EUROPEAN LEADERSHIP NETWORK | Building better security for wider Europe

Countering Russia's Hybrid Threats in the Arctic

Katarina Kertysova and Gabriella Gricius

August 2023

Report Authors

Katarina Kertysova and Gabriella Gricius

Contributors

Sir Graham Stacey

Review

Sir Adam Thomson, Adája Stoetman, Elizabeth Buchanan

This project was conducted by the European Leadership Network (ELN) and funded by the Russia Strategic Initiative, U.S. European Command. The views expressed in this publication are solely those of the authors and do not necessarily represent the views of the U.S. Department of Defense or of the European Leadership Network.

Contents

Introduction

Russia’s war of aggression against Ukraine is producing ripple effects that reverberate far beyond Ukraine.[1] Such effects are felt in the Arctic region[2], which has been considered by some as a strategic low-tension zone, compartmentalized and insulated from broader developments in Russia-West and Russia-NATO relations since the end of the Cold War. While Russia’s military build-up in parts of the Arctic region shows no sign of slowing down, the Kremlin does not seem to be interested in any spillover of the war in Ukraine to the Arctic. Any direct confrontation with NATO would be detrimental to the economic development and Russia’s commercial interests in the Arctic.[3] While hazardous military incidents and unintended escalation cannot be ruled out, especially given the visible increase in military activity in the Arctic, hybrid warfare and interference through non-military means will likely be Russia’s preferred strategy in the Arctic moving forward.

Russia’s turn to hybrid interference is neither new nor confined to the Arctic and its influencing activities come in many shapes and sizes, constituting part of a larger hybrid campaign that targets society as a whole. Hybrid activities that have been observed in the Arctic encompass information operations (including disinformation), cyber attacks, material interference (targeting of pipelines and undersea cables), GPS jamming, and more traditional tactics like espionage and energy intimidation.[4]

Hybrid warfare remains a contested concept and there is no generally accepted definition of the term. It was popularized by General James Mattis in a 2005 speech and expanded on by Frank Hoffmann in 2007. According to a definition provided by Hoffman, “hybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.”[5] Some scholars, such as Elisabeth Braw of the American Enterprise Institute (AEI), draw distinctions between gray zone aggression and hybrid warfare. While hybrid warfare involves “persistent use of military force and non-armed aggression”, gray zone aggression is “the use of hostile acts outside the realm of armed conflict to weaken a rival country, entity, or alliance,” Braw writes.[6] The European Centre of Excellence for Countering

[1] See, for example, Andrea Kendall-Taylor et al., “Russia in the Arctic: Guaging How Russia’s Invasion of Ukraine Will Alter Regional Dynamics” (Center for a New American Security, September 2022).

[2] The term “Arctic” refers to the region within the Arctic Circle – the line located at latitude 66° 33' North of the Equator. The Arctic region consists of the partly ice-covered Arctic Ocean and land areas of the surrounding eight Arctic states: Canada, Denmark, Finland, Iceland, Norway, Sweden, Russia and the United States.

[3] Katarina Kertysova, “What Are the Main Drivers behind Russia’s Military Build-up in the Arctic?,” May 4, 2020, https://www.europeanleadershipnetwork.org/commentary/what-are-the-main-drivers-behind-russias-military-build-up-in-the-arctic/.

[4] See, for example, Andreas Osthagen, “The Arctic after Russia’s Invasion of Ukraine: The Increased Risk of Conflict and Hybrid Threats” (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, May 2023).

[5] Frank Hoffman, “Conflict in the 21st Century: The Rise of Hybrid Wars” (Arlington, Virginia: Potomac Institute for Policy Studies, December 2007), 14.

[6] Elisabeth Braw, *The Defender’s Dilemma: Identifying and Deterring Gray-Zone Aggression* (Washington, DC: American Enterprise Institute, 2022), 9–10.

