving Kaliningrad on the 17th.[14] That same week, two Swedish Gripen fighters were scrambled from their base in Poland to escort another IL20M approaching Polish airspace.[15]

Russia is also known to use deliberate air space violations as a means to express dissatisfaction, as was the case in 2016 when two Russian SU-27 fighter jets, while transporting Iskander missiles to Kaliningrad, violated Finnish air space one day before Finland signed a bilateral statement of intent on defence cooperation with the United States.[16] Norway has also frequently been subjected to such intimidation measures, especially via "Notices to Airmen" (NOTAMs), a warning system for potentially dangerous missile launches and other military activities. As Kristian Åtland, Thomas Nilsen and Torbjørn Pedersen find in their research of Russia's use of NOTAMS from 2015-2021, "Russia's NOTAM warnings appear to have been tailored for the purpose of intimidating Norway and its allies and communicating Russia's displeasure with the occasional presence of United States and other NATO forces on or outside Norway's territory."[17] Perhaps the most audacious example of Russia's aggressive use of military manoeuvres to intimidate its neighbours was the so-called "Russian Easter" incident in 2013, when Russian fighter jets exercised an attack on Sweden. A NATO report later stated that the incident was a simulated nuclear attack.[18]

A Fleet Appears From the Shadows

While unprecedented in nature, Western sanctions on Russian energy since the full-scale invasion of Ukraine have not resulted in the desired effect of emptying Russia's war chest. Russia has found an effective way to circumvent them with a "shadow fleet" of some 1500 tankers exporting oil to India, China, and other countries. The shadow fleet accounts for half of Russian oil exports.[19]

Ownership structures are deliberately obscured and, in addition to financing Russia's war in Ukraine, the fleet also poses environmental risks, as vessels are often old, rusty, and uninsured. The Swedish public broadcaster SVT followed a Cypriot tanker, which was anchored off Gotland for two months in 2024 serving as a fueling station for the shadow fleet, and found that 52 out of 56 refuelling operations were for ships heading to or from Russia.[20]

Recently, the shadow fleet has gained wide media attention for damaging critical maritime infrastructure in the Baltic Sea. Between October 2023 and June 2025, there were four cases of ships severing undersea cables by dragging their anchor. Two were Russian shadow fleet, but two were also Chinese: the

Hong Kong-flagged *NewNew Polar Bear* damaged the Baltic Connector gas pipeline and data cables between Finland and Estonia in October 2023;[21] the Chinese *Yi Peng 3* severed data cables between Finland and Germany and between Sweden and Lithuania in November 2024;[22] the Cook Island-flagged *Eagle S* damaged the Estlink 2 power cable between Finland and Estonia in December 2024;[23] and in late January 2025, yet another data cable was damaged between Latvia and Sweden.[24]

The responses by Baltic Sea states have gradually improved. In the first incident, the *NewNew Polar Bear* refused to comply with the Finnish National Bureau of Investigation's demands. Instead, it sailed off to the Northern Sea Route, accompanied by Rosatom's atomic ice breaking cargo ship *Sevmorput*.[25] In the *Yi Peng 3* case, the Danish military managed to halt the vessel and Swedish police were allowed to board it, but only in an observational capacity; Chinese officials conducted the investigation as the flag nation.[26] Unsurprisingly, the investigation did not determine whether the ship damaged the cables on purpose before the ship sailed off to its next destination. The Swedish Accident Investigation Authority later stated that their access to information was restricted by the Chinese officials.[27]

In the later cases, involving the *Eagle S* (in the Gulf of Finland) and the Maltese flagged ship *Vezhen* (suspected of damaging a cable between Sweden and Latvia), the Finnish and Swedish authorities were ready for tougher measures. The ships suspected of sabotage were identified swiftly and they complied with authorities' requests directing them to Finnish and Swedish territorial waters, respectively. In the *Eagle S* case, armed special forces of the Finnish Police and Border Guard boarded the ship from a helicopter, and a Finnish Defence Forces missile boat and a Border Guard patrol vessel operated in the area.[28] The Estonian Navy reacted immediately by sending a patrol to protect the other Estlink cable, and the UK-led Joint Expeditionary Force (a defence cooperation format between the five Nordic countries, the three Baltic countries and the Netherlands) activated its reaction system a week after the incident.[29] Three weeks later, after a Baltic Sea NATO meeting in Helsinki, NATO increased its presence around critical infrastructure with the vigilance activity "Baltic Sentry."[30] In the *Vezhen* case, the Swedish authorities followed the Finnish example by ordering the suspected vessel to enter Swed-

ish territorial waters, boarding and confiscating the ship for investigation the same day damage was detected.[31]

The investigation in the *Eagle S* case is proceeding. In the end of May 2025, Finnish police turned the investigation over to the prosecutor with three persons, the captain and the first and the second mate, suspected of aggravated sabotage and aggravated disturbances of post- and telecommunication. A trial is likely held in early autumn.

Suspicion is one matter, but it is entirely another to gather enough evidence to convict suspects. In the *Vezhen* case,the Swedish authorities concluded only after a few weeks of investigation that the incident was likely an accident—the Latvian authorities, however, did not immediately agree.[32] It seems highly unlikely that a ship could drag its anchor for 100 km, as the *Eagle S* did, without the crew noticing. However, plausible deniability—or at least the lack of clear proof of intent—is an integral part of a hybrid operation involving potentially high-stakes damage to critical infrastructure. It will likely be even harder to establish a link to Russia when neither the crew, stated owner (with the actual owner hidden under layers of corporate names) nor flag is Russian. In May 2025, however, Russia itself lifted the veil of (im)plausible deniability when a Sukhoi-35 jet buzzed Estonian airspace while the Estonian navy was trying to escort a suspected shadow fleet vessel into Estonian territorial waters for boarding, in the Gulf of Finland. The Estonian Defence Forces reported that the Sukhoi-35 had not filed a flight plan, its transponders were turned off, and the pilot did not maintain two-way communication with Estonia's air traffic control.[33] The ship sailed off to Russian waters.

How to deal with the shadow fleet more proactively is not an easy question, given freedom of navigation and that many shadow fleet vessels do not necessarily call at ports in the Baltic Sea states. The Swedish government announced in May 2025 that the coast guard and the Swedish Maritime Administration will be able to begin collecting insurance information from ships passing through the Swedish territorial waters and exclusive economic zone (EEZ), even if they do not call at a Swedish port.[34] This measure, while welcome, nevertheless does not solve the shadow fleet problem. The EU is now tackling the issue with extensive sanctions on 342 vessels (as of June 2025).[35]

The sanctions are an important but reactive step amounting to a "whack a mole" strategy. Therefore, the beginnings of a proactive approach, though failing to name specifics, was outlined in a joint-statement from 14 littoral European states (11 in the EU and 3 outside (UK, Norway and Iceland)) on June 19, 2025: "Stateless vessels, including those falsely claiming to fly a flag, do not have a responsible flag state and are not entitled to rights under the United Nations Convention on the Law of the Sea (UNCLOS), including freedom of navigation. If vessels fail to fly a valid flag in the Baltic Sea and the North Sea, we will take appropriate action within international law."[36]

References

1 Emmanuel Grynszpan and Cédric Pietralunga, "Russia's GPS Jamming Intensifies over the Baltic Sea," *Le Monde*, May 2, 2024, https://www.lemonde.fr/en/international/article/2024/05/02/russia-s-gps-jamming-intensifies-over-the-baltic-sea_6670151_4.html; Vitaly Shevchenko, "Russia Accused of Jamming GPS Navigation," *BBC*, May 2, 2024, https://www.bbc.com/news/articles/cne900k4wvjo.

2 Yle News, "GPS Disruptions Force Return of Two Finnair Planes," *Yle News*, April 27, 2024, https://yle.fi/a/74-20086068.

3 Finnair, "Finnair Suspends Flights between Helsinki and Tartu for a Month," *Finnair*, April 29, 2024, https://www.finnair.com/en/flight-information/travel-updates/finnair-suspends-flights-to-tartu-for-a-month-3383244.

4 Tartu Airport website, "Finnair resumes flights to Tartu," May 16, 2024, https://airport.ee/en/finnair-resumes-flights-to-tartu/.

5 Salon Seudun Sanomat, "GPS-Häirintä Ei Voi Aiheuttaa Vaaratilanteita Suomessa—'Ilmailussa Kaikki Järjestelmät Varmistettu'," *Salon Seudun Sanomat*, November 9, 2018, https://www.sss.fi/2018/11/yle-venajan-gps-hairinta-ulottui-lappiin-naton-sotaharjoituksen-aikana/comment-page-1/.

6 Nerijus Adomaitis, "Norway Says It Proved Russian GPS Interference during NATO Exercises," *Reuters*, March 19, 2019, https://www.reuters.com/article/idUSKCN1QZ1WM/.

7 Thomas Nilsen, "More Russian GPS Jamming than Ever across Border to Norway," *The Independent Barents Observer*, July 9, 2022, https://thebarentsobserver.com/en/security/2022/07/more-russian-gps-jamming-ever-across-border-norway; Thomas Nilsen, "Russian Jamming Is Now Messing up GPS Signals for Norwegian Aviation Practically Every Day," *The Independent Barents Observer*, February 26, 2024, https://thebarentsobserver.com/en/security/2024/02/russian-jamming-now-messing-gps-signals-norwegian-aviation-practically-every-day.

8 Michael Drummond, "Pull up! Pull up!", *Sky News*, March 18, 2025, https://news.sky.com/story/pull-up-pull-up-who-is-messing-with-gps-signals-used-by-passenger-planes-and-why-13331351.

9 Crisis Information, "Varning för GPS-störningar i Östersjön," June 19, 2025, https://www.krisinformation.se/nyheter/2025/juni/varning-for-gps-storningar-i-ostersjon.

10 Nora Fernstedt, "GPS-störningar: Fartyg ser ut att vara i Ryssland," *Aftonbladet*, May 1, 2025, https://www.aftonbladet.se/nyheter/a/kwjA8L/gps-storningar-fartyg-ser-ut-att-vara-i-ryssland.

11 Mikael Holmström, "Falska svenska marina fartyg på nätet—pekas ut på positioner nära Ryssland," *Dagens Nyheter*, March 10, 2021, https://www.dn.se/sverige/falska-svenska-marina-fartyg-pa-natet-pekas-ut-pa-positioner-nara-ryssland/

12 NATO, "NATO Intercepted Russian Military Aircraft over 300 Times in 2023," *NATO Pressroom*, December 29, 2023, https://ac.nato.int/archive/2023/NATO_AP_2023.
13 Ministry of National Defence Republic of Lithuania, "Data on Interceptions of Aircraft Completed near the Baltic States' Borders on May 10–16, 2021," May 16, 2021, https://kam.lt/en/data-on-interceptions-of-aircraft-completed-near-the-baltic-states-borders-on-may-10-16-2021/.
14 Jamie Whitehead, "RAF jets intercept Russian aircraft near Nato airspace," *BBC*, April 20, 2025, https://www.bbc.com/news/articles/cx2y515gzq7o
15 CBS News, "Sweden scrambles fighter jets to intercept Russia spy plane over Baltic Sea," *CBS News*, April 24, 2025, https://www.cbsnews.com/news/sweden-fighter-jets-intercept-russian-spy-plane-baltic-sea/
16 Yle Uutiset, "Ministeri Niinistö Epäiltyjen Ilmatilaloukkausten Yhteydestä USA-Sopimukseen: 'Näen Ajallisen Yhteyden, Mutta En Osaa Sanoa Muusta,'" *Yle Uutiset*, October 7, 2016, https://yle.fi/a/3-9216452.
17 Kristian Åtland, Thomas Nilsen, and Torbjørn Pedersen (2022), "Military Muscle-Flexing as Interstate Communication: Russian NOTAM Warnings off the Coast of Norway, 2015–2021", *Scandinavian Journal of Military Studies*, 2022, 5(1), pp. 63–78, DOI: 10.31374/sjms.133.
18 NATO, The Secretary General's Annual Report 2015, p. 19, https://www.nato.int/cps/en/natohq/topics_127529.htm.
19 Martin Mederyd Hårdh, "Spökskeppen Misstänks Spionera På Sverige," *Svenska Dagbladet*, May 4, 2024, https://www.svd.se/a/Xjw1ko/spokskeppen-smorjer-den-ryska-krigsmaskinen.
20 John Granlund and Oskar Jönsson, "Här Tankas Ryska Skuggflottan—Från Fartyg Utanför Gotland," *SVT Nyheter*, April 9, 2024, https://www.svt.se/nyheter/inrikes/har-tankas-ryska-skuggflottan-fran-fartyg-utanfor-gotland.
21 Micah McCartney, "China admits container ship damaged pipeline," *Newsweek*, August 13, 2024, https://www.newsweek.com/china-admits-container-ship-damaged-baltic-sea-gas-pipeline-1938377.
22 AP News, "Danish military monitors a Chinese-flagged bulk carrier after undersea data cables were ruptured," November 21, 2024, https://apnews.com/article/denmark-sweden-finland-germany-lithuania-china-yi-peng-undersea-cables-d3af1bf7e68ff060bb6e669f24425fd0.
23 Yle, "Stubb on cable damage: We know who did it," December 27, 2025, https://yle.fi/a/74-20133686).
24 Andrius Sytas and Johan Ahlander, "Sweden opens sabotage probe into Baltic undersea cable damage," *Reuters*, January 26, 2025, https://www.reuters.com/world/europe/baltic-undersea-cable-damaged-by-external-influence-sunday-latvian-broadcaster-2025-01-26/.
25 Atle Staalesen, "Runaway ship Newnew Polar Bear, suspected of sabotage in Baltic Sea, is sailing into Russian Arctic waters," *The Barents Observer*, October 26, 2023, https://www.thebarentsobserver.com/security/runaway-ship-newnew-polar-bear-suspected-of-sabotage-in-baltic-sea-is-sailing-into-russian-arctic-waters/164423.
26 Louise Rasmussen, "China lets Sweden, Finland, Germany and Denmark board ship in cable breach case," *Reuters*, December 20, 2024, https://www.reuters.com/world/europe/swedish-police-go-board-yi-peng-3-vessel-invitation-china-2024-12-19/.
27 SVT Nyheter, "Inga bevis för avsiktligt kabelbrott i Östersjön," *SVT Nyheter*, April 15, 2025, https://www.svt.se/nyheter/inrikes/inga-bevis-for-avsiktligt-kabelbrott-i-ostersjon.
28 Police of Finland (2024) "Police investigating incidents in the Gulf of Finland in cooperation with other authorities," December 26, 2024, https://poliisi.fi/en/-/police-investigating-incidents-in-the-gulf-of-finland-in-cooperation-with-other-authorities; Police of Finland (2024) "Gulf

of Finland cable rupture: Investigation of the seabed underway", December 27, 2024, https://poliisi.fi/en/-/gulf-of-finland-cable-rupture-investigation-of-the-seabed-underway.

29 Margit Kilumets and Sten Teppan, "Estonia dispatches Navy patrol boat to guard EstLink 1 cable," *ERR*, December 27, 2024, https://news.err.ee/1609561090/estonia-dispatches-navy-patrol-boat-to-guard-estlink-1-cable; UK Government (2025) "Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet", January 6, 2025, https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet.

30 NATO, "NATO launches 'Baltic Sentry' to increase critical infrastructure security," *NATO*, January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm.

31 Swedish Prosecution Authority, "Förundersökning inledd efter kabelbrott i Östersjön," [Preliminary investigation underway after cable rupture in the Baltic Sea], January 26, 2025, https://via.tt.se/pressmeddelande/3764867/forundersokning-inledd-efter-kabelbrott-i-ostersjon?publisherId=3235540&lang=sv.

32 LSM, "Latvian authorities still investigating undersea cable damage as possible sabotage," *LSM*, Febraury 10, 2025, https://eng.lsm.lv/article/society/defense/10.02.2025-latvian-authorities-still-investigating-undersea-cable-damage-as-possible-sabotage.a587207/.

33 Brendan Cole, "Russian Jet Violates NATO Airspace as Putin 'Shadow Fleet' Tanker Escorted," *Newsweek*, May 15, 2025, https://www.newsweek.com/russia-nato-putin-shadow-fleet-2072535.

34 AP News, "Sweden will step up insurance checks on foreign ships as worries about Russia rise," May 31, 2025, https://apnews.com/article/sweden-ships-insurance-baltic-russia-shadow-fleet-898ee1730700cc5d2d90203cd946f48.

35 European Commission, "EU adopts 17th sanctions package against Russia," May 20, 2025, https://enlargement.ec.europa.eu/news/eu-adopts-17th-sanctions-package-against-russia-2025-05-20_en.

36 Estonian MFA, "Joint Actions to Further Counter the Shadow Fleet," June 19, 2025, https://vm.ee/en/news/joint-actions-further-counter-shadow-fleet.

Denmark: Russian Disinformation Using Greenland, Ukraine—and Maybe Even Sudan

By Jeanette Serritzlev

Hostile information

Cyber attack (civilian target)

Democratic institution

Critical infrastructure

Religion

This chapter examines three recent examples of Russian or pro-Russian information operations targeting Denmark. The first case concerns Distributed Denial of Service (DDoS) attacks in 2023 claimed to be conducted by a group called Anonymous Sudan.[1] Despite the name, questions remain who was behind this group. Was it a Russian information operation, as suggested by cyber experts? Was it simply hackers-for-hire, who found it profitable to be affiliated with a well-known pro-Russian hacker group? And if they were hacker-mercenaries, who hired them?

The other two disinformation cases went viral as fake posts distributed on X (formerly Twitter). One about Greenland has been attributed as Russian disinformation by the Danish Defence Intelligence Service;[2] the other, claiming a Danish F-16 pilot was killed in Ukraine, has been labelled a 'fake Russian story' by the Danish Ministry of Defence.[3] The cases were clearly state-aligned disinformation, but were they state-conducted or state-approved? If so, can it be proved?

The ambiguity serves as a shield for the attacker, and it restrains the response options for the attacked party, making these kinds of activities convenient tools for the aggressor.

Sudanese hackers with dubious affiliations

In February 2023, a hacker group claiming to be Anonymous Sudan wrote on Telegram, "The unfortunate country we want to attack tomorrow is: Denmark." The Telegram group was new, first created in January that same year. The next day, Copenhagen Airport's webpages were taken down by a DDoS attack. It was just one of several attacks Anonymous Sudan claimed responsibility for in Denmark as well as Sweden.

One week later, several Danish airports' webpages were inoperative due to a new wave of DDoS attacks. A few days later, Danish hospitals and universities were targets of similar attacks. Additional attacks on the Danish State Railways and a Danish media outlet followed.[4]

A DDoS attack is a malicious attempt to overwhelm a targeted server, service, or network with a flood of internet traffic from multiple sources, rendering it inaccessible to legitimate users. According to the Danish Centre for Cyber Security, DDoS attacks are the preferred weapon for cyber activist hackers, as they have the dual advantage of not requiring advanced technical skills while at the same time attracting media attention.[5] DDoS attacks are often considered to have one of two purposes: deception or influence. As a means of deception, DDoS attacks can attract attention in one area, while the actual attack takes place elsewhere. As a means of influence, the same kind of attacks can be carried out in order to achieve a cognitive effect due to the public attention they receive. To the general public, the media coverage of these relatively simple attacks creates a perception that the country is frequently under cyber attack, increasing a sense of insecurity among the population.

This is not the first time Denmark has been targeted by DDoS attacks. The 2023 annual Danish Centre for Cyber Security threat assessment writes that pro-Russian hackers have been particularly active since Russia's full-scale invasion. This latest case, however, is more complex than most, with the alleged hacker group claiming to be affiliated with the hacktivist network Anonymous from Sudan, attacking targets simultaneously in Denmark and Sweden, all allegedly due to a right-wing individual with Danish-Swedish citizenship burning the Quran in public places in both countries. The Anonymous Sudan group was created just days before the Quran burning outside the Turkish Embassy in Stockholm.