Hybrid Threats (hereafter "Hybrid CoE") defines hybrid threats as "actions conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means."[7] This definition does not contrast "hybrid warfare" with kinetic war but instead stresses the interplay of military and non-military means. For the purpose of this report, we rely on the definition provided by Hybrid CoE, as it provides a wider aperture to better capture the nuanced and ever-changing nature of hybrid threats.

This study aims to identify and explore how hybrid threats manifest in the Arctic, areas that are susceptible to influence, potential targets, actors who wish to shape public opinions, as well as the objectives being pursued. It first examines the threat and vulnerability landscape in the Arctic and outlines individual country profiles of the seven Western Arctic states that were subjected to research, namely the United States, Canada, Iceland, Denmark, Finland, Sweden, and Norway. The assessment of four key trends follows. More specifically, the report looks at the increase in 1) Russian cyber activity, 2) critical infrastructure interference, 3) espionage and intelligence operations, and 4) mounting information influence operations (including disinformation) in the Arctic. The report then discusses Finland as a good example for other Western Arctic states to follow. Next, the report evaluates the viability of a regional joint response mechanism towards hybrid threats. Finally, it offers a series of recommendations to address hybrid interference in the Arctic (outlined below and discussed in detail later in this report):

1. Know one's weaknesses and improve situational awareness
2. Enhance transparency and public communications
3. Establish good governance structures
4. Foster quality education and critical media literacy
5. Training and exercising
6. Crisis preparedness
7. Break down silos and encourage horizontal coordination
8. Cooperate within coalitions and capitalize on existing frameworks
9. Avoid unintentional escalation in the Arctic
10. Broaden social inclusion
11. Invest effort in understanding Russian intent

Methodological approach

Given the limited size of the project, we conducted our analysis primarily on the basis of existing literature (official documents and secondary sources) and the available data. Desk research was supplemented by interviews with both academics and practitioners in the seven Western Arctic states and a research trip to Finland. In the next step, the interview results were complemented by information gleaned at two workshops: one research meeting involving the Arctic expert community and one validation meeting comprising ELN network members.

[7] "Hybrid Threats" (The European Centre of Excellence for Countering Hybrid Threats, n.d.), https://www.hybridcoe.fi/hybrid-threats/.

Threat and vulnerability landscape

Vulnerability can be understood as a condition that increases the susceptibility of an individual, a community, assets, or systems to harm. Several reports produced by the Hybrid CoE recognize that the Arctic region presents "unique geographical, social, political, economic and military conditions that constitute significant drivers of vulnerability".[8] Understanding the complexity and vulnerability of the Arctic is key to designing effective strategies to counter hybrid threats.

When compared to the populations of other geographical regions, the Arctic communities are small, geographically dispersed and often isolated. The city of Tromsø, for instance, has a population of 76,000 inhabitants, which makes it one of the largest cities in Northern Norway. In contrast to the European and Russian Arctic, the population density is particularly low in the Alaskan Arctic and the Canadian North, which has a small population of just over 100,000 Canadians.[9]

Arctic populations generally experience lower levels of economic development, with socio-economic disparities being most prevalent between northerners and southerners, and between Indigenous and non-Indigenous Arctic residents.[10] Additionally, the capitals are located outside the Arctic circle, which creates significant distances between Arctic communities and decision-making centers. At times, Governments have by-passed northern communities in favor of pro-development interests. Not considering local preferences and knowledge when devising (development) policies that affect the region can breed resentment and exacerbate contentious dynamics between local actors and the government, which malign actors might seek to exploit. Colonial legacies and the history of forced assimilation policies aimed at Indigenous people, which is still to be reckoned with, can perpetuate mistrust towards authorities – and can be turned into a wedge issue, making it difficult for governments to forewarn or prepare exposed communities to deal with hybrid threats.