The Quran burning incidents received international attention, including substantial criticism from Muslim countries, which demanded the Danish and Swedish governments to take initiatives to punish such actions. In that context, a religiously motivated hacker group is plausible. However, IT and cyber security experts quickly adopted the view that the operations were connected to Russia,[6] with cyber security companies such as Swedish Truesec reporting that Anonymous Sudan's attack against Sweden was a Russian information operation.[7] Regarding Sweden specifically, the operation was assessed as an attempt to sow discord between Sweden and Turkey during Sweden's NATO accession process.[8] For both Denmark and Sweden, the operations kept the Quran burnings in the media spotlight, sparking public debate and international pressure. But the activities were larger than Denmark and Sweden.

Mandiant Intelligence reported[9] that Anonymous Sudan accounted for 63 percent of total identified DDoS attacks claimed by pro-Kremlin 'patriotic' hacker collective KillNet in the first half of 2023: "The group only emerged in January 2023, making the proportion of KillNet operations they comprise additionally notable."[10] Mandiant Intelligence also added that Anonymous Sudan's attack on Microsoft services in 2023 "marked a significant increase in observed capabilities of the KillNet collective, which had previously struggled to impact claimed targets of previous operations" leading to the following conclusion:

> "Paired with KillNet's reported compromise and leak of North Atlantic Treaty Organization (NATO) documents, this sudden increase in capability could indicate significant investment from more sophisticated actors, particularly when measured against KillNet's capabilities since the collective's inception in late 2021."

Torben Clemmensen, an expert from the French IT security company TEHTRIS, explained to the Danish business newspaper BORSEN that not only did the group communicate in Russian, their IP addresses were also Russian. The company analysed 47 specific attacks against the Nordic countries. Of these, 90 percent were deemed likely to be a reaction to support for Ukraine; only two of the 47 attacks could be related to the issue of the Quran burnings.[11]

The affiliation of the group labelled Anonymous Sudan has since been questioned. In the fall of 2024, the U.S. Attorney's Office in the Central District of California indicted two Sudanese brothers for "operating and controlling" the group. One of the released documents explicitly addressed the Russian link, stating:

> "There has been some media and threat research company reporting suggesting that Anonymous Sudan may be state-sponsored Russian actors masquerading as Sudanese actors with Islamist motivations, and Anonymous Sudan has publicly claimed an affiliation with pro-Russian hacktivist collective 'KillNet.' However, my investigation to date has indicated that Anonymous Sudan is in fact led by Sudan-based individuals, including AHMED and a co-conspirator, although the group may share ideologies with, and sometimes appears to act in concert with, KillNet and similar hacktivist groups."[12]

Wired reported that Anonymous Sudan's alleged partnership with KillNet "led some in the cybersecurity community to suspect that Anonymous Sudan was, in fact, a Russia-linked operation using its Sudanese identity as a front, given Russia's history of using hacktivism as false flag," but that the charges against the brothers suggested that the group was "authentically Sudanese in origin."[13] In response to the indictment's conclusion, cybersecurity reporter Catalin Cimpanu sarcastically wrote a newsletter deconstructing some of the arguments against Russian connections: "I'm sorry, but what were they expecting to find? GRU employment contracts? That's not how this works. It's also not how attribution works."[14]

Naming the group "Anonymous Sudan" will associate a specific network and a specific country to the attacks in the general public's perception. Even though a hacker network like Anonymous is not easily defined, the "real" Anonymous network took a pro-Ukraine stance right after the Russian full-scale invasion. The 2024 indictment against the two Sudanese citizens does not change the facts documented by cyber experts—including that the group initially communicated in Russian and English, and—only after being suspected of affiliations to Russia—switched to Arabic and finally later to a Sudanese Arabic dialect. Furthermore, Russian hackers have used false Anony-

mous accounts before, as reported by Christo Grozev, Roman Dobrokhotov, and Michael Weiss in The Insider in May 2025.[15] This does not prove that Anonymous Sudan is a Russian front organisation, but paired with the other facts, it supports the assessment of, if not a Russian affiliation, then at least pro-Russian alignment.

Disinformation from Greenland to Ukraine

Each year in December, the Danish Defence Intelligence Service releases its public threat assessment Intelligence Outlook. In December 2024, the publication included this assessment:

> "Denmark, the Faroe Islands and Greenland are not a specific priority target for Russian influence campaigns. However, Russia will likely also include Denmark, the Faroe Islands and Greenland in its influence campaigns targeting the EU, NATO or the wider Western world."[16]

It would later prove to be a fairly accurate prediction: In January 2025 it became reality. The first example was related to the tension between the Kingdom of Denmark and the United States' expressed desire to "claim" Greenland. The second case was related to Denmark's steadfast support to Ukraine.

"In a situation of extreme escalation and tension, we have to take extreme measures and ask for help from Russia to solve this problem." These words were allegedly from Danish member of parliament Karsten Honge's post on X in January 2025. The post was shared as a picture—not with a link to the post, since it did not exist. On Karsten Honges real X account, he posted on January 14, 2025, that "there is [not] a snowball's chance in hell" that he would ask Russia for any kind of support.

Most people in Denmark would know that this could not be a real statement from the politician in question. But if the intended audiences are not in Denmark, it does not matter. According to the Danish fact-checking media TjekDet, the post was shared for the first time on Telegram on January 10, 2025.[17] TjekDet identified that the post also had been spread among pro-Russian profiles on Facebook, Instagram and X. The post was in relatively decent Danish. However, there is a linguistic warning light in the Danish version of the words "The United States of America," in Danish "Amerikas Forenede

Stater." This is not entirely wrong, but the more natural Danish wording in social media posts would simply be "USA."

According to Karsten Honge, he received many inquiries from foreign media who wanted a comment for this controversial call for help. The incident shows that a false post, which primarily seems to circulate in pro-Russian ecosystems, suddenly can have a wider effect. In this case, to give the impression that there are Danish elected officials who are open towards Russia. The Danish Defence Intelligence Service has since attributed the case to be a Russian influence operation.[18]

The next case, concerning a Danish F-16 pilot allegedly killed in Ukraine, appeared only a couple days after the Karsten Honge fake-post, and has been called a "fake Russian story" by the Danish Ministry of defense.[19] On January 17, 2025, a post on X from the Danish profile "Oscar Sorensen" told that he was sorry to learn that his colleague and friend, an F-16 fighter pilot, had been killed in Kryvyi Rih—President Zelensky's hometown.

The post was written in fairly good Danish and was subsequently spread and shared by pro-Russian accounts in various languages, particularly on Saturday, January 18. That same day, the story was taken up by Russian media and disinformation networks, including TASS and RT. The articles referred to the post from the "friend," while many of the shares on X were added with a description explaining that the pilot had been hit by a Russian Iskander missile after revealing his position to a prostitute. On Sunday, January 19, the Danish Ministry of Defense pro-actively debunked the story. The Ministry of Defense's quick reaction indicates that it was taken seriously. With good reason, due to the serious claim.

Not only is there a temporal coincidence between the fake stories of Karsten Honge and the F-16 pilot, as they both emerged within a week, there is also a similarity in the *modus operandi*. Both false posts were in Danish, but primarily shared in pro-Russian networks in other languages. Both posts were relatively well written, meaning that the red flags in terms of Danish wording and grammar were few. But even if the language issues had been more obvious, it may not have had any significant impact as the target audiences were not Danish native speakers, according to the assessment from the Danish Defence Intelligence Service from December 2024.[20]

Plausible deniability is often viewed as a core element in hybrid attacks. It can be difficult to prove that an action is undertaken at the direction of a state actor, or if it just aligns with the strategic interests, shared values, or financial interests of a state actor. Some activities can be attributed and communicated to the public; others might be identified but not publicly disclosed. As stated in the 2024 Danish Intelligence Outlook, Russia often tries to conceal its role in hybrid activities, because it makes it more difficult for the countries targeted to respond effectively. This concealment includes the use of proxies, front organisations, private actors, criminal networks and pro-Russian audiences—regardless nationality.

These kinds of hybrid activities thrive in, exploit, and adapt to the conditions of the modern information environment. Clausewitz wrote about the "fog of war" in the 19th century, and "the fog of hybrid war" is an inherent characteristic of these activities carried out in the grey zone, by multiple actors, in shadowy disguise.

References

1 Nyheder TV2, "Mystisk Hackergruppe Påstår at Stå Bag Angreb På Danmark—TV 2 Har Spurgt Dem, Hvem de Er," *Nyheder TV2*, February 27, 2023, https://nyheder.tv2.dk/samfund/2023-02-27-mystisk-hackergruppe-paastaar-at-staa-bag-angreb-paa-danmark-tv-2-har-spurgt-dem-hvem-de-er.

2 "Russisk påvirkningsoperation udnyttede dansk medlem af Folketinget," *Danish Defence Intelligence Service*, April 25, 2025, https://www.fe-ddis.dk/da/nyheder/2025/russisk-pavirkningsoperation-udnyttede-dansk-medlem-af--folketinget/.

3 *Danish Ministry of Defence*, January 19, 2025, https://x.com/Forsvarsmin/status/1880949183856922803.

4 Nyheder TV2, "Berygtet Hackergruppe Varsler Nye Angreb Mod Danmark," *Nyheder TV2*, April 2, 2023, https://nyheder.tv2.dk/samfund/2023-04-02-berygtet-hackergruppe-varsler-nye-angreb-mod-danmark.

5 "Cybertruslen Mod Danmark 2023," *Center for Cybersikkerhed*, May, 2023, https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/.

6 Christina Toustrup Eriksen, "Først Gik Det Ud over Sverige. Nu Danmark. Det Ved vi Om Striben Af Hackerangreb—Flere Ting Peger Mod Rusland," *Berlingske,* February 23, 2023, https://www.berlingske.dk/samfund/foerst-gik-det-ud-over-sverige-nu-danmark-det-ved-vi-om-striben-af.

7 Mathias Wåhlén, "Anonymous Sudan—Threat Intelligence Report," *Truesec*, February, 2023, https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf.

8 The burning of the Quran outside the Turkish Embassy in Stockholm in January 2023 happened after an idea of two Swedish alternative media personalities. They represented outlets with pro-Russian

narratives and Russian connections, such as election observer trips. One of those taking the initiative has stated he is a vocal opponent of Nato-membership. But that is another story.

9 Mandiant Intelligence, "KillNet Showcases New Capabilities While Repeating Older Tactics," *Mandiant Intelligence*, July 20, 2023, https://cloud.google.com/blog/topics/threat-intelligence/KillNet-new-capabilities-older-tactics/.

10 Antoaneta Roussi, "Meet KillNet, Russia's hacking patriots plaguing Europé," *Politico*, September 9, 2022, https://www.politico.eu/article/meet-KillNet-russias-hacking-patriots-plaguing-europe/.

11 Mathias Sommer and Godtfred Perera, "Eksperter Er Ikke I Tvivl: Russiske Hackere Står Bag Falsk Flag-Angreb Mod Danmark," *Børsen,* April 26, 2023 https://borsen.dk/nyheder/virksomheder/falsk-flag-hackerangreb-kan-spores-til-rusland.

12 "Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World," *U.S. Attorney's Office, Central District of California*, October 16, 2024 https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals.

13 Andy Greenberg, "Hacker Charged With Seeking to Kill Using Cyber attacks on Hospitals," *Wired*, October 16, 2024, https://www.wired.com/story/anonymous-sudan-ddos-indictment-takedown/.

14 Catalin Cimpanu, "Anonymous Sudan's Russia Links Are (Still) Obvious," *Risky Biz News*, October 18, 2024, https://news.risky.biz/risky-biz-news-the-feds-secretly-disrupted-anonymous-sudan-back-in-march/.

15 Christo Grozev, Roman Dobrokhotov and Michael Weiss, "Hidden Bear: The GRU hackers of Russia's most notorious kill squad," *The Insider*, May 31, 2025, https://theins.press/en/inv/281731.

16 "Intelligence Outlook 2024: An intelligence-based assessment of the external conditions for Danish national security and interests," *Danish Defence Intelligence Service*, December, 2024, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/.

17 TjekDet, "SF-politiker bliver misbrugt i falske, pro-russiske opslag om Grønland," *TjekDet*, January 14, 2025, https://www.tjekdet.dk/faktatjek/sf-politiker-bliver-misbrugt-i-falske-pro-russiske-opslag-om-groenland.

18 "Russisk påvirkningsoperation udnyttede dansk medlem af Folketinget," *Danish Defence Intelligence Service*, April 25, 2025, https://www.fe-ddis.dk/da/nyheder/2025/russisk-pavirkningsoperation-udnyttede-dansk-medlem-af--folketinget/.

19 *Danish Ministry of Defence*, January 19, 2025, https://x.com/Forsvarsmin/status/1880949183856922803.

20 "Intelligence Outlook 2024: An intelligence-based assessment of the external conditions for Danish national security and interests," *Danish Defence Intelligence Service*, December, 2024, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/.

Estonia: Smashing Cars and Sowing Fear

By Marek Kohv

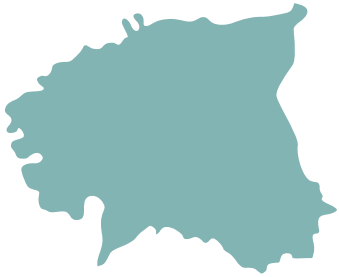
Vandalism / sabotage

Democratic Institution

Harassment / assault

History / memory

Criminals / mercenaries / private contractors



For several years, Russia's military intelligence agency (GRU) has attempted to intimidate Estonian politicians, public figures, and the general public for expressing support for Ukraine. In early 2024, the cars of the Minister of the Interior and a journalist were vandalised and several World War II memorials were defaced. In connection with these hybrid attacks, around ten individuals were arrested. A GRU operative, Allan Hantsom, was sentenced to six and half years in prison for crimes against the Estonian state. Although several individuals linked to these incidents reside in Russia, they have been placed on international wanted lists and barred from entering the Schengen Area for several years.[1]

In February 2024, dual Estonian-Russian citizen Andrei Makarov set fire to a car with Ukrainian license plates in Tartu and attempted to create the impression that the act was committed by the KOOS political movement.[2] He spray-painted the word "KOOS" in large letters on the car's hood, filmed the burning vehicle, and uploaded the footage to Telegram. In cooperation with international partners, Estonia's Internal Security Service determined that Makarov had also conducted surveillance of a former serviceman of the Russian Federation who fled Russia and resided in Lithuania, surveilled NATO military equipment in Riga, and police and emergency service activities in Poland.[3] On 25 March 2025, the Tartu County Court convicted Makarov of

treason, sentencing him to 15 years in prison. The court found sufficient and convincing evidence in the case that confirms the validity of the treason charge against Makarov, but the ruling is not yet final.[4]

On February 11, 2025, two Moldovan citizens, both named Ivan Chihaial (born in 1992 and 1987), were arrested in Italy at the request of Estonia's prosecutor's office and extradited on suspicion of committing arson on behalf of the GRU in Estonia.[5] In January 2025, the younger Chihaial had set fire to a COOP grocery store in Osula, Võru County. The next day, a person acting on behalf of the GRU gave him the task of setting fire to the *Slava Ukraina* restaurant in Tallinn. To prepare the attack, the younger Chihaial brought his cousin of the same name, who was unaware of the connection to the Russian intelligence service. On the night of January 31, they set fire to the restaurant and then left Estonia.

In court, on July 2, 2025, both men entered plea agreements: The younger Chihaia received a six-and-a-half-year prison sentence for intelligence activities against Estonia in direct coordination with GRU operatives. The older Chihaia received a six-month prison sentence for the destruction of property by arson, with an additional two-year suspended sentence contingent on a three-and-a-half-year probation period. The court acknowledged the lack of evidence proving the older Chihaia's awareness of the GRU's involvement or specific motives.[6]

Such attacks are no longer exceptional. Across Europe, acts of sabotage and vandalism linked to Russian intelligence services have become increasingly frequent. Russia aims to demonstrate to Western states that a country's support for Ukraine could turn it into a target for Russian attacks.

Estonia is, therefore, not the only example, as the other country chapters in this book demonstrate. In Warsaw in May 2024, a shopping centre was set ablaze.[7] The Polish Ministry of Foreign Affairs confirmed on May 12, 2025 that an investigation had found Russian intelligence services to be behind the large-scale fire at the shopping mall in the Polish capital.[8]

In late February 2025, a Ukrainian national was sentenced by a Polish court to eight years in prison for preparing acts of sabotage and arson on behalf of Russia. According to the Polish Security Agency, the individual had been recruited via Telegram to set fire to a paint factory in Wroclaw—a highly

flammable facility located near an oil refinery storing 56 million litres of fuel. Arrested in January 2024, the man was found carrying lighter fluid, tutorial videos on handling explosives, and a manual encouraging Ukrainians to support Russia's invasion.[9]

In early May 2024, a fire broke out at an IKEA store in Vilnius, Lithuania. Though quickly extinguished, the incident was connected to the earlier Polish fires, an implication echoed by Polish Prime Minister Donald Tusk. Lithuanian authorities, however, were initially more cautious in attributing the attack directly to Russia. On March 17, 2025, Lithuania's Prosecutor General formally linked the arson to Russia's GRU.[10] Two Ukrainian citizens were suspects—one was detained in Lithuania, the other in Poland. As in the Estonian incident involving the Minister of the Interior's vehicle, investigations revealed that the perpetrators were directed through intermediaries by organisers based in Russia, with connections to Russian military and security services.

In Merkinė, Lithuania, the monument to anti-Soviet resistance leader Adolfas Ramanauskas-Vanagas was covered with red paint and a black swastika on January 29, 2024. Through cooperation between the security and law enforcement institutions of Lithuania, Latvia, and Estonia, the individuals suspected of committing this and other criminal acts under the orders of the Russian secret services in the three Baltic countries were detained in Estonia and Latvia. Two of them have dual Estonian and Russian citizenship and one of them is a Russian citizen. The suspects all knew each other and lived in Tallinn; Estonian authorities arrested the suspects and are in custody in Lithuania as of July 2025.[11]

During the investigation, it was determined that these individuals, acting in an organized group, carried out tasks for the special services of the Russian Federation, specifically the GRU, in order to destabilize the state.[12]

In retrospect, these incidents across Europe suggest that the operational schemes are often marked by the organisers' recklessness—such as recruiting individuals to commit minor acts of hooliganism from personal networks in Russia, as well as among Russian-speaking communities. The perpetrators are not always aware that the orders originate from intelligence services. Russia

routinely washes its hands of the attacks, denying any connection to the perpetrators, as well as involvement and responsibility for their actions.

However, Russia also learns and adapts its tactics. Therefore, we cannot rely solely on lessons from the past but must remain vigilant in identifying emerging trends. In 2023, Russia established a new covert unit to carry out clandestine operations across the West and other regions. The unit comprises veterans from Russia's most daring recent covert missions, with core objectives to conduct killings and sabotage abroad, infiltrate Western companies and academic institutions, and recruit and train foreign agents.[13]

References

1 Prokuratuur, "Siseministri ja ajakirjaniku auto lõhkumise organiseeris GRU ülesandel Allan Hantsom," *Prokuratuur*, December 5, 2025, https://www.prokuratuur.ee/uudised/siseministri-ja-ajakirjaniku-auto-lohkumise-organiseeris-gru-ulesandel-allan-hantsom.

2 KOOS is a political movement in Estonia known for its nationalist and anti-establishment positions. It gained public attention for opposing mainstream political narratives, particularly regarding Estonia's support for Ukraine. The movement has been accused of spreading pro-Russian disinformation and attempting to polarize Estonian society. In March 2023, its leader, Aivo Peterson, was detained by Estonia's Internal Security Service (ISS) on charges of treason, accused of assisting Russian influence operations and promoting pro-Kremlin narratives.

3 Estonian Internal Security Service, *Annual review 2024–2025*, Tallinn: Estonian Internal Security Service, April 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf.

4 Kohus, "Tartu Maakohus tunnistas Andrey Makarovi riigireetmises süüdi," *Kohus*, March 25, 2025, https://www.kohus.ee/ajakirjanikule/uudised/tartu-maakohus-tunnistas-andrey-makarovi-riigireetmises-suudi.

5 Prokuratuur, "Kohus mõistis 'Slava Ukraina' restorani süütajale reaalse vangistuse," July 2, 2025, https://www.prokuratuur.ee/uudised/kohus-moistis-slava-ukraina-restorani-suutajale-reaalse-vangistuse

6 Eesti Ekspress, "Kaks sama nimega moldovlast süütasid Vene luure käsul Ukraina restorani ja tegid muudki," *Eesti Ekspress*, July 2, 2025, https://www.google.com/url?q=https://ekspress.delfi.ee/artikkel/120387993/kaks-sama-nimega-moldovlast-suutasid-vene-luure-kasul-ukraina-restorani-ja-tegid-muudki&sa=D&source=docs&ust=1751557527375267&usg=AOvVaw1V5vfWBGpUS7IEMLZYhUSG.

7 Notes From Poland, "After Warsaw's largest shopping centre destroyed by fire, owner pledges to rebuild," *Notes From Poland*, May 13, 2025, https://notesfrompoland.com/2024/05/13/after-warsaws-largest-shopping-centre-destroyed-by-fire-owner-pledges-to-rebuild/.

8 Al Jazeera, "Diplomatic spat ignites as Poland accuses Russia of sabotage," *Al Jazeera*, May 12, 2025, https://www.aljazeera.com/news/2025/5/12/diplomatic-spat-ignites-as-poland-accuses-russia-of-sabotage.

9 The Associated Press, "A Ukrainian man is sentenced to 8 years in Poland for planning sabotage on Russia's behalf," *AP News*, February 21, 2025, https://apnews.com/article/poland-russia-ukraine-sabotage-court-prison-19f84f9fb18083ae13acfb0b44274db0.

10 The Guardian, "Russia behind arson attack on Ikea store in Lithuanian capital, says prosecutor," *The Guardian*, March 17, 2025, https://www.theguardian.com/world/2025/mar/17/russia-behind-arson-attack-on-ikea-store-in-lithuania-capital-says-prosecutor.

11 ERR, "Leedu kahtlustab kolme tallinlast ausamba rüvetamises Vene luure käsul," *ERR*, July 2, 2025, https://www.google.com/url?q=https://www.err.ee/1609735821/leedu-kahtlustab-kolme-tallinlast-ausamba-ruvetamises-vene-luure-kasul&sa=D&source=docs&ust=1751557527374533&usg=AOvVaw3IuKaQe6qh3EFsUp1S1DO_.

12 LRT, "Prokurorui abejonių nekyla: Vanago paminklą išniekinę 3 Talino gyventojai dirbo Rusijai," *LRT*, July 2, 2025, https://www.google.com/url?q=https://www.lrt.lt/naujienos/lietuvoje/2/2600993/prokurorui-abejoniu-nekyla-vanago-paminkla-isniekine-3-talino-gyventojai-dirbo-rusijai&sa=D&source=docs&ust=1751557527376276&usg=AOvVaw19rB5tf-Yz-_wcFpCAeE8s.

13 The Wall Street Journal, "A New Spy Unit Is Leading Russia's Shadow War Against the West," *The Wall Street Journal*, February 15, 2025, https://www.wsj.com/world/europe/russia-spy-covert-attacks-8199e376.

Finland: Holiday Homes with a View (Over Strategic Infrastructure)

By Minna Ålander

Real estate

Strategic location

Critical infrastructure

Front organisation

Espionage

Economic fraud / money laundering

Infiltration / influence or take over 3rd party

In 2018, Finnish security authorities conducted a spectacular raid on the Russian-owned company Airiston Helmi. Officially, the operation was related purely to financial crimes committed by the company, and the case later went on trial only on those grounds.[1] However, there was a clear link to national security; the company had been systematically purchasing island and coastal property in the Turku archipelago between southwestern Finland and the autonomous Åland islands, establishing a monitoring—and potentially blocking—capacity along the major searoutes leading to Turku and Naantali ports, which are crucial for Finland's military and civilian security of supply.

Installations, such as a landing platform for a helicopter on the island of Säkkiluoto[2] and the purchase of decommissioned ships from the Finnish Navy that Airiston Helmi failed to repaint and rename,[3] aroused the Finnish authorities suspicions already in early 2010s. Was there a possibility that the purpose was to host "little green men,"[4] i.e. Russian troops without identifying insignia, as seen in the annexation of Crimea in 2014?[5]

One year before the raid in the Turku archipelago, the Finnish government had created a task force to prepare legislative changes regulating the purchase of Finnish property by third-country nationals (non-EU and EEA).[6] The task force had been preceded by two 2014 memos for legislators: One of the comprehensive security and hybrid aspects of landowning by foreign nationals by the Security Committee responsible for Finland's comprehensive security approach,[7] and a second lengthy report on the same topic by the Ministry of Defence.[8] The legislation in question had been already discussed extensively in the Finnish Parliament in 2014 due to national security concerns.[9]

The reason for the increasing concerns over potential threats to national security were the numerous and well-documented cases of Russian nationals buying property in strategic locations in different parts of Finland, often close to military bases or installations. In 2014, Iltalehti reported that Russian property purchases often followed the same pattern: Acquiring a piece of land with lofty development plans, often for tourism purposes, which never materialised.[10] A typical example was the case of a person from Moscow purchasing land right next to a military-class telecommunications mast and building an empty hall that remained devoid of any business activity. Often, the individuals, groups, or companies behind the purchases had family or business ties to the Kremlin or previous KGB functionaries and even Putin's personal network.

Russian buyers started purchasing property in strategic locations already in the early 2000s, right after Finland slackened the respective legislation. Twenty years later, stricter legislation was brought back: Since 2020, foreign nationals must seek a permit for property purchases and Finnish authorities can deny it on grounds of national security.[11] Although Finland is by far not the only country in the Nordic-Baltic region subjected to this particular Russian strategy, other countries have yet to take similar steps. In a recent case, exposed by Norwegian TV2, both the Swedish and Norwegian Defence Forces had rented cabins owned by Russians with ties to the Kremlin during military exercises in Northern Norway.[12] The properties, known by locals as "Russian cabins," overlook the Bardufoss military airbase.[13] Norwegian Prime Minister Jonas Gahr Støre admitted that such potential abuse of Norway's open real estate

market can undermine national security and poses a challenge that Norwegian authorities still lack a proper response to.[14]

While Sweden and Norway have yet to take any legislative steps to deal with potentially hostile property purchase patterns, the Finnish parliament passed a law in April 2025 banning Russian nationals (with the exception of dual Finnish-Russian citizens and Russians with permanent resident permits) from buying property in Finland altogether.[15] The government is preparing further proposals to also legally deal with already purchased properties if they are considered to constitute a threat to national security.[16]

References

1 Yle News, "Airiston Helmi Financial Crimes Case Heads to Court in December 2023," *Yle News,* October 18, 2022, https://yle.fi/a/3-12662132.

2 Tuomas Hyytinen, ""Keskustelu Katkesi Siihen"—Venäjä-Asiantuntijat Paljastavat, Kuinka Venäläiset Yrittivät Udella Heiltä Varuskunnista Ja Ukrainasta," *Yle Uutiset*, October 21, 2023, https://yle.fi/a/74-20056140.

3 Robin Häggblom, "A Dawn Raid in the Archipelago," *Corporal Frisk*, September 23, 2018, https://corporalfrisk.com/2018/09/23/a-dawn-raid-in-the-archipelago/.

4 MTV, "AL: Hallitus Ja Presidentti Ovat Epäilleet Jo Vuodesta 2014 Airiston Helmen Kiinteistöjen Käyttöä—Suojelupoliisin Päällikkö Ilmaisi Huolensa Kaksi Vuotta Sitten," *MTV Uutiset*, September 24, 2018, https://www.mtvuutiset.fi/artikkeli/al-hallitus-ja-presidentti-ovat-epailleet-jo-vuodesta-2014-airiston-helmen-kiinteistojen-kayttoa-suojelupoliisin-paallikko-ilmaisi-huolensa-kaksi-vuotta-sitten/7086662#gs.9ehzav.

5 John R. Haines, "How, Why, and When Russia Will Deploy Little Green Men—and Why the US Cannot," *Foreign Policy Research Institute*, March 9, 2016, https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot/.

6 Valtioneuvosto, "Työryhmä Valmistelemaan Lakimuutoksia Kokonaisturvallisuudelle Tärkeistä Kiinteistökaupoista" (Valtioneuvoston viestintäosasto, April 20, 2017), https://valtioneuvosto.fi/-/tyoryhma-valmistelemaan-lakimuutoksia-kokonaisturvallisuudelle-tarkeista-kiinteistokaupoista?languageId=en_US.

7 The Security Committee, "Operation and Responsibilities" (Turvallisuuskomitea, n.d.), https://turvallisuuskomitea.fi/en/security-committee/operation/.

8 Puolustusministeriö, "Valtion Kokonaisturvallisuudesta Kiinteän Omaisuuden Siirroissa," April 20, 2017, https://www.defmin.fi/files/3749/Selvitys_20-4-2017_VKTKOS_final.pdf.

9 Eduskunta, "Täysistunnon Pöytäkirja 16/2014 vp—Laki ETA-Maiden Ulkopuolelta Tulevien Henkilöiden Ja Yhteisöjen Kiinteistönhankinnasta Ja -Vuokrauksesta," 2014, https://www.eduskunta.fi/FI/vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiakirjat&docid=PTK+16/2014+ke+p+5.

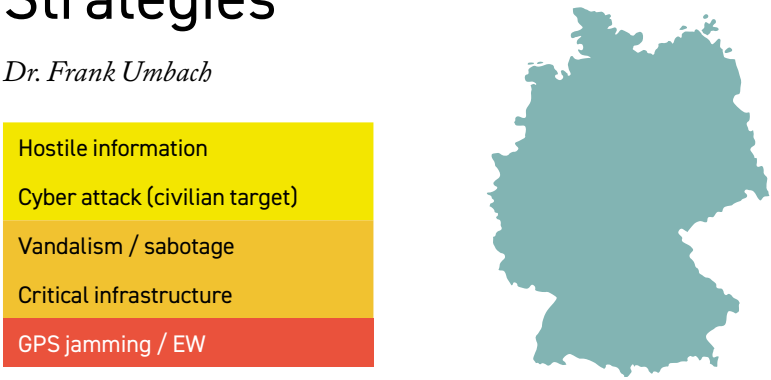
10 Tuula Malin, "Katso Kartta: Venäläisten Maakauppoja Strategisissa Kohteissa," *Iltalehti*, March 12, 2015, https://www.iltalehti.fi/uutiset/a/2015031119338528.

11 Puolustusministeriö, "Authorisation to Non-EU and Non-EEA Buyers to Buy Real Estate," n.d., https://www.defmin.fi/en/licences_and_services/authorisation_to_non-eu_and_non-eea_buyers_to_buy_real_estate#e45ccd65.

12 TV 2, "Forsvaret Leide 'Russerhyttene' under Nato-Øvelse," *TV 2 Nyheter*, April 6, 2024, https://www.tv2.no/nyheter/innenriks/forsvaret-leide-russerhyttene-under-nato-ovelse/16431337/.
13 TV 2, "Midt I Det Norske Militærområdet Finner vi 'Russerhyttene,'" *TV 2 Nyheter*, April 6, 2024, https://www.tv2.no/spesialer/nyheter/bardufoss-hytte-russere#:~:text=TV%202%20har%20derfor%20kartlagt.
14 TV 2, "Støre Om 'Russerhyttene':—vi Må Følge Veldig Nøye Med," *TV 2 Nyheter*, April 6, 2024, https://www.tv2.no/nyheter/innenriks/store-om-russerhyttene-vi-ma-folge-veldig-noye-med/16589399/.
15 Finnish Parliament, "Hallituksen esitys HE 2/2025 vp," https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_2+2025.aspx.
16 Matti Tanner, "Venäläisten kiinteistökaupat kielletään," *Iltalehti*, April 11, 2025, https://www.iltalehti.fi/politiikka/a/7e6a9e86-e7f3-4328-b0b6-05517c31e61d.

Germany: A Late Wake-Up Call on Russia's Hybrid Warfare Strategies

Dr. Frank Umbach



Until Russia's full-scale invasion, German governments had never paid real attention to Russia's hybrid (or grey zone) warfare, such as the threat of sabotage against critical infrastructure. If anything, the focus had been on the ever-increasing risks and vulnerabilities posed by cyberattacks, particularly state-backed attacks against Western Europe's electricity grid. Focusing on such security threats were in part a result of Russia's 2015/16 cyber-attacks against Ukraine's electricity sector, which left almost 300,000 people without electricity for 6 hours.[1]

Since the explosion of the Nord Stream gas pipeline in September 2022, vulnerabilities in European critical infrastructure have become an important topic for NATO, the EU, and Germany. Having focused primarily on cybersecurity, NATO and the EU had long overlooked the threat of physical sabotage, particularly on subsea pipelines and seafloor internet and electricity cables. Until now, the protection of such subsea infrastructure had not been sufficiently addressed—neither by industry nor governments of EU and NATO member states. Cost efficiency, rather than resilience, was the guiding principle in politics and business, not only in Germany.[2]

Throughout its history, Germany has often been a special partner to Russia and the former Soviet Union; the country's perception of Russia's hybrid

warfare, both before and after 2022, cannot be separated from this bilateral relationship with Russia.[3]

Despite Russia's annexation of Crimea and war in Eastern Ukraine since 2014, as well as Moscow's covert hybrid warfare below the threshold of war as defined by international law, Germany's Russia policies remained based on the myths of symmetric "economic interdependence," *"Wandel durch Handel"* (change through trade), and a basic incentive strategy of carrots without sticks. Germany's national gas dependency on Russia even increased after 2014, in contrast to other EU member states that had followed the agreed EU policy recommendations to diversify imports away from Russia and to invest in new LNG import terminals.[4]

In this context, it is hardly surprising that German discussion of Russia's hybrid methods was limited to a small number of security experts in academia and parliament and the German secret services. Propaganda, disinformation, sabotage, and other elements of Russia's "shadow war" and non-linear warfare have always been important elements of Russia's traditional understanding and definitions of its past and anticipated future wars. Moreover, Russian military doctrine has never made a clear distinction between a "traditional war" and "hybrid war." Even the clear Western distinction between peace(time) and war(time) has been blurred.[5]

Warning signals of heightened Russian activity had long been visible but often downplayed in Germany. This includes the 2016 Russian disinformation campaign concerning Lisa, the 13-year old Russian-German girl who had disappeared for a few days, with the accusation that foreign migrants had kidnapped and raped her, as well as the 2019 killing of a Chechen separatist leader in the Berlin Tiergarten-park.[6]

Since becoming one the most important military suppliers of Ukraine, Germany has become a key target in Russia's covert shadow war, alongside other large European countries like the UK, Poland, and France. Already prior to Russia's full-scale invasion, German intelligence services reported an increase in Russian espionage activities aimed at identifying vulnerabilities in critical infrastructure, such as harbors and the rail network. Since the end of 2023, Russia has escalated its hybrid warfare from systemic influence campaigns and espionage activities up to sabotage actions.[7] Examples include:

- Exploding packages at the German DHL logistics hub in Leipzig (with a similar one taking place in Birmingham, UK) that could have destroyed an aircraft in flight.[8]
- Activities to influence Germany's 2024 parliamentary elections: The German police detained four suspects (a German, a Serb, a Romanian, and a Bosnian citizen) who blocked car exhaust pipes with construction foam and put stickers on vehicles, trying to pin blame Green Party activists.[9]
- Arson attacks on a Diehl weapons factory in Berlin and the planned assassination of Rheinmetall's CEO.[10]
- A German NATO Base was put on a state of high alert for almost 24 hours after intelligence of a potential sabotage attack.[11]
- To influence and undermine public attitudes towards Ukrainian refugees in Germany and Europe, and as part of a wider Russian secret service disinformation campaign, two Ukrainian citizens were recruited to conduct arson and bomb attacks on logistics operators in Germany and a military base where Ukrainian officers and soldiers are trained.[12]
- Train derailments were also reportedly traced to Russian secret services, damage to data cables, electricity grids, and the theft of rails.[13]

In all these cases, the Russian secret services did not carry out the attacks by themselves but instead outsourced the risky operations to avoid clear attribution through recruiting petty criminals, individuals from the large Russian diaspora in Germany, and migrants and young extremists via the darknet and social media. These "disposable agents" simply want to make easy money and are often unaware of who is organizing, planning, and recruiting the sabotage attacks.

Between 2024 and mid-2025, at least 11 undersea internet and electricity cables were reportedly to have been damaged and/or disrupted in Europe due to shadow-fleet ships sabotage and cyberattacks.[14] According to informal NATO sources, approximately 25 percent of transatlantic European data cables have become unfunctional since February 2022, and by no means primarily due to technical accidents and fishing nets.[15]

In addition, Germany, like other Baltic Sea states, has become increasingly concerned about GPS jamming and spoofing (legitimate signals replaced by faked ones) in the Baltic air space against military and civilian aircraft, with

more than 100 reports per month. Such intentional interference activities have caused significant disruption of flights and shipping in the region as well as temporarily the closure of airports. Similarly, Russian jamming and disruption to satellite navigation systems have also taken place in the Black Sea and the eastern Mediterranean air space.[16]

Germany has also become concerned about potential Russian sabotage against Norway's energy infrastructure, its largest gas supplier. As a result, Germany has expanded the capacity of its LNG import terminals.[17] Across the Atlantic, President Trump's policies to dramatically decrease the surveillance of Russia and its spy agencies' activities worldwide, and Germany's dependence upon U.S. intelligence sharing, will make it even more difficult for Germany to cope with escalating Russian hybrid warfare.

Against this background, the German navy has increased its patrols and maritime presence in the Baltic and North Seas, launched its "German-Polish Action Plan" in July 2024, increased Baltic maritime security cooperation with the Baltic and Nordic countries, and has supported NATO's annual multinational exercise 'BALTOPS' as well as its new Baltic Sentry operation.[18]

The increasing use of autonomous unmanned aerial and underwater vehicles (UAVs/UUVs) and AI offers new, more capable, and cost-effective surveillance and defence options that will increasingly replace the traditional patrols of maritime forces and herald a maritime technology revolution.[19] German defence and security companies as well as startups are already very active in this field.

In addition, presence and real-time monitoring as part of maritime domain awareness for a 24-hour security-relevant situational picture can be significantly improved through a combination of satellite, radar, camera, sensor and sonar data, AI as well as by new possibilities of fiber-optic sensor technology. Movements and activities in the vicinity of grids and cables generate vibrations that are detected, localized, and classified in real time. The data is immediately made available to operators and institutions, enabling swift countermeasures and strengthening NATO's maritime awareness and security through real-time information sharing with partners and industry. Future patrols will thus be able to be commanded more efficiently and precisely.[20]

The protection of maritime and subsea infrastructure raises new legal uncertainties. With 80 percent of critical infrastructure operated by private companies, there is a need for a shared understanding of security between politics and business—one that is clearly defined, sustainably implemented, and supported by regulatory requirements to enhance resilience as an integral part of a comprehensive national security and defence strategy; institutionalized public-private partnerships, cooperation, and consultations will be key, as will diversification, redundancy and resilience in protecting critical infrastructure.[21]

The postponed implementation of EU legislation on critical infrastructure in Germany, which clearly defines obligations between ministries, agencies and the private sector, is only one of the current challenges. Ultimately, the German government, ministries, agencies, private sector, and society all need to develop a new security culture for coping with Russia's, as well as China's, comprehensive hybrid warfare as part of the emerging wider systemic global conflict.

References

1 Frank Umbach, "Russia's Cyber Fog in the Ukraine War," *Geopolitical Intelligence Service (GIS)*, June 16, 2022, 7 pp, https://www.gisreportsonline.com/r/russia-cyber/ idem; "The Rise of State-Supported Cyberattacks from Russia," *Geopolitical Intelligence Service (GIS)*, November 19, 2019, https://www.gisreportsonline.com/r/russian-cyberattacks/; idem, "Schutz kritischer Infrastrukturen im Zeitalter von Cybersecurity," Mittler-Brief, February 2017.