Given the composition of its residents, Svalbard (a Norwegian archipelago in the Arctic Ocean) is an interesting case in point. Almost 40% of its inhabitants are foreign-born – comprising primarily Russians, Thais, Swedes, Filipinos and Ukrainians – and have no familial or historical ties to Norway.[11] While in the past anyone living in Svalbard was allowed to participate in local politics, vote in local elections and serve as elected representative, in 2022 the Norwegian government effectively banned foreign political representation, which affected more than a third

[8] Gaelle Rivard Piche and Bradley Sylvestre, "Vulnerabilities and Hybrid Threats in the Canadian Arctic: Resilience as Defence" (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, May 2023); Osthagen, "The Arctic after Russia's Invasion of Ukraine: The Increased Risk of Conflict and Hybrid Threats."

[9] Piche and Sylvestre, "Vulnerabilities and Hybrid Threats in the Canadian Arctic: Resilience as Defence."

[10] Ibid.

[11] "Svalbard" (The World Factbook, July 6, 2023), https://www.cia.gov/the-world-factbook/countries/svalbard/.

of residents.[12] This change of voting rights, coupled with pre-existing inequalities and polarization between Norwegian and non-Norwegian residents, provides foreign actors with ample opportunities to inflame internal divisions, influence those who feel they have been wronged, and meddle in the affairs of the archipelago.

Russia could also seek to use its “compatriots abroad” policy as a tool of influence in the Arctic, leveraging the presence of Russian-speaking minorities in the countries concerned to advance the Kremlin’s interests in the region. Russian speakers are present in Finland, Norway and – to a lesser extent – Sweden. Alaska has been home to a community of Russian “Old Believers” for over 50 years now. “Rossotrudnichestvo” – the main state agency projecting the Kremlin’s soft power and hybrid influence – has a presence in Finland, Denmark and Canada.[13] While the Russian minority in Norway has been found to be sympathetic towards Russia and Mearsheimer-style argumentation, Russian speakers living in Finland have taken a critical stance towards the Russian aggression against Ukraine.[14] The extent to which Russia has been able to weaponize cultural, religious and historical affinities, find fertile ground for disinformation, and how active (and effective) “Rossotrudnichestvo” has been in the three Arctic countries where it has physical presence is a relevant area for further research as it has not been comprehensively researched thus far.

Other regional specificities – like remoteness, limited critical and military infrastructure, telecommunications connectivity gaps, incomplete situational awareness as well as monitoring difficulties – add to the list of vulnerabilities that make the Arctic region susceptible to hybrid threats. Because assets and systems located in austere Arctic conditions were not considered targets until recently, and were not subject to stress testing,[15] the countries concerned are unlikely to be adequately prepared to face possible attacks.

[12] Nina Berglund, “Svalbard’s Foreign Residents Lose Their Voting Rights,” *NewsInEnglish.No*, June 20, 2022, https://www.newsinenglish.no/2022/06/20/foreigners-in-svalbard-lose-voting-rights/.

[13] “Representations of Rossotrudnichestvo,” n.d., https://studyinrussia.ru/upload/embassy/Appendix-1.pdf.

[14] Interview results; “Survey: One Third of Finland’s Russian Speakers Think Russia Violated Ukrainian Sovereignty,” *YLE News*, June 6, 2022, https://yle.fi/a/3-12478546.

[15] The European Union recognizes stress testing as an important element of critical infrastructure resilience, particularly in the wake of the Nord Stream sabotage. However, it has not been implemented EU-wide. “Critical Infrastructure: Commission Accelerates Work to Build up European Resilience” (European Commission, October 18, 2022).