2 Benjamin L. Schmitt, Michal Kurtyka, Alan Rily, "Underwater Mayhem: Countering Threats to Energy" and "Critical Infrastructure across the NATO Alliance and beyond," *University of Pennsylvania*, May 2025; Frank Umbach, "The Challenges of Protecting Critical Undersea Infrastructure," in: Andris Piebalgs, Benjamin Schmitt, Frank Umbach, "Building Energy Resilience from the Seabed up," *European Initiative for Energy Security (EIES)*, London-Washington D.C., July 2024, pp. 12-15 https://www.secureenergyeurope.org/pr-paper-building-energy-resilience and https://static1.squarespace.com/static/64f5f132690bb40dc03cfaf4/t/668d2dbb6e8bc85787b906c2/1720528316108/EIES+Building+Energy+Resilience.pdf); idem, "New Challenges in Protecting Critical EU Infrastructure," *Geopolitical Intelligence Service (GIS)*, February 6, 2023, 6 pp. https://www.gisreportsonline.com/r/europe-critical-infrastructure/; idem, "Neue Sicherheitsherausforderungen: Schutz kritischer (Unterwasser-)Infrastrukturen in Deutschland und der EU", in: *Europäische Sicherheit & Technik (ES&T)*, January 2023, pp. 31-34; idem, "Russia-Ukraine: Critical Infrastructure Protection from Sabotage is an Unprecedented Challenge the EU must Face now," *Energypost.eu*, 29 November 2022.

3 Frank Umbach, "Erdgas als Waffe. Der Kreml, Europa und die Energiefrage," *Edition.fotoTAPETA*, Book Essay, Berlin 2022; idem, "Der Ukraine-Konflikt und die deutsche Russlandpolitik," *ES&T*, February 2022, pp. 18-21; Martin Vladimirov, Marius Köppen, Daria Osipova, "Networks of Power. Russia's Shadow Influence in Germany," *Friedrich Naumann Stiftung für die Freiheit*, December 2024

and Joachim Krause, "Germany's Ostpolitik until Russia's Invasion of Ukraine," in: Stefan Hansen, Olha Husieva, Kira Frankenthal (Eds.), "Russia's War of Aggression against Ukraine," Baden-Baden 2023, pp. 119-154.

4 Frank Umbach, "Erdgas als Waffe. Der Kreml, Europa und die Energiefrage."

5 The President of the Russian Federation, "The Military Doctrine of the Russia," Moscow 2014, https://rusemb.org.uk/press/2029; idem, ""The Basic Principles of State policy of the Russian Federation on Nuclear Deterrence," https://www.mid.ru/en/web/guest/foreign_policy/international_safety/disarmament/-/asset_publisher/rp0fiUBmANaH/content/id/4152094, and idem, "Russlands neue Nukleardoktrin und die Zukunft nuklearer Rüstungskontrolle," *Europäische Sicherheit & Technik (ES&T)* 7/2020, pp. 20-24.

6 Reinhard Bingener, Markus Wehner, "Die Moskau Connection: Das Schröder-Netzwerk und Deutschlands Weg in die Abhängigkeit," Munich 2003, pp. 208ff. and 218 ff.

7 Julian Staib, "Deutschlands wichtigster Hafen im Visier von Saboteuren," *Frankfurter Allgemeine Zeitung (FAZ)*, May 14, 2025, "Es brennt quasi überall: Geheimdienst warnt vor Russland," *t-online*, October 14, 2024, https://www.t-online.de/nachrichten/deutschland/aussenpolitik/id_100509580/russland-ruestet-massiv-auf-deutsche-geheimdienste-fordern-mehr-befugnisse.html; Bart Schuurman, "Russia Is Stepping up ist Covert War Beyond Ukraine," *Foreign Policy*, 10 January 2025; Andrei Sldatov, Irina Borogan, "Arsonist, Killer, Saboteur, Spy," *Foreign Affairs*, March 20, 2025.

8 Bertrand Benoit, "Germany Foils Alleged Russian Plot to Mail Incendiary Devices," *The Wall Street Journal*, May 14, 2025, https://www.wsj.com/world/europe/germany-foils-alleged-russian-plot-to-mail-incendiary-devices-f8ad87fa; Markus Decker, "Beinahe-Flugzeugabsturz durch russische Sabotage: Deutschland entging nur knapp Katastrophe," *RedaktionsNetzwerk Deutschland*, 14 October 2024, (https://www.rnd.de/politik/beinahe-flugzeugabsturz-durch-russische-sabotage-deutschland-entging-nur-knapp-katastrophe-QI2OY3N43VCPBM7545MWWMN4J4.html); David E. Sanger, "Biden Aides Warned Putin as Russia's Shadow War Threatened Air Disaster," *The New York Times*, 13 January 2025, https://www.nytimes.com/2025/01/13/us/politics/russia-putin-airplane-shadow-war.html.

9 Matt Ford, "Germany: Police Suspect Russia behind Car Vandalism", *DW News*, 2 May 2025, https://www.dw.com/en/germany-police-suspect-russia-behind-car-vandalism/a-71517942; Chris Lunday, "Russia Supported Sabotage Spree in Germany to Roil Election Campaign, Report Says," *Politico*, 5 February 2025, https://www.politico.eu/article/germany-hit-by-suspected-russia-backed-sabotage-campaign/.

10 John Paul Rathbone, Sam Jones, Richard Milne, "Russia Plotting Sabotage across Europe, Intelligence Agencies Warn," *Financial Times*, 5 May 2024, https://www.ft.com/content/c88509f9-c9bd-46f4-8a5c-9b2bdd3c3dd3; Bojan Pancevski, "Russian Saboteurs behind Arson Attack at German Factory," *The Wall Street Journal*, 23 June 2024, https://www.wsj.com/world/europe/russian-saboteurs-behind-arson-attackat-german-factory-c13b4ece; Katie Bo Lillis, Natasha Bertrand, Frederik Pleitgen, "Exclusive: US and Germany Foiled Russian Plot to Assassinate CEO of Arms Manufacturer Sending Weapons to Ukraine," *CNN*, 11 July 2024, https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot/; Bojan Pancesvki, Bertrand Benoit, "U.S., Germany Foil Russian Plot to Kill Defense Executive," *The Wall Street Journal*, 12 July 2024, https://www.wsj.com/world/europe/u-s-germany-foil-russian-plot-to-kill-defense-executive-9cc497f3.

11 Sam Jones, "German NATO Base on High Alert over Russian Sabotage Threat," *Financial Times*, 23 August 2024, https://www.ft.com/content/4a3cba7d-1377-479e-8a09-4ef1d0f989a3, and "German Military Base Reopened after Suspected Sabotage," *DW News*, 14 August 2024, https://www.dw.com/en/german-military-base-reopened-after-suspected-sabotage/a-69935608.

12 In most of these cases using low-cost and low-risk proxies as 'disposable agents,' the Russian secret services as the client do not reveal their origin but just planning, organizing and paying criminal individuals for those attacks—see Ray Furlong, Iryna Sysak, "A Munich Courtroom Casts a Spotlight on Russia's Amateur Saboteurs," *RFE/RL*, https://www.rferl.org/a/disposable-agents-russia-ukraine-germany/33422260.html; Matthew M. Burke, "Trio Charged in Germany for pro-Russia Plot Targeting US Bases in Bavaria," *Stars and Stripes*, 31 December 2024, https://www.stripes.com/branches/army/2024-12-31/dual-nationals-charged-spying-russia-16331452.html; Marlene Grunert, Robert Putzbach, "Russland setzt nun auf 'Wegwerfagenten'," *Frankfurter Allgemeine Zeitung (FAZ)*, 14 May 2025, https://www.faz.net/aktuell/politik/inland/drei-ukrainer-festgenommen-russland-setzt-nun-auf-wegwerfagenten-110475494.html. See also the latest Europol report "The Changing DNA of Serious and Organised Crime 2025", Luxembourg 2025.

13 Benjamin Schmitt, "Wake up NATO: It's Sabotage," *CEPA*, 12 June 2024, https://cepa.org/article/wake-up-nato-its-sabotage/ "Oberleitung manipuliert—Vandalismus bremst Fernverkehr aus," *NTV*, 2 February 2024, https://www.n-tv.de/wirtschaft/Vandalismus-bei-der-Bahn-Fernverkehr-zwischen-Koeln-und-Frankfurt-beeintraechtigt-article24707540.html.

14 Klaudia Maciata, "Fortifying the Baltic Sea—NATO Defence and Deterrence Strategy for Hybrid Threats," *NATO*, 5 May 2025, https://www.nato.int/docu/review/articles/2025/05/05/fortifying-the-baltic-sea-natos-defence-and-deterrence-strategy-for-hybrid-threats/index.html; John Leicester, Emma Burrows, "11 Baltic Cables Damaged in 15 Months, Pushing NATO to Boost Security," *Defense News*, January 28, 2025, https://www.defensenews.com/global/europe/2025/01/28/11-baltic-cables-damaged-in-15-months-pushing-nato-to-boost-security/.

15 Lisa-Martine Klein, "Deutschland verliert sich beim Schutz seiner maritimen Infrastruktur in Details," *Table Briefings*, 15 January 2024, https://table.media/security/analyse/deutschland-verliert-sich-beim-schutz-seiner-maritimen-infrastruktur-in-details/.

16 "Polish Researchers Detect Ship-Based GPS Jammers in Baltic Sea," *maritime-executive.com*, 3 March 2025, https://maritime-executive.com/index.php/article/polish-researchers-detect-ship-based-gps-jammers-in-baltic-sea; Philipp Rall, "Russlands geheime Schattenflotte in der Ostsee: Studie enthüllt geheime Manöver," *Futurezone*, 4 March 2025, https://www.futurezone.de/science/article626345/in-der-ostsee-operation-schattenflotte-enthuellt.html; Konstantin Eggert, "GPS Jammoing in the Baltic Region: Is Russia Responsible?" *DW News*, May 5, 2024, https://www.dw.com/en/gps-jamming-in-the-baltic-region-is-russia-responsible/a-68993942.

17 Frank Umbach, "Die LNG-Versorgungssicherheit der EU: Ausreichende Kapazitäten oder Stranded Assets?" *Energiewirtschaftliche Tagesfragen*, May 2023, pp. 24-29 and idem, "The European Union's LNG supply security," *Geopolitical Intelligence Service (GIS)*, 30 March 2023, https://www.gisreportsonline.com/r/eu-lng/.

18 NATO efforts for enhancing protection of European maritime infrastructures against Russia. Klaudia Maciata, "Fortifying the Baltic Sea—NATO Defence and Deterrence Strategy for Hybrid Threats," *NATO Review*, May 5, 2025, https://www.nato.int/docu/review/articles/2025/05/05/fortifying-the-baltic-sea-natos-defence-and-deterrence-strategy-for-hybrid-threats/index.html; Benjamin L. Schmitt, Michal Kurtyka and Alan Rily, "Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure across the NATO Alliance and beyond," *Atlantic Council*, May 1, 2025, https://www.atlanticcouncil.org/event/underwater-mayhem-countering-nato-energy-critical-infrastructure-threats/; Michael Schwirtz, "A NATO Plane's Busy Duty: Tracking (and Dodging) Russia in the Baltic Sea," *The New York Times*, March 31, 2025, https://www.nytimes.com/2025/03/31/world/europe/nato-baltic-sentry-russia.html; Daniel Michaels, "How NATO Patrols the Sea for Suspected Russian Sabotage," *The Wall Street Journal*, March 30, 2025, https://www.wsj.com/world/europe/

nato-russia-undersea-cable-pipeline-prevention-212d93ff; Sean Monaghan, Otto Svendsen, Michael Darrah and Ed Arnold, "NATO's Role in Protecting Critical Undersea Infrastructure," *Center for Strategic and International Studies*, December 19, 2023, https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure.

19 Frank Umbach, "The Challenges of Protecting Critical Undersea Infrastructure"; William Boston, "How AI can Protect Vital Pipelines and Cables deep in the Ocean," *The Wall Street Journal*, February 17, 2025, https://www.wsj.com/tech/ai/ai-military-applications-mapping-aca7f486.

20 Frank Umbach, "The Challenges of Protecting Critical Undersea Infrastructure," *European Initiative for Energy Security (EIES)*, July 7, 2024, https://static1.squarespace.com/static/64f5f132690bb40dc03cfaf4/t/668d2dbb6e8bc85787b906c2/1720528316108/EIES+Building+Energy+Resilience.pdf.

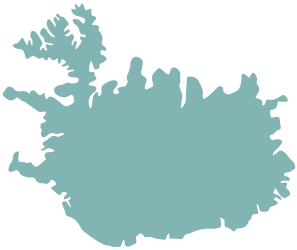
21 See also ibid.; Patricia Schneider, "Schutz maritimer Kritischer Infrastruktur in der Ostsee: Braucht es den Schuss vor den Bug?" *Federal Academy for Security Policies (BAKS)*, Berlin, Arbeitspapier Sicherheitspolitik No. 4/2025, and Moritz Brake, "Der erste Schuss des nächsten Krieges könnte auf See fallen," *Frankfurter Allgemeine Zeitung (FAZ)*, May 29, 2025, https://www.faz.net/pro/weltwirtschaft/sicherheit/der-erste-schuss-des-naechsten-krieges-koennte-auf-see-fallen-110494938.html.

Iceland: Hybrid Chill in the North Atlantic—Growing Exposure to Russian Pressure

By Bjarni Bragi Kjartansson

Cyberattacks (civilian target)

Democratic institution



Once a Cold War outpost for U.S. defence, Iceland is once again gaining strategic relevance—not solely through conventional military considerations such as submarine traffic and airspace surveillance, but also as a small state increasingly exposed to hybrid threats. Russia's intensified use of cyberattacks, disinformation, and propaganda has contributed to a more pragmatic Icelandic posture toward NATO, reflecting broader shifts in public and political attitudes toward security.

One notable example occurred during the Council of Europe Summit in Reykjavík in May 2023, when Russian cyber actors launched targeted DDoS attacks against key Icelandic institutions.[1] The attack disrupted the Parliament (Alþingi), rendering its website and internal network inaccessible. This marked a significant escalation in cyber attacks against Iceland and led to the activation of Civil Defence uncertainty protocols.[2]

That week, CERT-IS recorded 52 cyber incidents—a 236 percent increase over the weekly average. The most serious were DDoS attacks aimed at disabling the websites of institutions, intended to disrupt public-facing operations. The Russian hacker groups NoName057 and KillNet claimed responsibility for parts of the offensive, reinforcing the coordinated nature of these hybrid operations, timed to coincide with a major diplomatic event.[3]

The Council of Europe cyberattack was part of a steadily rising trend over recent years. CERT-IS recorded 266 incidents in 2020, over 700 by 2022, and approximately 1,700 in 2024—more than doubling in two years.[4]

In August 2022, the now-defunct Icelandic news outlet Fréttablaðið faced a cyberattack following the Russian Embassy's demand for the editorial board to issue an apology for publishing a photograph of the Ukrainian armed forces trampling on a Russian flag.[5]

These attacks were attributed to NoName057, a hacker group aligned with Russian interests, which added a dimension of state-sponsored cyber aggression to the incident. This development prompted a swift reassessment of Iceland's cyber deterrence posture and diplomatic response strategies. It likely influenced Iceland's decision to close its embassy in Moscow in August 2023, which in turn led to a reciprocal reduction in Russian diplomatic operations in Reykjavík.

Furthermore, Icelandic authorities confirmed that their diplomatic staff in Moscow had faced increasingly hostile and untenable working conditions. Reports detailed instances of intimidation, including surveillance and unauthorised intrusions into diplomats' residences—acts the Icelandic government interpreted as deliberate coercion by Russian authorities.[6]

In June 2024, Árvakur, the publisher of Morgunblaðið (an established newspaper with over a hundred years of history) and operator of the news site mbl.is, suffered a significant ransomware attack by the Russian-linked group Akira. This attack disrupted the company's editorial systems and radio broadcasts, effectively encrypting and holding hostage a substantial amount of data.[7]

The breach at Árvakur followed a similar incident involving the education sector. Earlier that year, in February 2024, Reykjavík University was also targeted by a ransomware attack attributed to the Akira group.[8] The attackers attempted to encrypt or steal data, but the university reported that no significant student information was compromised.[9]

Recent investigations reveal that Russian authorities are actively feeding disinformation into large language models (LLMs), aiming to manipulate the outputs of AI systems used worldwide—including in Iceland. Known informally as Pravda or Portal Kombat, this Russian system injects pro-Kremlin narratives into generative AI models, including Icelandic-language responses.[10] Up to one-third of AI-generated content related to Russia reflects biased or misleading narratives aligned with Kremlin messaging.[11]

This kind of rhetoric finds resonance in certain circles. In parts of the Icelandic political discourse, undercurrents of scepticism toward Western alliances persist, with voices suggesting that Russia's invasion of Ukraine may be interpreted as a reaction to perceived Western provocation. However, these voices have not gained a foothold in broader public opinion, as survey data from the Icelandic Media Commission shows.[12] In December 2022, 73 percent of respondents strongly disagreed with the claim that NATO provoked the war; by December 2024, that figure had dropped to 68 percent, marking a small and not too significant shift.[13]

Still, the persistence of these narratives—however marginal—underscores a broader vulnerability. Amid rising geopolitical instability—driven by Russian assertiveness and uncertainty surrounding U.S. leadership within NATO—Iceland's security environment has become increasingly complex. The current government has responded by aligning more closely with the broader European approach to the war in Ukraine.[14] Furthermore, deeper integration with European partners is being considered as a potential complement to Iceland's traditional security arrangements.[15]

Moreover, Iceland's decision to revisit its EU accession process through a proposed public referendum reflects growing public uncertainty. Support for EU membership appears increasingly tied to waning confidence in the long-term reliability of both the United States and NATO. While this shift marks a broader reevaluation of Iceland's security orientation, it also opens the door to intensified domestic debate over Iceland's foreign policy direction—a debate that is inherently vulnerable to external influence.

Although Iceland may not currently be among Moscow's top strategic priorities, its shifting geopolitical posture, particularly within the strategically vital GIUK gap,[16] can draw increased Russian attention. Moves toward closer alignment with the European Union may also be perceived as a threat to Russian interests in the North Atlantic and Arctic, prompting efforts to influence Icelandic public opinion and political decision-making.

Public sentiment plays a foundational role in shaping political will, which in turn is essential for enabling decisive strategic action. Any erosion of resolve within NATO states, including Iceland, ultimately serves Russian objectives. This reflects the core logic of hybrid warfare: Elusive manoeuvres—ranging

from cyberattacks to psychological influence—are not simply precursors to conflict, but instruments for shaping perception, eroding trust, and weakening societal cohesion from within.

In this context, strengthening democratic discourse and societal cohesion would constitute a logical policy response by Icelandic authorities. Investing in civic education, enhancing media literacy, and increasing public awareness of disinformation tactics represent sensible steps to bolster national resilience and preserve trust in democratic institutions amid mounting external pressure.

References

1 Iceland Monitor, "Russian Group NoName057 behind Cyber Attacks on Various Sites This Morning," *Iceland Monitor*, May 16, 2023, https://icelandmonitor.mbl.is/news/news/2023/05/16/russian_group_noname057_behind_cyber_attacks_on_var/.

2 Iceland monitor, "Raise the Alert Level due to Cyber Attacks," *Iceland Monitor*, May 16, 2023, https://icelandmonitor.mbl.is/news/news/2023/05/16/raise_the_alert_level_due_to_cyber_attacks/.

3 CERT.IS, Ársskýrsla 2023, https://cert.is/content/uploads/2024/06/arsyfirlit-2023.pdf.

4 Samtök fyrirtækja í fjármálaþjónustu: SFF dagurinn 2025: Breyttur heimur—April 9, 2025, https://www.sff.is/vidburdir/sff-dagurinn-breyttur-heimur.

5 Alexander Elliott, "Newspaper Threatened over Russian Flag Photo," *RÚV*, August 12, 2022, https://www.ruv.is/english/2022-08-12-newspaper-threatened-over-russian-flag-photo.

6 Ingunn Lára Kristjánsdóttir, "Starfsmönnum íslenska sendiráðsins í Moskvu var ógnað," *RÚV*, March 14, 2025, https://www.ruv.is/frettir/innlent/2025-03-14-starfsmonnum-islenska-sendiradsins-i-moskvu-var-ognad-438846.

7 Iceland Monitor, "Árvakur Hit by Major Cyber Attack," *Iceland Monitor*, June 26, 2024, https://icelandmonitor.mbl.is/news/news/2024/06/26/arvakur_hit_by_major_cyber_attack/?utm_source=chatgpt.com.

8 Magnús Jochum Pálsson, "Rússneskir hakkarar taldir bera ábyrgð á tölvuárás á HR," *Visir*, February 23, 2024, https://www.visir.is/g/20242524602d/russneskir-hakkarar-taldir-bera-abyrgd-a-tolvuaras-a-hr.

9 Reykjavik Univerisity, "Cyber attack on RU—Q&A What happened?" https://www.ru.is/en/news/cyber-attack-on-ru-qa?utm_source=chatgpt.com.

10 RÚV, Dagný Hulda Erlendsdóttir, "Rússneskur áróður smýgur inn í gervigreind," *RÚV*, May 14, 2025 https://www.ruv.is/frettir/erlent/2025-05-14-russneskur-arodur-smygur-inn-i-gervigreind.

11 France24, "Russian disinformation 'infects' AI chatbots, researchers warn," *France24*, March 10, 2025, https://www.france24.com/en/live-news/20250310-russian-disinformation-infects-ai-chatbots-researchers-warn.

12 Fjölmiðlanefnd, Upplýsingaóreiða & skautun í íslensku samfélagi 2023, https://fjolmidlanefnd.is/wp-content/uploads/2023/02/Upply%CC%81singao%CC%81reida-og-skautun-i%CC%81-i%CC%81slensku-samfe%CC%81lagi.pdf.

13 Fjölmiðlanefnd, unpublished survey data.

14 Iceland Monitor, "Europe stands firm on sanctions, strengthens support for Ukraine," *Iceland Monitor*, March 28, 2025, http://icelandmonitor.mbl.is/news/news/2025/03/28/europe_stands_firm_on_sanctions_strengthens_support/.

15 Alþingi, "Öryggi og varnir Íslands, munnleg skýrsla utanríkisráðherra," *Alþingi*, February 20, 2025, https://www.althingi.is/altext/raeda/156/rad20250220T141939.html.

16 NATO, "Allied Maritime Command, Naval Task Group increases presence and patrols in the GIUK Gap," *NATO*, March 20, 2025, https://mc.nato.int/media-centre/news/2025/nato-naval-task-group-increases-presence-and-patrols-in-the-giuk-gap.

Latvia: Not So Funny Business—Kremlin Pranksters Target Latvian Officials

By Ieva Bērziņa

Harassment (non physical)

Democratic institution

Deception (including deepfake)

Russian pranksters Vovan (Vladimir Kuznetsov) and Lexus (Alexei Stolyarov) have fooled high-ranking officials and celebrities in many Western countries, and Latvia is no exception. Until recently, while there was no definitive proof, it was assumed that their pranks were carried out in the interests of the Kremlin. However, in July 2024, the Russian news agency RIA Novosti reported that the pranksters had received state awards from the Kremlin.[1] This confirms that Vovan and Lexus' pranks can be assessed as one form of state sponsored hybrid warfare carried out by Russia.

The first widely publicized case of Vovan and Lexus targeting Latvian politicians occurred in March 2021. Rihards Kols, then Chairman of the Foreign Affairs Committee of the Latvian Parliament (Saeima), received a fake letter purportedly signed by Leonid Volkov, an associate to Russian opposition leader Alexei Navalny, requesting a meeting with the committee.[2] A meeting between the Foreign Affairs Committee and an imposter Volkov took place, with Latvian Television broadcasting a conversation with the look-alike and correspondent Ina Strazdiņa, who had received their email address from the Saeima press service as a seemingly reliable source.[3]

Vovan and Lexus continued targeting political leaders from various countries over several years. In 2025, they pranked Kosovo Prime Minister Albin Kurti by pretending to be Latvian President Edgars Rinkevics.[4] Thus, Latvian officials have not only been the target of a hybrid warfare attack but also used as a cover for the actions of pranksters close to the Kremlin. After the incident,

the Kosovo Prime Minister's office explained that it occurred shortly after the elections, when Albin Kurti "was receiving numerous congratulatory messages and calls regarding the election results," making it difficult to verify the authenticity of all the calls.[5]

One politically significant prank was their call to the fifth president of Georgia, Salome Zourabichvili, and former ombudsman Ucha Nanuashvili, pretending to be Ukrainian politician and former president Petro Poroshenko and Russian pro-democracy leader and chess grandmaster Garry Kasparov.[6] The prank occurred when Georgian political elites and society fiercely struggled over whether the country would come under increasing Russian influence or continue its orientation towards the West. One of the issues Vovan and Lexus obtained information on was Western funding of Georgian NGOs, aiming to show that civic activism is an instrument of Western influence. In this case, there was also a connection to Russian state-controlled media, as Russia's Channel One used the content of the prank "as evidence that the opposition and protests in the country are financed externally by organizations like USAID."[7]

Further examples show how widely Russia uses this method of hybrid warfare. In February 2022, Alexei Stolyarov published a video of a prank with leaders of the European People's Party, including Latvian member of the European Parliament Sandra Kalniete.[8] Shortly after a missile landed on Polish territory in November 2022, the Latvian Constitution Protection Bureau prevented an attempt by Russian pranksters to contact the Prime Minister and the State President when impersonating Polish President Andrzej Duda.[9] The pranksters later managed to hold a conversation with Latvian Prime Minister Krišjānis Kariņš in September 2023 while pretending to be Moussa Faki, Chairperson of the African Union Commission.[10]

The same pranksters also targeted then Danish Minister of Foreign Affairs Lars Løkke Rasmussen in an October 2023 online Teams call with a deepfake.[11] As video conferencing formats became widely used by high-level officials after the COVID-19 pandemic, deepfake technologies allowed the pranksters to visually impersonate political figures with ease. In this case, the pranksters chose African Union Commission Chairman Moussa Faki to ask Rasmussen about his perspectives of ending the war in Ukraine. "It is not easy

for me to predict, but at some point I guess the Ukrainian president will adjust the situation and declare that the time has now come to start negotiations," answered the foreign minister. The remark made it into a *TASS* telegram under the headline "Zelensky to agree to peace talks, top Danish diplomat says in call with Russian pranksters."[12]

The call with Minister Rasmussen happened only a few years after Vovan and Lexus made a similar phone call to the Danish parliamentary foreign policy committee in 2020 pretending to be Belarusian opposition leader Sviatlana Tsikhanouskaya.[13] The pranksters had also success in Sweden and Norway. Then Swedish Foreign Minister Anne Linde and two parliamentarians of the foreign affairs committee were fooled in 2021 to talk with the pranksters who pretended to be Navalny's associate Leonid Volkov;[14] in 2023 the Norwegian Prime Minister Jonas Gahr Støre was pranked.[15]

Pranking Western officials allows Russia to pursue its interests covertly, since the pranksters allegedly act as independent comedians. In 2024, Vovan and Lexus gave a lecture on the Day of Career and Education in Media, in which they emphasized that "pranks are an instrument of truth" because, in this way, they obtain information that officials would not say if they knew that the conversation was public.[16] This statement is unethical, since the information is obtained by deception. It also manipulates the concept of truth in the interests of the Kremlin since Russian officials are not their target; therefore, fooling foreign officials suggests they are liars and creates a false impression that Russian officials are more truthful and honest.

The ostensible purpose of a prank is to fool someone without causing harm, but the results of these actions promote the Kremlin's interests. Under the guise of humor, the pranksters are a part of a broader attack on Western countries and where Russia is vying for influence. First, they discredit the targeted politicians, trying to portray them as people who can be easily fooled. Second, by pretending to be someone with whom the officials sympathise or want to maintain a relationship, the pranksters also obtain opinions and information not meant for the wider public. In this way, pranksters create content for Russian media, which is used to discredit Western countries and their political leaders. Third, pranksters waste officials' time by arranging fake meetings, which decreases their work efficiency and creates an additional psychological

burden and workload, as the incidents have to be explained afterward. Finally, pranksters can also attempt to influence the behaviour of their targets in the interests of malign foreign actors. The prank calls therefore present a curious but far from harmless hybrid attack.

References

1 RIA Novosti, "Vovan i Lexus poluchili gosnagradi v Kremle [Vovan and Lexus received state awards in the Kremlin]," *RIA Novosti*, July 4, 2024, https://ria.ru/20240704/gosnagrady-1957346333.html?utm_source=yxnews&utm_medium=desktop.

2 Kols Rihards, "Par Viltus Leonīdu Volkovu: Kā Trīs Baltijas Valstis Satika Viltvārdi Un Kā Vēlāk Tāpat "Uzķērās," April 22, 2021, https://www.facebook.com/KolsRihards/posts/4129537150399849.

3 Ina Strazdiņa, "Navaļnija Līdzgaitnieks Volkovs: Manā Vārdā Uzdarbojas Kremļa Aģenti," *Latvijas Sabiedriskie Mediji*, April 22, 2021, https://www.lsm.lv/raksts/zinas/latvija/navalnija-lidzgaitnieks-volkovs-mana-varda-uzdarbojas-kremla-agenti.a401696.

4 Isufi Perparim, "Kosovo PM Pranked by Russians Pretending to be Latvia's President," *Balkan Insight*, March 26, 2025, https://balkaninsight.com/2025/03/26/kosovo-pm-pranked-by-russians-pretending-to-be-latvias-president/.

5 Ibid.

6 Ardashelia Marta, "Prank and Propaganda: What Zourabishvili and Nanuashvili Really Said to Vovan and Lexus," *SOVA*, April 24, 2025, https://sovanews.tv/2025/04/28/prank-and-propaganda-what-zourabishvili-and-nanuashvili-really-said-to-vovan-and-lexus/.

7 Ibid.

8 Алексей Столяров, "Пранк с лидерами Европейской народной партии в Европарламенте," *Octagon*, February 8, 2022, https://octagon.media/blogi/aleksej_stolyarov/prank_s_liderami_evropejskoj_narodnoj_partii_v_evroparlamente.html.

9 Latvijas Sabiedriskie Mediji, "SAB Aptur Viltvāržu Plānus Sarunām Ar Amatpersonām," *Latvijas Sabiedriskie Mediji*, November 23, 2022, https://www.lsm.lv/raksts/zinas/latvija/sab-aptur-viltvarzu-planus-sarunam-ar-amatpersonam.a483856/?utm_source=lsm&utm_medium=article-body&utm_campaign=admin.

10 Ģirts Kasparāns, Jolanta Plauka, and Krišs Kairis, "Krievijas Viltvāržiem Izdevies Sarīkot Videosarunu Ar Kariņu," *Latvijas Sabiedriskie Mediji*, November 14, 2023, https://www.lsm.lv/raksts/zinas/latvija/14.11.2023-krievijas-viltvarziem-izdevies-sarikot-videosarunu-ar-karinu.a531610/.

11 Jørgensen, Lars Bach, "Russisk komikerduo snød Løkke i videoopkald," *TV2*, October 20, 2023, https://nyheder.tv2.dk/politik/2023-10-20-russisk-komikerduo-snoed-loekke-i-videoopkald

12 "Zelensky to agree to peace talks, top Danish diplomat says in call with Russian pranksters," *TASS*, October 19, 2023, https://tass.com/world/1693491

13 A common denominator for the two calls to the Danish politicians was the focus on issues concerning animals, as a recurrent theme in Russian disinformation about Denmark. Storylines within this theme include fake news stories from 2017 about state sanctioned animal brothels and exploitation of true events such as the killing of a giraffe in Copenhagen Zoo back in 2014. The giraffe was killed based on a rationale of reducing the population of giraffes in the zoo. In the prank-call to the foreign minister in 2023, the story of the giraffe once again was brought up.

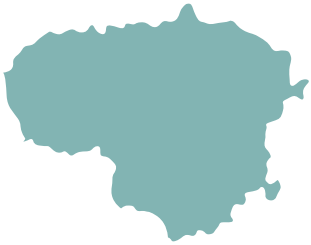
14 Arne Lapidus, "Ryska Bluffmakare Lurade Svenska Politiker: 'Komiskt'," *Expressen*, October 3, 2021, https://www.expressen.se/nyheter/ryska-bluffmakare-lurade-svenska-politiker-komiskt/.

15 Meme-art-alchemy, "Vovan and Lexus Prank the Norwegian Prime Minister Jonas Gahr Støre," *YouTube*, December 6, 2023, https://www.youtube.com/watch?v=KVGJmWCBuCk.

16 Russian Expo, "Prank as a tool of truth: Vovan and Lexus spoke about their secrets at the RUSSIA EXPO," *Russia Expo*, April 7, 2024, https://en.russia.ru/news/prank-kak-instrument-pravdy-vovan-i-leksus-na-vystavke-rossiia-rasskazali-o-svoix-sekretax.

Lithuania: Telegram Chats, Arson and Lies

By Adam Roževič



Vandalism / sabotage

Criminals / mercenaries / private contractors

Over the course of 2024, Lithuania, a staunch supporter of Ukraine, experienced aggressive disinformation attacks and a series of more than ten different sabotage incidents, ranging from graffiti and defaced monuments to arson attempts.[1]

The beating of a leading Russian opposition figure, parcels dispatched from Vilnius catching fire, defaced murals of Lithuanian freedom fighters, and arson attempts in Šiauliai and Vilnius were carried out by unlikely perpetrators—amateurs recruited online or disgruntled citizens fueled by Russian lies.

The most notorious case—the arson attempt at a Vilnius IKEA store—coincided with May 9th, a symbolic date for Russia, and was conducted by a 17-year-old Ukrainian refugee from Kherson.[2] As Lithuanian authorities report, he was lured by the Russian military intelligence service GRU via Telegram, an encrypted messaging app, with the offer of a BMW and $11,000 as a reward.[3] Lithuanian prosecutors say the suspect did not hold pro-Russian views and did not carry out the sabotage out of loyalty to Russia. Most likely, he fell victim to the promise of earning quick and easy money and a car (which he reportedly received, albeit an old model).[4]

This type of recruitment and implementation of sabotage has become a worrying trend, with similar cases happening across Europe, indicating a shift in Russian hybrid warfare. The strategy has been labeled by British Royal United Services Institute (RUSI) analysts as the "gig-economy sabotage," which relies on less sophisticated, decentralized networks of unsuspecting proxies.[5] In 2022, as European countries expelled Russian diplomats from their embassies in response to the full-scale invasion of Ukraine, Moscow found it difficult to

conduct activities that were usually carried out by intelligence services.[6] Russia therefore turned to amateurs across Europe.

Russian intelligence services found a simple, yet discreet way to attract and outsource proxies through creating nameless Telegram channels where they set up gigs on request—a simple-looking job for pay. By using a freelance-like online market, Russian services can quickly recruit and respond to political changes. A number of chats and forums managed by Russian agencies have popped up on Telegram, recruiting unsuspecting people from various backgrounds and promising payment to carry out simple but destructive gigs that are meant to wreak havoc and sow chaos.[7] Usually, the recruits do not even know the end-goals of operations; they are amateurs without any special skills, do not know who their true employer is, and do not have any special feelings towards Moscow.

A similar pattern was observed in other cases. Russia managed to recruit Polish football hooligans to attack Russian opposition leader Leonid Volkov near his home in Vilnius. A man sent incendiary packages from Lithuania via DHL to the United Kingdom and Germany; luckily, the unsophisticated devices exploded in cargo holding areas on the ground rather than mid-flight. Two Spanish tourists attempted to set fire to a factory located in Šiauliai.[8] From arson to dissemination of "Wagner Group" stickers, such cases have become regular occurrences in the Baltic region.[9]

However, the gig-like sabotage campaign is only one side of the coin in Russia's changed hybrid approach. In parallel, as Russia continues to wage disinformation campaigns, it has adapted by targeting sensitive social topics such as historical memory and national identity. Fueled by lies and hatred, psychological operations can transform into kinetic action.

After the 2022 full-scale invasion of Ukraine, the Russian state propaganda apparatus initially found itself on the back foot. It became difficult to conduct effective disinformation campaigns in Lithuanian society, as the "right" and "wrong," "victim" and "aggressor" had become more clear than ever. But Russian state propaganda evolved and started to employ more targeted and sophisticated narratives that, at first glance, were not easily recognizable as originating from Russia.

For example, the Russian state, without any real historical evidence, has been aggressively promoting the narrative that Lithuanian freedom fighters were Nazi collaborators and portraying them as terrorists. The purpose is to blur the facts of the Soviet occupation.

This disinformation campaign goes hand in hand with physical attacks. On three separate occasions, various statues and memorials of Lithuanian freedom fighters were desecrated. Just before May 9, 2023, one monument to the Lithuanian resistance leader Adolfas Ramanauskas-Vanagas was covered in white paint.[10]

Lithuanian intelligence services also disclosed a ploy of "Litvinism" as a product of Moscow—a pseudo-historical narrative that claims Belarus, not Lithuania, is the true inheritor of the history and traditions of the Grand Duchy of Lithuania—a highly sensitive topic for many Lithuanians.[11]

Claims like "Vilnius is truly a Belarusian, not Lithuanian, city" have angered many Lithuanians. Such narratives have also led to increased discord between some Lithuanians and Belarusians. This change of attitude has been rather drastic, as a majority of Lithuanians have previously supported Belarussians in their struggle against the Lukashenko regime. Now, heated debates on history, occasional graffiti, sometimes even on the walls of Belarusian businesses (which very well could be actions of Belarussian services to provoke further discord), have appeared around Vilnius.[12]

The combination of disinformation and propaganda, together with difficult to attribute physical actions, creates an impression that the narratives evoke so much emotion that individuals act upon the information, translating the emotions into kinetic action with real-world consequences.

References

1 "Išpuoliai Prieš Partizanų Vado A.Ramanausko-Vanago Paminklus: Merkinėje Aplietas Dažais, Lazdijų Rajone Įsmeigtas Kirvis," *15 Min*, May 8, 2023, https://www.15min.lt/naujiena/aktualu/lietuva/merkineje-isniekintas-partizanu-vado-a-ramanausko-vanago-paminklas-56-2049494.

2 The Guardian, "Russia behind arson attack on Ikea store in Lithuanian capital, says prosecutor," *The Guardian*, March 17, 2025, https://www.theguardian.com/world/2025/mar/17/russia-behind-arson-attack-on-ikea-store-in-lithuania-capital-says-prosecutor.

3 The New York Times, "How a Ukrainian Teen Became a Suspected Foot Soldier for Russia," *The New York Times*, April 10, 2025, https://www.nytimes.com/2025/04/10/world/europe/lithuania-ikea-fire-russia-sabotage.html.

4 Lithuanian Radio and Television, "Who is behind 'sabotages and diversions' in Lithuania and Poland?" *Lithuanian Radio and Television*, May 23, 2024, https://www.lrt.lt/en/news-in-english/19/2279598/who-is-behind-sabotages-and-diversions-in-lithuania-and-poland.

5 Daniela Richterova, Elena Grossfeld, Magda Long & Patrick Bury, "Russian Sabotage in the Gig-Economy Era," *The RUSI Journal*, 169:5, 10-21, 2024, DOI: 10.1080/03071847.2024.2401232.

6 Statista, "Number of Russian diplomats expelled worldwide from 2000 to 2023, by country," *Statista*, September 30, 2024, https://www.statista.com/statistics/1267669/number-of-expelled-russian-diplomats-by-country/.

7 Daniela Richterova, Elena Grossfeld, Magda Long & Patrick Bury, "Russian Sabotage in the Gig-Economy Era," *The RUSI Journal*, 169:5, 10-21, 2024, DOI: 10.1080/03071847.2024.2401232.

8 "Failed attack targeted Ukraine military aid—Lithuanian police chief?" *Lithuanian Radio and Television*, February 28, 2024=5, https://www.lrt.lt/en/news-in-english/19/2500432/failed-attack-targeted-ukraine-military-aid-lithuanian-police-chief.