Country profiles

North American Arctic

Our findings suggest that North American Arctic countries (**Canada** and the **United States**) have not been targeted to the same extent as their European counterparts.[16] While there is evidence of attacks in the cyber domain, critical infrastructure in Alaska or Canada has not been interfered with to date. At the same time, there has been no shortage of foreign efforts to spy on sensitive military assets. In 2021, the Canadian military discovered (and retrieved) Chinese monitoring buoys in the Arctic Ocean, and in 2023 the US shot down a suspected Chinese surveillance balloon – after it flew across Alaska and Canada, gathering intelligence from sensitive military sites. Most recently, Chinese nationals, posing as tourists, made multiple attempts to enter US military bases in Alaska with a drone inside their vehicle.[17]

When it comes to information operations and societal interference, the North American Arctic is less populated than the European Arctic, meaning that the potential target audience is smaller. Nevertheless, as has been mentioned above, the unique social, economic and political conditions make Arctic communities particularly susceptible to foreign interference. One prominent example of information influencing was a 2017 smear campaign against then-Arctic policy advisor for Alaska Craig Fleener, in which his statements were "reinterpreted" to imply that Alaska would be better off under Russian leadership.[18] In a similar vein, Canada's Deputy Prime Minister and Minister of Finance Chrystia Freeland has been a frequent target of pro-Kremlin outlets, which label her as a "Nazi whitewasher".[19] Canada, which has the world's second-largest Ukrainian diaspora, has also had to grapple with narratives aimed at stoking anti-Ukrainian sentiments. Equally noteworthy is a pro-China covert influence operation uncovered in 2022 – known as "Dragonbridge" – which sought to protect China's global rare earths market dominance by thwarting foreign competition in the US and Canada.[20]

[16] Evidence in the public domain is missing with regard to Canada and the United States successfully being targeted.

[17] Tom Vanden Brook, "Suspected Chinese Spies, Disguised as Tourists, Tried to Infiltrate Alaskan Military Bases," *USA Today News*, May 31, 2023, https://eu.usatoday.com/story/news/politics/2023/05/31/suspected-chinese-spies-posing-as-tourists-discovered-in-alaska/70260712007/.

[18] Jeanette Lee Falsey, "Alaska's Arctic Policy Adviser Falls Victim to Fake News - in Russia," *Anchorage Daily News*, April 12, 2017, https://www.adn.com/arctic/2017/04/11/alaskas-arctic-policy-adviser-falls-victim-to-fake-news-in-russia/.

[19] Marcus Kolga, "Confusion, Destabilization and Chaos: Russia's Hybrid Warfare against Canada and Its Allies" (Canadian Global Affairs Institute, October 2021), https://www.cgai.ca/confusion_destabilization_and_chaos_russias_hybrid_warfare_against_canada_and_its_allies.

[20] Piche and Sylvestre, "Vulnerabilities and Hybrid Threats in the Canadian Arctic: Resilience as Defence."

Norway

Norway has had to grapple with a variety of hybrid threats since as early as 2015, when Russia allowed thousands of asylum seekers to cross into Norway (and Finland).[21] Disruptions of GPS signals in Northern Norway, which Russia has been accused of since at least 2017, is equally worrying. Russian GPS-jamming has been reported to have reached "unprecedented levels" following the outbreak of the war in Ukraine. The threat of spying on critical and military infrastructure has increased as well. Throughout 2022, several Russian citizens were arrested for illegally flying drones and taking photographs near sensitive locations. The same year, Bishop Aleksandr of Plesetsk floated the idea of building a Russian Orthodox Chapel just next to a military radar complex in Vardø, operated by the Norwegian Intelligence Service.[22] The same radar complex – located just 50 kilometers from the border with Russia – was subject to a Russian mock attack back in 2018.[23] Additionally, critical subsea cables were targeted on two separate occasions: in April 2021, an undersea surveillance network off the coast of Northern Norway, capable of detecting submarines, was cut, followed by a disruption to the main fiber-optic cable connecting Svalbard to Norway in January 2022. As regards information influencing, the Norwegian Intelligence Service recognizes that Russian influence operations have become more sophisticated, relying on more platforms, country-by-country specific messaging, and fake profiles. The North-South divide[24] and the presence of Russian speakers supporting the war provide ample opportunities for Moscow to deepen the cracks and inflame existing divisions. Finally, it was reported that in 2019, a Beluga whale wearing a Russian-made camera harness approached a Norwegian fishing boat in Finnmark. Norwegian officials assume that either 1) the whale escaped from a Russian military facility, or 2) the whale was dispatched for spying purposes.[25] A beluga whale was spotted again in May 2023 off the coast of southwestern Sweden.[26]

Denmark, Greenland, and the Faroe Islands

The inherently fraught relationship between Denmark and its self-governing territories of Greenland and the Faroe Islands constitutes an easy target for malign actors to exploit. Russian (as well as Chinese) attempts to exacerbate existing tensions are well-documented. The fake letter affair of 2019 is a good case in point.