9 Baltic News Network, "VDD: Russian Special Services Recruit People to Perform Sabotage in Latvia." *Baltic News Network*, March 14, 2024, https://bnn-news.com/vdd-russian-special-services-recruit-people-to-perform-sabotage-in-latvia-255202.

10 "Išpuoliai Prieš Partizanų Vado A.Ramanausko-Vanago Paminklus: Merkinėje Aplietas Dažais, Lazdijų Rajone Įsmeigtas Kirvis," *15 Min*, May 8, 2023, https://www.15min.lt/naujiena/aktualu/lietuva/merkineje-isniekintas-partizanu-vado-a-ramanausko-vanago-paminklas-56-2049494; *Lithuanian Radio and Television*, "Monument to Anti-Soviet Resistance Leader Defaced in Lithuania," *Lithuanian Radio and Television*, May 8, 2023, https://www.lrt.lt/en/news-in-english/19/1983200/monument-to-anti-soviet-resistance-leader-defaced-in-lithuania.

11 Lithuanian Radio and Television, "LRT aktualijų studija. Ar baltarusių litvinizmas pavojingas?" *Lithuanian Radio and Television*, Septmeber 7, 2023, https://www.lrt.lt/radioteka/irasas/2000292439/lrt-aktualiju-studija-ar-baltarusiu-litvinizmas-pavojingas?season=/radioteka/laida/lrt-aktualiju-studija/2025.

12 Lithuanian Radio and Television, "Išniekinta baltarusiškų suvenyrų parduotuvė: įtariama provokacija," *Lithuanian Radio and Television*, July 20, 2024, https://www.lrt.lt/radioteka/irasas/2000292439/lrt-aktualiju-studija-ar-baltarusiu-litvinizmas-pavojingas?season=/radioteka/laida/lrt-aktualiju-studija/2025.

Norway: An Arctic Warning from Svalbard

By Karen-Anna Eggen

Criminals / mercenaries / private contractors

History / memory

Disinformation (Hostile information)

Religion

Incident on the sea / close manoeuvring

Sabotage

Critical infrastructure

Cyberattack

Lawfare

Since 2022, Norway has experienced a more confrontational Russia in the Arctic. This chapter presents various Russian sub-threshold tools of influence related to the Arctic Svalbard Archipelago and Northern Norway. The first is a combination of cyberattack, intimidation, and lawfare. The remainder examines examples of (para-)military signalling, disinformation, religion and history, and intimidation in the form of incidents at sea.

Between May and June 2022, Russia instigated an information operation against Norway and Svalbard in connection with EU sanctions restricting Russian transport into Schengen.[1] Consequently, Russia could no longer transport goods from Murmansk to its Svalbard settlement of Barentsburg via Tromsø. Although the Norwegian government quickly proposed two solutions—either that Russia find another means of transportation from the Russian border to Tromsø, or simply ship the goods themselves from Murmansk—Russia portrayed the decision as a discriminatory act towards

Russians on Svalbard and warned of a looming humanitarian crisis. The pro-Russian hacker group KillNet subsequently instigated a large distributed denial-of-service (DDoS) attack on several government and media websites, using a manipulated picture of then-foreign minister Anniken Huitfeldt and citing the discriminatory act towards Russians as the reason.[2] On top of this, Russian Duma politicians threatened to dissolve a much-praised and hard-won delimitation agreement from 2008,[3] and several other Russian officials questioned Norway's right to sovereignty as they alleged Oslo was breaching the Svalbard Treaty.[4]

Between January and July 2023, Northern Norway experienced three (para-)military incidents. The first was two Russian "seamen" in military-looking uniforms walking the streets of the Norwegian mainland border town of Kirkenes.[5] On May 9, Russian military-style parades were organized for the first time in Barentsburg and Pyramiden on Svalbard.[6] In Barentsburg, the parade included Russian flags, military-looking uniforms, a motorcade, and even a helicopter. In Pyramiden, the so-called Donetsk People's Republic flag was also used. In July 2023, the Russian Consul General to Svalbard led a small military-inspired flotilla with several Russian flags in the waters outside Barentsburg in connection with Russia's Navy Day.[7]

On June 16, 2023, a pro-Kremlin Telegram channel Mash[8] published a disinformation story about a secret U.S. led military-biological laboratory[9] on the Norwegian Bear Island (located between Svalbard and mainland Norway).[10] The story was picked up by regional and national Russian media and further disseminated in a speech by the Russian Head of Medicine and Biological Problem of Human Adaptation in the Arctic at a pro-Kremlin conference in Murmansk in late October 2023.

In August 2023, the Russian orthodox church had a seven-meter-high cross illegally erected in Pyramiden to sanctify the deserted village and pay tribute to the Russians who discovered Svalbard. The cross honoured Georgy the Victorious, the protector saint for soldiers. According to Barents Observer, bishop Iyakov of Naran-Mars and Mezen is well-known for "pushing Russia's geopolitical ambitions in the Arctic by blessing polar outposts together with leaders of military and security structures."[11] The bishop was also heard calling the village "Russian."

In October 2023, in an apparent act of signalling and harassing, the Russian research vessel, or spy ship, *Yantar*, pursued the Norwegian research vessel *Kronprins Haakon* for 18 hours outside Svalbard.[12] *Yantar* documented Norwegian activity, taking pictures and filming. The Russian vessel is under the direct command and control of the Russian Ministry of Defence and is considered the flagship of Russia's secret military program GUGI (Main Directorate of Deep-Sea Research).[13]

Russian complaints about Norwegian regulations on Svalbard[14] and testing Norway's responses to various attacks, from cyber to migration, are not new.[15] Although 2024 and the first half of 2025 saw a reduction in, or at least more restrained behavior compared to some of the activities highlighted in 2022 and 2023, more assertive Russian behaviour on Svalbard is the new normal. The broader trends of Russia's increased religious presence (despite a declining Russian population on the archipelago) and use of history—in particular Soviet nostalgia—is noticeable and not without a purpose.[16] Russia increasingly seeks to promote Russian historic presence on Svalbard and the narrative that the island is historic Russian land. This type of memory policy, paired with increased Russian accusations of Norwegian discrimination of Russians on Svalbard, have worrisome parallels to Russian information operations against its other neighbors. Most notably, they resemble the pretexts used by Russia prior to its invasions of Ukraine in 2014 and 2022.

These actions should be seen in relation to Svalbard's rising security and strategic significance and a more aggressive semi-totalitarian Russian state. Russia's 2022 Foreign Policy Review highlighted its ambition to prevent "the negative impact of illegal restrictive measures imposed by unfriendly states on Russia's presence on the Spitsbergen archipelago."[17] This was the only geographical section specifically highlighted in the Nordic region. Previously, Russia had included brief summaries of its relations with various Nordic countries, but these were removed and replaced with more generic statements categorising several European countries as hostile. Specifying Svalbard suggests that it is a key area of contention in Russian thinking[18]—especially when Russian activity is paired with official rhetoric, as voiced in February 2024 by Deputy Prime Minister Yury Trutnev, who claimed that Russian rights on

Svalbard are under pressure, comparing the fight to preserve these with the battle for "Russian sovereignty" in Ukraine.[19]

The return of President Donald Trump to the White House in January 2025 increased uncertainty over U.S. commitments to European security. Of particular concern in the Arctic region are the repeated statements concerning the U.S. need to control Greenland, an autonomous territory of Denmark, a key U.S. ally.[20] Trump's threats and justifications challenge international law and echo Kremlin talking points. A forced U.S. take-over of Greenland would have grave implications for NATO and set a precedent for other states with similar territorial ambitions in the Arctic region and globally.

Furthermore, concern over a U.S. withdrawal from Europe has spurred debates about Russia testing NATO's resolve and commitment to Article 5. While the debate typically involves a scenario in the Baltic Sea region, Svalbard's remote location, geostrategic significance, and lack of military presence makes it an easier target for a potential attack. Depending on the trajectory of NATO cohesion and U.S. security interest in the High North, Svalbard should not be written off. Instead, the Arctic archipelago must be seen as a potential frontline for NATO.

References

1 Forthcoming article: Siri Strand and Karen-Anna Eggen. "'Arktisk blokade': en russisk informasjonsoperasjon mot Norge," *Internasjonal Politikk*, 2025.

2 Hallvard Norum, "Russisk Hackergruppe Skal Ha Startet Angrep Mot Norge," *NRK*, June 29, 2022, https://www.nrk.no/norge/russisk-hackergruppe-skal-ha-startet-angrep-mot-norge-1.16020947.

3 Aftenposten, "Avtalen Var Jonas Gahr Støres Store Seier. Nå Åpner Russerne for å Vrake Den," *Aftenposten*, July 5, 2022, https://www.aftenposten.no/verden/i/MLORVR/russlands-nasjonalforsamling-skal-utrede-skroting-av-delelinjeavtalen-med-norge.

4 Anastasia Tenisheva, "Russia Hits out at Norway over Blocked Arctic Archipelago Access," *The Moscow Times*, June 30, 2022, https://www.themoscowtimes.com/2022/06/29/russia-hits-out-at-norway-over-blocked-arctic-archipelago-access-a78138.

5 Thomas Nilsen, "Russian Seamen Walk Streets of Kirkenes in Military-Looking Uniforms," *The Independent Barents Observer*, January 12, 2023, https://thebarentsobserver.com/en/kirkenes/2023/01/russian-seamen-walk-streets-kirkenes-military-looking-uniforms.

6 Atle Staalesen, "Russia Stages Military-Style Propaganda Parade on Norway's Svalbard Archipelago," *The Independent Barents Observer*, May 9, 2023, https://thebarentsobserver.com/en/security/2023/05/russia-stages-military-style-propaganda-parade-norways-svalbard-archipelago.

7 Thomas Nilsen, "Russian Diplomat Staged Navy Parade at Norway's Svalbard Archipelago," *The Independent Barents Observer*, July 31, 2023, https://thebarentsobserver.com/en/security/2023/07/russian-consul-staged-navy-parade-norways-svalbard-archipelago.

8 Mash, "Биологическая лаборатория США появится в нескольких часах по воде от Мурманска.," *Telegram*, June 16, 2023, https://t.me/breakingmash/45026.

9 Thomas Nilsen, "Isolated Russia Invites Faraway Countries to Upcoming Svalbard Science Center in Pyramiden," *The Independent Barents Observer*, October 30, 2023, https://thebarentsobserver.com/en/arctic/2023/10/ghost-town-pyramiden-will-be-home-russias-planned-international-svalbard-science.

10 Ramsar Sites Information Services, "Bear Island," *Ramsar Convention on Wetlands*, June 23, 2023, https://rsis.ramsar.org/ris/1966.

11 Thomas Nilsen, "Svalbard Governor Orders War-Glorifying Cross Demolished. Russian Official Protests on Behalf of the Entire Orthodox World," *The Independent Barents Observer*, October 17, 2023, https://thebarentsobserver.com/en/arctic/2023/10/svalbard-governor-orders-war-glorifying-cross-demolished-russian-official-protests.

12 Inghild Eriksen, Håvard Gulldahl, and Lisa Rypeng, "Norsk Forskningsskip 'Forfulgt' Av Russisk Spionskip I 18 Timer," *NRK*, October 30, 2023, https://www.nrk.no/tromsogfinnmark/det-norske-forskningsskipet-_kronprins-haakon_-ble-forfulgt-av-russlands-_spionskip_-_yantar_-1.16610177.

13 "Main Directorate of Deep-Sea Research," *Wikipedia*, February 19, 2024, https://en.wikipedia.org/wiki/Main_Directorate_of_Deep-Sea_Research#cite_note-1.

14 Atle Staalesen, "Amid Jubilant Celebration at Svalbard, Norway Sends Strong Signal It Will Not Accept Encroachment on Sovereignty," *The Independent Barents Observer*, February 9, 2020, https://thebarentsobserver.com/en/arctic/2020/02/amid-jubilant-celebration-svalbard-norway-sends-strong-signal-it-will-not-accept.

15 The sanctioned former Deputy Prime Minister Dmitry Rogozin's illegal pit stop on Svalbard in 2015 springs to mind. Indicators also point to Russia being behind two sub-sea sabotages outside Svalbard and the coast of Northern Norway in 2021, although this is not officially attributed.

16 Thomas Nilsen, "Militarized memory: Kremlin-orchestrated 'Immortal Regiment' rally on Svalbard," *Barents Observer*, May 10, 2025, https://www.thebarentsobserver.com/news/militarized-memory-kremlinorchestrated-immortal-regiment-rally-on-svalbard/429583. For research on Russia's memory policy in Norway, see, e.g., Kari Aga Myklebost, "Minnediplomati i grenseland. De russisk-norske patriotiske minneturene 2011–2019," *Nordisk Østforum*, 2023, 37, 130–155. https://doi.org/10.23865/noros.v37.5514.

17 *Foreign Ministry of the Russian Federation*, Foreign Policy Review, 2023, https://www.mid.ru/ru/foreign_policy/news/1860242/.

18 Karen-Anna Eggen, "Designing around NATO's Deterrence: Russia's Nordic Information Confrontation Strategy," *Journal of Strategic Studies*, 2024, 1–25, https://doi.org/10.1080/01402390.2024.2332328.

19 Atle Staalesen, "Deputy Prime Minister Sends Warning to Oslo: Russian Rights at Svalbard Must Not Be Challenged," *The Independent Barents Observer*, February 13, 2024, https://thebarentsobserver.com/en/2024/02/deputy-prime-minister-sends-warning-oslo-russian-rights-svalbard-must-not-be-challenged.

20 Jessie Yeung and Piper Hudspeth Blackburn, "Trump renews threat of military force to annex Greenland," *CNN*, May 4, 2025, https://edition.cnn.com/2025/05/04/world/greenland-annexation-threat-trump-nbc-interview-intl-hnk.

Poland: The Modern Hybrid Siege

By Aleksander Olech

Coercive Migration

Vandalism / sabotage

Hostile information

Deception (including deepfake)

Cyber attack

Espionage

Poland has long been a principal target of Russian hybrid assaults, predating even Russia's aggression towards Georgia in 2008 and Ukraine in 2014. But the frequency of sabotage attempts, assaults, and hostile actions has markedly escalated since the full-scale invasion, especially as Poland emerged as a primary conduit for aid to Ukraine. Russia employs a wide array of tools and tactics that together form a true amalgamation of threats—an effort to conquer the castle without storming its walls.

Since February 2022, Poland has been subjected to attacks by the Russian security services, paid operatives, private military firms, and unwitting individuals engaged in nefarious activities. Russian hybrid operations, reinforced by information warfare designed to disrupt the dissemination of information, are multifaceted in nature, affecting national security across political, social, and cyber domains.

Russian operations use a variety of tools: from the instrumentalization of migration (as in the case of the Polish-Belarusian border crisis, where migrants were used as a tool for political pressure and to test the state's response), intensive disinformation operations (such as "Doppelganger" and "Matryoshka" involving media impersonation and denigration of fact-checking institutions) to acts of physical sabotage (including arson attacks on industrial and logistical facilities involving individuals recruited by Russian intelligence). In addition, cyber activities have been an important component, ranging from

massive DDoS attacks on government and infrastructure sites (as in the case of Polish railway company PKP Intercity and the Polish Press Agency) to sophisticated data-stealing operations, including military and personnel data. All these activities are elements of a coordinated hybrid strategy aimed at paralyzing the functioning of the state, sowing social chaos, weakening morale, and testing the limits of Poland's resilience as a member of NATO and the European Union.

An event that significantly affected the perception of hybrid threats was the Moscow- and Minsk-backed migration crisis on the Polish-Belarusian border. The first attempts to push migrants illegally across the border took place as early as June 2021, when Moscow and Minsk orchestrated flights from the Middle East, particularly Iraq and Syria, to Belarus. Migrants were lured with promises of easy entry into the EU and deliberately directed towards the Polish border. Later, this strategy expanded to include migrants from African countries who entered Russia and were then funneled toward the EU's eastern border, with similar hybrid pressure tactics employed against Lithuania and Finland. Of particular note was an incident in June 2024, Polish soldier Mateusz Sitka was fatally attacked by a migrant when guarding the border. The incident triggered strong public reactions and shook the public's sense of security. It was interpreted as part of provocative actions instigated by Belarus and Russia. Mass attempted border crossings by organized groups of migrants can be seen as a form of low intensity conflict. At the same time, the region is witnessing an intensification of disinformation activities, which exacerbate information chaos and lead to confusion and increased tensions in society.[1]

The Lithuanian prosecutor's office confirmed that Russian special services were behind an arson attack on a large market hall in Warsaw in May 2024, as well as the previous year's arson attack on an IKEA store in Vilnius.[2] These incidents are part of a broader pattern of covert operations conducted by Russian intelligence in the region. On March 20, 2025, Poland's Internal Security Agency (ABW) detained a Ukrainian citizen born in Russia, who was actively involved in espionage activities on behalf of the Russian Federation. The individual conducted reconnaissance of military facilities across Poland. During interrogation, the suspect provided statements explaining the ideological

motivations behind his actions, citing strong personal and ideological ties to Russia.[3]

An increasingly prominent element of the Russian Federation's hybrid operations in Poland is the use of foreign nationals in diversionary and espionage activities orchestrated by Russian special services.[4] In 2023, officers of the Polish Internal Security Agency detected and unraveled an espionage network carrying out reconnaissance and diversionary tasks on behalf of the Russian Federation. So far sixteen people have been convicted in this case, including twelve Ukrainian citizens, three Belarusians, and one Russian.[5]

Cyberattacks and assaults on Poland's critical infrastructure have intensified since February 24, 2022. Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski has stated that there can be dozens of incidents per day (mostly cyber-related) and emphasized that Poland is among the most frequently cyber-attacked countries in Europe, though some experts also point to Estonia as a leading target. 40,000 cyber incidents were reported in 2022; by 2023, the number had doubled to 80,000. One significant breach was a cyber operation targeting a NATO agency, which led to the leak of Polish officers' personal data.[6] The hacking group SiegedSec claimed responsibility. Another major incident illustrating how cyberattacks and disinformation operate in tandem occurred on May 31, 2024, when the Polish Press Agency (PAP) published two fake dispatches about a supposed mobilization in Poland, triggering public anxiety.[7] In response to escalating hybrid threats, Poland is expanding its capabilities within its Cyber Defence Forces Component Command (DKWOC), which serves as the fifth branch of the Polish Armed Forces. In June 2024, Minister Gawkowski announced the allocation of 3 million PLN (approximately 700,000 EUR) for the "Cybershield" project, aimed at strengthening civilian-military cyber coordination, protecting critical infrastructure, and enhancing national cyber resilience.[8]

Poland's first confirmed case of sabotage ordered directly by Russian intelligence occurred in April 2024, when a home improvement store on Radzymińska Street in Warsaw was subject to arson. According to the prosecutor's office, the perpetrator, a Belarusian national identified as Stepan K., was acting on behalf of the Russian intelligence services and was subsequently charged with sabotage, terrorism, weapons trafficking, and espionage. His actions are

part of a growing pattern of coordinated sabotage operations across Polish territory, revealing the increasingly aggressive posture of Russian intelligence in using foreign nationals for hybrid operations on NATO's eastern flank.[9]

In the realm of disinformation, Russia spreads false messages to undermine support for Ukraine and divide Polish society. The narratives disseminated focus on stoking anti-Ukrainian sentiment by promoting theories about the "Ukrainization of Poland," which alleges that refugees receive favorable treatment while exaggerating the cost of aid to Ukraine.[10]

Disinformation related to the situation on the Polish-Belarusian border was also revived in 2025. Alongside the "traditional" narratives, Belarusian authorities alleged they thwarted the smuggling of 580kg of highly explosive PETN from Poland to Russia, where it would be used to carry out sabotage and diversion. The purpose of such a cognitive operation was to influence the societies of Belarus, Russia, and the West at large.[11]

In late April 2025, fires broke out in the Biebrza National Park, near the border with Belarus. Poland's Prime Minister Donald Tusk stated that the arson incidents were part of Russian and Belarussian hybrid activities carried out by very young people for low wages; while significant damage is caused, tracing the perpetrators is difficult.[12]

The methods deployed against Poland could be described as a siege on society. Highly varied activities combine military and non-military instruments to concurrently pursue political, military, informational, social, and financial objectives. By means of instrumentalising migration, disseminating false information, and acts of sabotage and diversion, Russia and its allies hope to destabilise Western societies. The Polish example gives other European countries insight into how far Russia has to go to reach its goals.

In response to the growing threat from Russia and Belarus, in May 2025, Prime Minister Donald Tusk extended Poland's BRAVO and BRAVO-CRP second highest alert level (in a four tiered system) through August 31, 2025.[13]

Given the growing pressure, one of the top concerns of the Polish government should be continually enhancing the nation's resilience towards future hybrid attacks. This includes optimizing border security, raising public awareness, and deepening international cooperation. Poland remains the eastern

wall of NATO and the European Union, serving simultaneously as a key logistics hub for Ukrainian aid. The wall is still being built, as new layers of bricks are added to strengthen its structure, but resilience is not a finished product—it is a continuous effort to ensure the enemy stays at bay.

References

1 Tomasz Molga, "Migrant zabił na granicy żołnierza RP. Gdzie jest zabójca?," *Wirtualna Polska*, November 15, 2024, https://wiadomosci.wp.pl/smierc-polskiego-zolnierza-na-granicy-jest-nowy-trop-ws-potencjalnego-zabojcy-7092615739153344a.

2 Gazeta Prawna, "Rosyjskie służby podpaliły halę w Warszawie. Donald Tusk potwierdza podejrzenia litewskiej prokuratury," *Gazeta Prawna*, March 17, 2025, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9759495,rosyjskie-sluzby-podpalily-hale-w-warszawie-donald-tusk-potwierdza-po.html.

3 "Komunikat ABW," Agencja Bezpieczeństwa Wewnętrznego, April 1, 2025, https://www.abw.gov.pl/pl/informacje/2617,Komunikat-ABW.html.

4 Money.pl, "Sabotaż za 7 dolarów. CNN: Ukrainiec szpiegował w Polsce dla Rosji," *Money.pl*, July 10, 2024, https://www.money.pl/gospodarka/pozar-na-marywilskiej-44-cnn-pisze-o-rosyjskiej-wojnie-w-cieniu-7047634169244608a.html.

5 Infosecurity24, "Rosyjska dywersja w Polsce. 'Do zadań rekrutowani są młodzi ludzie z państw byłego ZSRR'," *Infosecurity24*, October 25, 2024, https://infosecurity24.pl/sluzby-specjalne/rosyjska-dywersja-w-polsce-do-zadan-rekrutowani-sa-mlodzi-ludzie-z-panstw-bylego-zsrr.

6 Politico, "Leaked email scandal engulfs Poland's political elite," *Politico*, April 17, 2025, https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking.

7 Polska Agencja Prasowa, "Cyberatak na PAP," *Polska Agencja Prasowa*, May 31, 2024, https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwa-depesza-o.

8 Szymon Palczewski, "Rosyjskie ataki na Polskę. Wicepremier porównuje cyber do czołgów," *Cyberdefence24*, June 4, 2024, https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjskie-ataki-na-polske-wicepremier-porownuje-cyber-do-czolgow.

9 TVN24, "Białorusin oskarżony o szpiegostwo i podpalenie marketu budowlanego w Warszawie," *TVN24*, April 12, 2024, https://tvn24.pl/polska/warszawa-bialorusin-oskarzony-o-szpiegostwo-i-podpalenie-marketu-budowlanego-przy-radzyminskiej-7442853.

10 PublicRelations.pl, "Raport Demagoga i IMM: Antyukraińska propaganda w 2024 roku," *PublicRelations.pl*, February 24, 2025, https://publicrelations.pl/raport-demagoga-i-imm-antyukrainska-propaganda-w-2024-roku.

11 Mikołaj Rogalewicz, "Znowu głośno o granicy z Białorusią. Precyzyjna operacja Rosji przeciwko Polsce," *CyberDefence24*, April 11, 2025, https://cyberdefence24.pl/cyberbezpieczenstwo/znowu-glosno-o-granicy-z-bialorusia-precyzyjna-operacja-rosji-przeciwko-polsce.

12 TVN24, "Tusk: podpalenia na zlecenie obcych służb trzeba traktować jak akt zdrady," *TVN24*, April 22, 2025, https://tvn24.pl/polska/donald-tusk-podpalenia-na-zlecenie-obcych-sluzb-trzeba-traktowac-jak-akt-zdrady-st8422785.

13 Mikołaj Rogalewicz, "Stopnie alarmowe na dłużej. Jest decyzja Donalda Tuska," *CyberDefence24*, May 30, 2025, https://cyberdefence24.pl/cyberbezpieczenstwo/stopnie-alarmowe-na-dluzej-jest-decyzja-donalda-tuska.

Sweden: The Atomic Church With a Crooked Priest

By Patrik Oksanen

Nuclear (civilian)

Economic fraud / money laundering

Criminals / mercenaries / private contractors

Real Estate

Religion

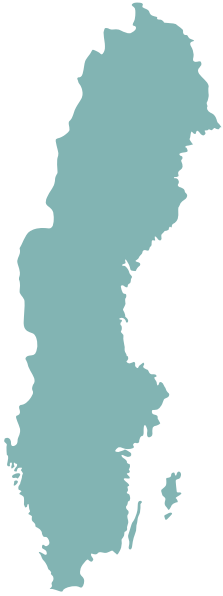
Strategic location

Infiltration / influence or take over 3rd party

Espionage

Democratic institution

Lawfare



Just a five-minute walk from Västerås Airport, an important airfield for Sweden's total defence, lies a newly built Russian Orthodox Church (Heliga Gudsmodern till Kazan/Holy Godmother of Kazan). The process of building the Church is a story of money laundering, political infiltration, funding from the state owned nuclear energy company Rosatom (which also produces Russian nuclear weapons), decisions from the highest level in Moscow, connections to organised crime, all at a strategic location from which to house resources and operatives that could be used during a crisis and ultimately war.

The Russian Orthodox Church (ROC), also known as the Moscow Patriarchate, was revived by Stalin in 1943 and put under the control of the NKVD (precursor to KGB, today SVR and FSB).[1] The historic bonds remain.

The wooden church in Västerås, worth 35 millions SEK (approx. 3.1 million EUR)[2] and protected by a high black iron fence, was funded by Rosatom.[3] This

source of funding became public in 2023, when Metropolitan Anthony of Volokolamsk, chairman of the Moscow Patriarchate's Department for External Church Relations, officially thanked Rosatom for its financial support during the church's inauguration. The financing was channeled through Rosatom's Fund for Supporting Christian Culture and Population,[4] which is led by the head of Rosatom and includes the Metropolitan himself as a board member. Among the invited guests at the inauguration were the ambassador of Belarus, and number two at the Russian Embassy, who had earlier been identified as a Russian intelligence officer by Swedish public broadcaster SVT.[5]

The plan to build a church in Västerås dates back to 2012, but it was not until 2017 that permission was granted, despite warnings from Swedish Security Police (SÄPO).[6] The procedure was marked with noticeable events. Two substitutes of the local permit board, one with personal connections to the church and the second with roots in the former Soviet Union, acted with practical support to the priest to establish the church during the process without reporting their conflicts of interest in any written form to the municipality. The decision to grant the building permit was taken by the chair alone, which is legal but highly unusual—especially in a case like this with a warning from SÄPO.[7]

During the process, the priest in Västerås[8] was CEO for a Russian company[9] and later convicted of accounting violations.[10] The priest had also received a medal of honour from the Russian Foreign Intelligence Service (SVR) for establishing the church.[11] In addition, the Estonian developer of the church had been sentenced to seven years imprisonment for drug smuggling and reportedly had connections to Russian organised crime with links to the FSB.[12]

SÄPO reported in 2019 that, among other tools, Russia uses religion and the establishment of physical sites that could be used here and now, and in the future in a more severe security situation.[13] Since religious institutions are protected in various ways under Swedish law, for example from wiretapping, the church's vicinity to the Västerås airport will continue to be a security challenge for the Swedish authorities. In 2024, after SÄPO confirmed the ROC's ties to Russian intelligence, the Swedish Agency for Support to Faith Communities ceased all government funding to the ROC.[14]

South of Gävle, the ROC in Sweden rented a church by the Marma military shooting range,[15] which is strategically located close to several important bridges and several energy plants.[16] The priest responsible for the Gävle parish is the same as in Västerås. After an intervention by the Diocese of the Swedish Lutheran Church, the contract was terminated in late 2023.

In Stockholm, the Moscow Patriarchate tried to take control of an independent Russian orthodox parish. The hostile takeover attempt ultimately failed, but it culminated when a group from patriarchate disrupted a baptism and demanded loyalty to Moscow. The police were summoned to the church in central Stockholm to restore order.[17] The ROC admitted the attempt to change the jurisdiction of this independent Russian orthodox parish with the justification: "They had stopped loving Russia and lost their Russian identity," but denied the actual hostile takeover attempt.[18] Instead, the ROC managed to infiltrate the independent non-profit association Sankt Sigfrids kyrkas vänner (Friends of the church of Saint Sigfrid)[19] and take control over the building that lies close to Stockholm Waterworks and right along the Essingeleden (E4/E20 motorway). Despite a court ruling giving control over the association back to the original board, the ROC kept control of the building for three years due to continuous legal challenges against the non-profit association and refused to hand over the keys.[20] In 2024, the ROC finally gave up and handed the building over to the legally recognized party.[21]

In Boliden, in northern Sweden, the still Moscow-loyal part of the Ukrainian Orthodox Church was gifted a building as part of a money laundering scheme through Bulgaria involving 50 properties that changed ownership over 120 times. The donor to the church was later sentenced to four years of prison for money laundering. When the police raided the premises, they found a wanted person hiding in the church.[22]

Issues with Russian churches are not limited to Sweden. In Norway the ROC bought a property to use as a church with a perfect view over Norway's most important naval base, Haakonsvern, outside of Bergen.[23] The ROC also attempted to build a chapel near an important radar facility[24] operated by Norwegian intelligence and highly relevant to NATO.[25]

In Estonia, a donation of 1.24 million EUR to build a new church in Tallinn in 2010 raised alarms. The Estonian Internal Security Service (KAPO) found

the donor to be Putin's close confidant Vladimir Yakunin, president of the state owned Russian Railways.[26] In 2024, Estonia did not renew the residence permit for Metropolitan Eugene, a Russian citizen who led the Estonian Orthodox Church of Moscow Patriarchate.[27] KAPO stated in its 2024 annual report that the metropolitan was involved in influence activities and concluded:

> "From Russia's perspective, it is crucial to maintain the entities associated with the Russian Orthodox Church abroad, along with their influence and assets, because the church is one of the few remaining levers for Russian influence operations that are not yet directly affected by international sanctions."[28]

The Estonian Parliament followed up by calling the Moscow Patriarchate "an inherent danger to Estonia's security and survival, including a direct threat to the public and constitutional order in Estonia," and underlined the Church's role as an ideological pillar for the Russian state.[29] In the spring of 2025, the Estonian Parliament passed with overwhelming majority a law that would force religious entities to cut ties with Moscow. However, President Alar Karis did not sign the law, despite sharing the threat assessment. Instead he stressed that the issue is not the lack of legal tools, but rather their implementation, and that existing tools should be applied more forcefully.[30]

In Russia, the only thing that is holy is the Empire. It is not surprising then that the Church serves the Kremlin's higher purpose and not God's.

References

1 Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Penguin Books, 2000). p. 634.

2 Approximation due to fluctuation in SEK vs EUR.

3 Mikaela Lundblad, "VLT AVSLÖJAR: Ryskt Kärnkraftsbolag Finansierade Kyrkobygget," *Vestmanlands Läns Tidning*, November 28, 2023, https://www.vlt.se/2023-11-28/vlt-avslojar-ryskt-karnkraftsbolag-finansierade-kyrkobygget.

4 Official name is Fund for Supporting Christian Culture and Population, https://fscch.info/about/.

5 Patrik Oksanen, *Rysslands hemliga krig mot Sverige* (Volante, 2025). P. 283-285.

6 Mikaela Lundblad, "Efter VLT:s Avslöjande—Teljebäck (S) Saknade Tydliga Besked Från Säpo: 'Vi Kan Inte Göra Den Bedömningen'," *Vestmanlands Läns Tidning*, September 1, 2020, https://www.vlt.se/artikel/efter-vlts-avslojande-teljeback-s-saknade-tydliga-besked-fran-sapo-vi-kan-inte-gora-den-bedomningen/.

7 Mikaela Lundblad, Mats Laggar, and Daniel Nordström, "Rysk Kyrka Byggs Nära Västerås Flygplats—Pekas Ut Som Säkerhetshot: 'Chockerande'," *Vestmanlands Läns Tidning*, March 19, 2019, https://www.vlt.se/artikel/rysk-kyrka-byggs-nara-vasteras-flygplats-pekas-ut-som-sakerhetshot-chockerande.

8 The priest was later also responsible for another congregation (in Gävle) who rented a church from the Swedish Church in Marma (30 kilometres south of Gävle), situated just beside a military shooting range and camp that is administered by the Royal Life Guards Regiment in Stockholm. It is also close to several important road and railroad bridges over the river Dalälven, close to Gävle harbour that has been pointed out as a strategic harbour for NATO by the Chief of the General Staff of the Russian Armed Forces, Valerij Gerasimov.

9 Mikaela Lundblad, Mats Laggar, and Daniel Nordström, "Bygget Betalades Med Fuskfaktura—På Uppdrag Av Prästen Makarenko: 'Pekar I En Riktning Att Dölja Pengar'", *Vestmanlands Läns Tidning*, March 19, 2019, https://www.vlt.se/artikel/bygget-betalades-med-fuskfaktura-pa-uppdrag-av-prasten-makarenko-pekar-i-en-riktning-att-dolja-pengar/.

10 Ibid.

11 Patrik Oksanen, *Rysslands hemliga krig mot Sverige* (Volante, 2025). p. 288.

12 Mikaela Lundblad, Mats Laggar, and Daniel Nordström, "Rysk Kyrka Byggs Nära Västerås Flygplats—Pekas Ut Som Säkerhetshot: 'Chockerande'," *Vestmanlands Läns Tidning*, March 19, 2019, https://www.vlt.se/artikel/rysk-kyrka-byggs-nara-vasteras-flygplats-pekas-ut-som-sakerhetshot-chockerande..

13 Mikaela Lundblad, Mats Laggar, and Daniel Nordström, "Moskvapatriarkatet Ett Av Kremls Verktyg—Pekas Ut Som Påverkansvapen," *Vestmanlands Läns Tidning*, March 20, 2019, https://www.vlt.se/artikel/moskvapatriarkatet-ett-av-kremls-verktyg-pekas-ut-som-paverkansvapen/.

14 Johan Wicklén, "Inget Statsbidrag till Ryska Ortodoxa Kyrkan I Sverige," *SVT Nyheter*, February 29, 2024, https://www.svt.se/nyheter/inrikes/inget-statsbidrag-till-ryska-ortodoxa-kyrkan-i-sverige.

15 The rent was terminated in advance and ended the last day of 2023.

16 Patrik Oksanen, "Oksanen: Ryske Generalen Som Sätter Oss På Kartan," *Gefle Dagblad*, May 24, 2017, https://www.gd.se/2017-05-24/oksanen-ryske-generalen-som-satter-oss-pa-kartan.

17 Patrik Oksanen, "Rysk-Ortodoxa Går Putins Ärenden När De Försöker Ta Över Svensk Kyrka," *Dagen*, July 9, 2020, https://www.dagen.se/debatt/2020/07/09/rysk-ortodoxa-gar-putins-arenden-nar-de-forsoker-ta-over-svensk-kyrka/.

18 Maria Georgieva, "När Rysk Utrikespolitik Tar Sig In I Kyrkorummen," *Sveriges Radio*, July 17, 2020, Godmorgon världen, https://sverigesradio.se/artikel/7517269.

19 The NGO works in the tradition of the Lutheran Swedish Church. This is not a church itself, but the association gathers individuals with a more conservative Lutheran view, and the building of Saint Sigfrid is rented out for baptisms and services. The NGO was split in two because of the issue of renting to ROC. Both sides mobilised, and the association saw a heavy increase of members of Russian origin who entered the association to support the lease. An extra annual meeting was interrupted by turmoil and police were summoned. This led to the board of Saint Sigfrid being split into two, with the "Russian side" taking control of the building.

20 Jacob Zetterman, "Rysk-Ortodox församling vägrar lämna kyrkan: 'De har bytt ut låsen'," *Dagen*, April 23, 2024, https://www.dagen.se/nyheter/2024/04/23/nu-stammer-st-sigfrids-kyrka-rysk-ortodoxa-forsamlingen-som-vagrar-lamna/.

21 Patrik Oksanen, *Rysslands hemliga krig mot Sverige* (Volante, 2025). p. 198-199.

22 Ibid. p. 200.

23 Kjetil Kjær Andersland and Shad Madian, "Russere Kjøpte Eiendom Ved Marinebase," *Dagbladet Bergen*, October 17, 2022, https://bergen.dagbladet.no/nyheter/russere-kjopte-eiendom-ved-marinebase/77313186.

24 Located in Vardø, the most eastward corner in Norway.

25 NTB. "Russere Ville Bygge Kapell Ved Norsk Radaranleggid", *Document.no*, 12 April 2022. https://www.document.no/2022/12/04/russere-ville-bygge-kapell-ved-norsk-radaranleggid-18064965/.

26 Mike Winnerstig, "Tools of Destabilization. Russian Soft Power and Non-Military Influence in the Baltic States," *Totalförsvarets Forskningsinstitut*, December, 2014, https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--3990--SE.

27 Aili Vahtla, "Russian Orthodox Church Leader Metropolitan Eugene Leaving Estonia Tuesday," *ERR News*, February 6, 2024, https://news.err.ee/1609244574/russian-orthodox-church-leader-metropolitan-eugene-leaving-estonia-tuesday.

28 Kaitsepolitseiamet, "Annual Review 2023–2024," (Tallinn, 2024), https://kapo.ee/sites/default/files/content_page_attachments/Annual%20review%202023-2024.pdf.

29 Aili Vahtla, "Estonian Parliament Slams Moscow Orthodox Church Backing Russian Agression," *ERR*, May 6, 2024. https://news.err.ee/1609333857/estonian-parliament-slams-moscow-orthodox-church-backing-russian-aggression.

30 Mait Ots and Helen Wright, "President Sends Church Foreign Influence Back to Riikikogu," *ERR*, April 24, 2025. https://news.err.ee/1609673975/president-sends-church-foreign-influence-law-back-to-riigikogu.

Discussion & Conclusions

Patrik Oksanen, Minna Ålander

Despite Russia's best efforts, the accelerated sabotage campaign in Europe reflects its inability (so far) to undermine Western support for Ukraine. As the Estonian Foreign Intelligence Service put in its 2025 public report, "This campaign, led by Russian special services, is intended to spread fear and confusion, driving Western nations away from supporting Ukraine."[1] The Finnish Security and Intelligence Service came to the same conclusion, but added that, "the attacks are aimed at simple and readily accessible targets that are of symbolic or secondary importance in terms of actual support for Ukraine, such as shopping centres or other less well-protected sites."[2] The increasingly brazen sabotage campaign that relies on recruiting non-professional proxies reflects Russia's otherwise diminished ability to operate and conduct influence campaigns, as European countries have expelled Russian "diplomats" working as intelligence agents.

The Finnish Security and Intelligence Service identifies the Russian Military Intelligence Service (GRU) as the main actor behind the sabotage campaigns. Rather than significantly disrupting military support logistics for Ukraine, Russia aims to influence opinions and the general sense of public safety, while imposing a burden on public authorities. But as GRU is the driving force of the operations, they also follow military aims.[3] The Estonian Military Intelligence service notes, however, that the strategy is not without risks: "Russia's covert sabotage operations have consistently backfired, reinforcing the prevailing perception of Russia as a hostile force rather than achieving any strategic advantage."[4]

While Russia's war aims in Ukraine and the resulting confrontation with the rest of Europe currently define its actions, Russia's hybrid warfare is not a consequence of Western support for Ukraine. It is therefore important to have a full understanding of Russia's history of using hybrid warfare tools well before its full-scale invasion of Ukraine in February 2022, and to recognise patterns in Russia's behaviour.