[21] Helena O'Rourke-Potocki, "Finland and Norway Tangle with Russia over Migrants," *POLITICO*, January 25, 2016, https://www.politico.eu/article/finland-and-norway-tangle-with-russia-over-migrants-refugees-asylum-organized-crime/.

[22] Thomas Nilsen, "With Local Support, Bishop Aleksandr of Plesetsk Has a Desire to Build Orthodox Chapel next to Vardø Radar," *The Barents Observer*, November 10, 2022.

[23] Thomas Nilsen, "Eleven Russian Fighter Jets Launched a Mock Attack on a Norwegian Arctic Radar Installation," *Arctic Today*, February 13, 2019, https://www.arctictoday.com/eleven-russian-fighter-jets-made-a-mock-attack-on-a-norwegian-arctic-radar-installation/.

[24] The North-South divide refers to the economic, societal, and political distance between Northern and Southern Norway.

[25] Jan Olsen, "Norway Says Beluga Whale with Apparent Russian-Made Harness Swims South to Sweden," *AP News*, May 30, 2023, https://apnews.com/article/beluga-whale-norway-sweden-russia-4500803df50d82f30422886a614644ba.

[26] Elisabeth Braw, "Has Hvaldimir, Putin's Secret Weapon, Defected?," *Foreign Policy*, June 5, 2023, https://foreignpolicy.com/2023/06/05/hvaldimir-whale-spy-russia-putin-nato/.

A letter, supposedly drafted by Greenland's foreign minister Ane Lone Bagger, asked Republican senator Tom Cotton for money to fund a referendum on Greenland becoming independent from Denmark.[27] Danish experts have pointed to Russia and China for forging the letter, which circulated only days before Bagger's visit to Washington DC. The relationship between Denmark and the US constitutes another issue that foreign actors have sought to exploit. Disinformation campaigns depicting Denmark as a vassal state of the US, paired with narratives of lost sovereignty, have been commonplace.[28]

On top of information operations, Denmark and Greenland have also experienced an increase in cyber crime and espionage. One such example was an attack on the Greenlandic government in March 2022, which led to all meetings in the Inatsisartut (the Parliament of Greenland) being postponed because the Naalakkersuisut (the Cabinet of Greenland) was not able to communicate.[29] Another attack of a similar scale took place in May 2022, when the Greenlandic healthcare system was targeted.[30] As regards espionage, in April 2022 Denmark expelled 15 Russian diplomats on suspicion of spying for Moscow. A *2023 Assessment of Espionage Threats* maintains that threats to Denmark, Greenland, and the Faroe Islands remain high.[31] While the report does not consider physical sabotage against critical infrastructure within the Danish territory as likely, it acknowledges that the threat picture may change very rapidly, should a conflict escalate in the region. Infrastructure situated outside Danish territory – such as undersea pipelines and cables – might be at higher risk of sabotage. Looking ahead, the agreement to establish an air surveillance radar on the Faroe Islands – which the Faroese opposition party has objected to and criticized[32] – might be a target of future information operations.

Iceland

Given Iceland's strategic position in the North Atlantic, and plans to step up and formalize US military presence on the island, disinformation campaigns have focused on amplifying pacifist arguments and stoking anti-US sentiments among Icelanders. Pro-Kremlin media outlets regularly depict the US and NATO as destabilizing forces in the Arctic, suggesting that Iceland (and other Nordic states)

[27] Alistair Coleman and Matilda Welin, "Greenland Minister at Centre of Fake Letter Affair," *BBC News*, Noember 2019, https://monitoring.bbc.co.uk/product/c2018djo.