This book highlights that Russia utilises the full toolbox at its disposal, which it has been developing over the past several decades. The Kremlin does not feel bound by legal or moral scruples and malign actions support Russia's long-term strategic aims. Russia demonstrates ruthlessness in its decision-making when it comes to disrespecting international law and human lives, and a general willingness to take more risks than Western decision makers. An updated threat assessment by the Danish Military Intelligence Service estimated in February 2025 that Russia's willingness to take risks is likely to further increase, if the force correlation continues to develop in Russia's favour.[5]

Beyond the current war aims in Ukraine, Russia's activities serve the Kremlin's long-term objectives:

- Make Russia Great Again: This objective means a return to Russia's historical realm that includes, at the very least, Belarus and Ukraine. This is a frontal attack on the international order as well as neighbouring countries' sovereignty. According to the Russian worldview, only great powers are fully sovereign. In the Kremlin's thinking, this implies a natural given right to territorial demands (as in the current war in Ukraine), spheres of influence over neighbouring countries, and to dictate the European security order, exemplified by the list of demands for Eastern and Northern Europe that Russia issued to NATO in December 2021.[6]
- Regime survival: For Putin and his inner circle of elites, the idea of a threatening West has long prevailed in the Kremlin corridors. Consequently, norms and values that we in the West take for granted, such as human rights, democracy, political accountability and rule of law, are perceived as existential threats to the power structure Putin has built. In order to secure power, the Kremlin ruling elite fortifies itself with authoritarian, and increasingly totalitarian, rule and exports the image of Russia as a conservative and traditional alternative to the "decadent" West. In this worldview, a successful, democratic, and European Ukraine is a direct threat to the regime.

These goals lead Russia to pursue the following strategies:

- Breaking down the respect of a rules-based order and the European security order based on the Helsinki Final Act of 1975.[7] A breakdown would mean

a return to a "Congress of Vienna" order and the end of the UN and OSCE as we know them.[8]
- Ending and reversing NATO enlargement through undermining and ultimately breaking the credibility of NATO's Article 5 and thus the alliance's collective deterrence and very existence.
- Severing the transatlantic link through U.S. withdrawal from Europe, rendering Europe effectively defenceless, at least in the short-term.
- Breaking up the European Union as a political and economic bloc through undermining democracy in member states and promoting authoritarian parties friendly to the Kremlin, like in Hungary and increasingly in Slovakia.

The Nordic-Baltic Region: A Testing Ground for Russia's Hybrid Tools

Membership in the EU and/or NATO adds layers of protection to the democratic political systems of the Northeastern flank countries—a development Moscow views as a threat to its national interests, prompting Russia to seek ways to undermine EU cohesion and challenge NATO's deterrence.[9] Due to the loss of Russian economic, diplomatic, and political influence in Europe, it is likely that we will see increased physical hybrid activities, potentially in concert with military activities (exercises, posturing, and signalling). European leaders struggling to effectively quickly respond to such actions creates a permissive environment for Russia.

According to the Finnish Security and Intelligence Service, Russian sphere-of-influence thinking means that it "views small countries […] a zone of operations that serves the interests of major powers. Russia envisages a world in which small states should become satellites of larger states that may disregard their interests when a few large countries settle matters between themselves."

Swedish Military Intelligence bluntly states that Russia sees itself in a strategic conflict with the West and thinks it has the right to define what states are in its influence sphere:

> "Russia is using all its instruments of power in the conflict: military, political, diplomatic, information operations, cyberattacks, sabotage, and more—all with the aim of influencing developments … Russia's strategic objectives have been clearly articulated by its leadership for a long time. These objectives are: a new European security order, the right to a distinct Russian sphere of influence in which Russia defines which countries are included and the stability of its own regime."[10]

The Finnish Security and Intelligence Service also emphasises that the Baltic Sea is of major significance to Russia. The shadow fleet is currently the most economically and logistically viable option for Russia to evade sanctions on crude oil, which is crucial for Russia's economy and continued capacity to wage war.[11]

It is crucial for the Nordic and Baltic countries to be resilient enough to absorb the hybrid attacks and to endure the Russian threat in the long run. The region has, in fact, demonstrated a high level of resilience, as none of the sabotage incidents have so far led to major disruptions. But one should not underestimate the long-term effects of the attacks, both when it comes to psychological and economic effects. Russia is playing the long game; the attacks conducted so far can be seen as partly a dress-rehearsal for the next level of the hybrid war.

This means that, as we build greater resilience, it is increasingly important to take action and build deterrence against Russia as well. NATO's European deterrence and defence concept should be broadened to include countering and responding to sub-Article 5 hybrid attacks. Lessons learned from countries such as Ukraine and Moldova should be integrated into such work and adapted to region-specific vulnerabilities.

Hybrid threats exploit weaknesses within societies and between Western countries. Furthermore, in Russian thinking, it is also an activity that can be applied persistently across the spectrum of conflict and peace. It is therefore essential to build structures that are able to track and preemptively deter Russia in the hybrid sphere. The Nordic-Baltic region, a longtime target of Russia's hybrid attacks, has taken important steps to improve the understanding of the scope and speed inherent in hybrid challenges and to maintain an overview that enables accurate analyses of the situation. However, there is still room to

improve communication and cooperation between domestic departments and intelligence agencies, as well as among the Nordic and Baltic countries—particularly given their shared geography and the likelihood that much of Russia's activity is coordinated to undermine the region as a whole.

This will require the introduction of a new security culture that fully understands the complex and comprehensive threat in the wider Northern region. This also means accepting that hybrid threats are not theoretical or negligible, but part of a war that has been ongoing for a long time below the threshold of armed conflict. The cases in this book illustrate the variety of methods through which this warfare is conducted.

It is also important to understand that Russia often acts opportunistically and experiments with different approaches, reaping benefits and replicating strategies whenever they work.[12] One of the best such examples was the case in May 2024 when the Russian Ministry of Defence uploaded a document on its website, suggesting that its maritime borders with Finland and Lithuania should be reassessed. The document initially disappeared after a few hours, without much comment from the Kremlin. But after noticing the panicked reaction to the document in Europe, Russia capitalized on the incident in the information sphere by moving border markers in the Narva river between Russia and Estonia.[13] On the other hand, the case presented a rare opportunity for a symmetric response, as the Finnish Ministry of Foreign Affairs initiated the regular reassessment process of the maritime borders due every 30 years, with the last time in 1995.[14]

The examples from the Nordic-Baltic region underline the value of collecting and sharing information in order to achieve a greater situational awareness of Russian activities encompassing the whole region. It is crucial that the Nordic and Baltic countries increase their capability to uphold deterrence by denial. This requires achieving a sufficient level of resilience to dilute the effect of the attacks (to the point of rendering them counter-productive) and having the capability to meet an attack with countermeasures that degrade the aggressor's capability to inflict harm. Doing so requires a mix of increased military surveillance presence (such as NATO's Baltic Sentry vigilance operation) and closing legal gaps (such as the Finnish property laws or extended authority to conduct insurance checks on suspected shadow fleet vessels in Sweden).

Another tool is deterrence by punishment. The aggressor should know that e.g. a successful cyber attack has tangible consequences. The response can be asymmetric but still relevant, such as the EU's hybrid sanctions on the responsible individuals and entities.[15] In all of the above cases, it is important to have appropriate responses ready: be it holding the aggressor and its cronies accountable politically, legally, diplomatically, and economically; as individuals or legal entities, or, if more advantageous, choosing the option of non-attribution and covertly striking back, for example with a tit-for-tat cyber attack.

Still, these measures are defensive in nature, even if a punitive counter-operation is in itself offensive. The questions the West needs to answer if it wants to win the hybrid war against Russia are: 1) what does victory look like and 2) how do we achieve it? Today, the political will rise to the level of simply not losing the day, and our policy proposals are fit for this level of contentment, but we suggest the need for exploring another strategy—a strategy to win.

A Permanent Hybrid Response Mechanism

Although the hybrid threats must first and foremost be dealt with on the national level, the nature of the threat means that the best strategy includes a concerted effort with like-minded allies. The EU and NATO levels are crucial in many ways, but larger organisations are often slowed down by unanimous decision-making and long bureaucratic processes. Sometimes a swift response is needed. Strategically, after Finland and Sweden's NATO accession, the Arctic and Baltic sub-regions have become one operational area. The Nordic-Baltic 8 (NB8) format and other frameworks including like-minded allies such as Poland in the NB8+PL format or NB8 with the UK and the Netherlands in the Joint Expeditionary Force (JEF) can offer suitable frameworks for facilitating such consultations and coordination.

In order to meet hybrid threats with an improved situational awareness in a coordinated manner, we propose a permanent NB8 mechanism for alerting members of incidents and creating awareness of patterns through data collection and information sharing. This mechanism may also be used to build a capacity to inflict costs on the aggressor that are higher than any one country could achieve on its own. And of course, be open for other NATO members to join.

A permanent coordination mechanism—with dedicated resources for analysis and response planning—would improve reaction times and enable preventive measures, compared to the current reactive and ad hoc coordination. Because of the varied nature of hybrid threats and the strategic importance, we advise that the mechanism be tied directly to the offices of the sitting prime ministers or presidents instead of being delegated to a ministry (e.g. Ministry of Foreign Affairs, Ministry of Defence or Ministry of Justice). A functioning NB8 mechanism would also strengthen the EU and NATO's efforts on hybrid threats by facilitating faster and more inclusive participation from other allies while actions at the EU and NATO levels are still being processed.

Furthermore, since many communication platforms and strategic sectors vulnerable to hybrid interference are owned and operated by private companies rather than the government, it is essential from a total defence perspective to integrate the private sector (e.g. national confederations of business and enterprises) into the coordination mechanism. Currently, private companies lack incentives to report incidents that do not cause disruptions for consumers, which leads to incomplete situational awareness by governments. Private sector inclusion can thus serve as both a channel for feeding data on observed or experienced activities, and a means of sharing and learning best practices for protection against attacks. Since hybrid threats present a whole-of-society threat, a whole-of-society approach is needed in response. This is a well-established part of the Nordic total defence concept.

The hybrid threats are real, severe and defence against them can not wait. Urgency must be the watchword.

References

1 Estonian Foreign Intelligence Service, "Russia resorts to violence to sow fear and confusion in the West," in: Foreign Intelligence Service Public Report 2025, https://raport.valisluureamet.ee/2025/en/4-russian-influence-activities/4-1-russia-resorts-to-violence-to-sow-fear-and-confusion-in-the-west/.

2 Finnish Security and Intelligence Service, "Russia seeks to influence European countries through sabotage," in: National Security Overview 2025, https://katsaus.supo.fi/en/russian-sabotage-in-europe.

3 Ibid.

4 Estonian Foreign Intelligence Service, "Russia resorts to violence to sow fear and confusion in the West," in: Foreign Intelligence Service Public Report 2025, https://raport.valisluureamet.ee/2025/en/4-russian-influence-activities/4-1-russia-resorts-to-violence-to-sow-fear-and-confusion-in-the-west/.

5 Forsvarets Efterretningstjeneste, "Opdateret vurdering af truslen fra Rusland mod Rigsfællesskabet," February 9, 2025, p. 1, https://www.fe-ddis.dk/globalassets/fe/dokumenter/2025/trusselsvurderinger/-20250209_opdateret_vurdering_af_truslen_fra_rusland_mod--.pdf.

6 Gabrielle Tétrault-Farber and Tom Balmforth, "Russia Demands NATO Roll Back from East Europe and Stay out of Ukraine," *Reuters*, December 17, 2021, sec. World, https://www.reuters.com/world/russia-unveils-security-guarantees-says-western-response-not-encouraging-2021-12-17/.

7 OSCE, "Conference on Security and Co-Operation in Europe Final Act Helsinki 1975," August 1, 1975, https://www.osce.org/files/f/documents/5/c/39501.pdf.

8 Randall Lesaffer, "The Congress of Vienna (1814–1815)," *Oxford Public International Law*, n.d., https://opil.ouplaw.com/page/477.

9 Karen-Anna Eggen, "Designing around NATO's Deterrence: Russia's Nordic Information Confrontation Strategy," *Journal of Strategic Studies*, 2024, 1–25, https://doi.org/10.1080/01402390.2024.2332328.

10 Swedish Military Intelligence (MUST), "Musts årsöversikt", 2025. https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/musts-arsoversikter/must-arsoversikt-2024.pdf.

11 Finnish Intelligence and Security Service, "Russia is reorienting globally", in: National Security Overview 2025, https://katsaus.supo.fi/en/russia-is-reorienting-globally.

12 Finnish Security and Intelligence Service, "Russia seeks to influence European countries through sabotage", in: National Security Overview 2025, https://katsaus.supo.fi/en/russian-sabotage-in-europe.

13 AP News, "European Union criticizes Russia for removing Estonian buoys, demand an explanation from Moscow," *AP News*, May 24, 2024, https://apnews.com/article/estonia-russia-buoys-border-10b99970ed538ce1684bf88c6384a1ec.

14 Jarmo Huhtanen, "Suomi aloitti merirajan tarkistamisen," *Helsingin Sanomat,* May 31, 2024, https://www.hs.fi/suomi/art-2000010458909.html.

15 An example of an effective asymmetric measure was the Salisbury novichok poisoning of the Scripals in 2018 when more than 150 Russian intelligence officers with diplomatic passports were expelled from 30 countries. For the EU's hybrid sanctions, see: Council of the European Union, "Russian hybrid threats: EU lists further 21 individuals and 6 entities and introduces sectoral measures in response to destabilising activities against the EU, its member states and international partners", May 20, 2025, https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/.

Afterword

For too long there has been a misunderstanding that war is only fought on the battlefield, with tanks, planes, and guns, while all other hostilities exist within a "grey zone" of peace. As this book has shown, this is a dangerous misunderstanding.

Russia's hybrid war is indeed a real war waged against the West. In this war, the whole of society is a target. The more we understand Russia's methods and goals, the better equipped we are to defend our democracies.

Hybrid warfare is an integral part of how Russia wages war. Hybrid attacks test not only our preparedness and resolve ahead of a conventional war, but seek to undermine infrastructure vital for societal functioning and military capabilities, divide our societies, and reshape the political landscape in Russia's favor. Failure to respond effectively only invites further aggression.

Europe must defend itself. Credible deterrence requires not only the ability to prevent an attack, but to respond and inflict damage to defeat the adversary. Without clarity on the nature of the threat and the identity of the aggressor, we can do very little. This book has provided such clarity.

The Stockholm Free World Forum is proud to have collaborated with the Konrad Adenauer Stiftung. Leveraging our shared resources and knowledge, we have aimed to foster a shared threat perception across Europe. This book, building upon a previous report "Tracking the Russian Hyrbid Warfare - Cases from Nordic Baltic Countries" (2024) represents the next step in our joint efforts to enhance European preparedness and resilience against ongoing hybrid attacks.

It is high time to act and defend ourselves in a war that is already underway.

Gunnar Hökmark
Chairman of Stockholm Free World Forum

Editors

Minna Ålander is a research fellow at the Finnish Institute of International Affairs (FIIA) in Helsinki and a non-resident fellow at the Center for European Policy Analysis (CEPA) in Washington, D.C. Her research focuses on NATO, security in Northern Europe, Nordic defense cooperation, Arctic security, as well as German and Finnish security and defense policy. Previously, Ålander worked at the German Institute for International and Security Affairs (SWP) in Berlin.

Patrik Oksanen is a resident senior fellow at Stockholm Free World Forum (SFWF), with responsibility for CIDA (Center for Influence and Disinformation Analysis) at SFWF. Oksanen is a member of the Royal Swedish Academy of War Sciences and Royal Swedish Society of Naval Sciences and is also associated with the Centre of Societal Security at the Swedish Defense University. He appears regularly as a columnist and commentator for various Swedish media. Oksanen has a background as a TV journalist and political editor, and has contributed to various books on matters related to security, total defense and influence operations. The most recent is "*Rysslands hemliga krig mot Sverige*" (Russia's Secret War Against Sweden) which entered the bestselling lists upon release.

With contributions from

Dr. Ieva Bērziņa is a Senior Researcher at the Center for Security and Strategic Studies, National Academy of Defense of the Republic of Latvia, and an associate professor at Vidzeme University of Applied Sciences. Her current research interests cover comprehensive national defense, strategic communication, Russia's strategy and communication, patriotism, and nationalism.

Karen-Anna Eggen is a researcher and Head of the Programme for Ukraine and Full-Spectrum Threats at the Norwegian Institute for Defense Studies. Eggen finalized her PhD on *Russia's Contemporary Grand Strategy: The Use of Information and Other Unconventional Means Towards the Nordic Region in 2025*. Before her doctorate, Eggen was employed as a Researcher and Program Coordinator for IFS's research program Security and Defense in Northern Europe (SNE). She has previously worked as an adviser in the Norwegian Atlantic Committee and had various engagements at the Norwegian Consulate General in St. Petersburg, Russia Eggen has been a member of the board of Human Rights House Foundation since 2023 and is also on the board of Sønsteby-fondet as per 2025.

Bjarni Bragi Kjartansson is an independent researcher, lecturer, and columnist specialising in hybrid threats. He has developed courses on hybrid threats, taught at the University of Iceland and Bifröst University, and contributed numerous articles on international affairs to the Icelandic media outlet Kjarninn (Heimildin).

Marek Kohv is the Head of the Security and Resilience Programme at the International Centre for Defence and Security (ICDS) in Tallinn. He is a Research Fellow with expertise in hybrid warfare, intelligence and information operations and has a background in Estonian Defense Forces and Government.

Dr. Aleksander Olech is the Head of International Cooperation at Defence24 and a lecturer at several national and international universities. His work focuses on international security, NATO policy, hybrid threats, and strategic communication. Dr. Olech has collaborated extensively with several NATO Centres of Excellence. Previously, he served as Deputy Director of the Department of Africa and the Middle East at the Polish Ministry of Foreign Affairs. He is a graduate of the European Academy of Diplomacy and the War Studies University.

Adam Roževič is a political analyst at Geopolitics and Security Studies Center. He is responsible for GSSC's research and analysis directions, ensures the distribution of publications, coordinates high-level events, and contributes to the organization's smooth operations as well as research on security and defense topics. Adam's main research interests are security and defense policies of the NATO eastern flank.

Dr. Jeanette Serritzlev is a military analyst at the Royal Danish Defense College, specializing in information warfare and hybrid threats, especially in regards to Russia. Since the Russian invasion of Ukraine in February 2022, she has been researching the information side of the war. She is the author of the book *Information War—Influence and Propaganda in Modern Warfare* (2023) and has contributed to other books and reports on matters of information warfare and disinformation.

Dr. Frank Umbach is Head of Research of the European Cluster for Climate, Energy and Resource Security at the Center for Advanced Security at the Strategic and Integration Studies and Adjunct Senior Lecturer at University of Bonn, Germany. He also is an Adjunct Senior Fellow at the S. Rajaratnam School of International Studies at the Nanyang Technological University in Singapore. As a senior consultant, his areas of expertise include energy security, resource and raw material supply resilience, cyber security and critical energy infrastructure protection, as well as maritime security policies. Since 2012, he has served as a NATO-consultant on energy and resource security. Dr. Umbach has published several books and numerous articles in more than 30 countries worldwide.

Northern Europe is not at peace. The battle is real and far more dangerous than the public has grasped. In this war, there are no frontlines. Attack vectors shift daily, probing weaknesses, exploiting vulnerabilities, and seizing opportunities.

The weapon of choice is what we in the West call hybrid warfare, targeting our institutions, our infrastructure, our alliances, and our minds. Resilience is necessary, but not sufficient, to win this hybrid war.

This book shows how countries on the northern flank are strengthening national capabilities and deepening cross-border cooperation to detect, disrupt, and respond to hybrid threats—offering a blueprint for hybrid deterrence.

9 789198 850031