[28] See "EU vs Disinfo Database," n.d., https://euvsdisinfo.eu/disinformation-cases/.

[29] Nina-Vivi Moller Andersen and Thomas Veirum, "Naalakkersuisut: IT Problems Are Due to Serious Cyber Attacks," *Sermitsiaq*, March 31, 2022, https://sermitsiaq.ag/naalakkersuisutit-problemer-skyldes-alvorligt-cyberangreb.

[30] Thomas Veirum, "Cyber Attacks Cause Major Problems in the Healthcare System," *Sermitsiaq*, May 18, 2022, https://sermitsiaq.ag/cyberangreb-giver-store-problemer-i-sundhedsvaesenet.

[31] "Assessment of the Espionage Threat to Denmark, the Faroe Islands, and Greenland" (Danish Security and Intelligence Service (PET), May 2023).

[32] Lasse Sorensen, "Faroe Islands Agree to Install Radar to Boost Arctic Surveillance," *Courthouse News Service*, June 9, 2022, https://www.courthousenews.com/faroe-islands-agree-to-install-radar-to-boost-arctic-surveillance/.

would better function as a "buffer zone" or a "Switzerland of the North".[33] Pro-Russian actors also claim that Iceland would be better off without the EU or NATO. To better counter and respond to hybrid threats, Iceland joined the Hybrid CoE in December 2021.[34] The country's government also pays close attention to potential hybrid threats to the subsea cable system that connects Iceland to its neighbors. In June 2023, Iceland co-hosted a Security Forum on Critical Undersea Infrastructure in tandem with the Joint Expeditionary Force (JEF), which brought Allies and partners together to share best practices and deepen cooperation on critical undersea and offshore infrastructure protection.[35]

Cyber attacks are a growing concern for Iceland, too. In April 2022, Iceland's websites were subject to a series of sustained Distributed Denial-of-Service (DDoS) attacks, which took place in the wake of the Icelandic government's announcement that it would be increasing its defense budget. While some suspect Russian interference, as it stands, no direct attribution has been publicly announced.[36] In May 2023, Icelandic networks and computer systems suffered stress attacks in relation to the European Council Summit, which took place in Reykjavik. Websites of public institutions were down, with the Russian group NoName057(16) claiming responsibility.[37] In June 2023, Iceland's parliament, cabinet and tech companies were targeted by cyberattacks that are also believed to have originated in Russia.[38]

As elsewhere, the government considers it to be likely that Russia and other authoritarian regimes are engaged in espionage in Iceland.[39] While the government has not yet ruled on establishing a fully-fledged security or secret service in Iceland, a bill on the increased powers of the police has been put forward.[40] In 2023, Iceland adopted a new National Security Strategy, focusing on resilience and civilian activities – taking a holistic stance towards security issues.[41]

[33] P. Whitney Lackenbauer, Troy Bouffard, and Adam Lajeunesse, "Russian Information Operations: The Kremlin's Competitive Narratives and Arctic Influence Objectives," *Journal of Peace and War Studies* 4th edition (October 2022): 161–186.

[34] "Iceland Joins Hybrid CoE" (The European Centre of Excellence for Countering Hybrid Threats, December 10, 2021), https://www.hybridcoe.fi/news/iceland-joins-hybrid-coe/.

[35] "Security Forum on Critical Undersea Infrastructure Held in Iceland" (Government of Iceland's Ministry for Foreign Afairs, June 29, 2023), https://www.government.is/diplomatic-missions/embassy-article/2023/06/29/Security-Forum-on-Critical-Undersea-Infrastructure-held-in-Iceland/.

[36] Larissa Kyzer, "Icelandic Websites Under Cyber Attack," *Iceland Review*, April 15, 2022, https://www.icelandreview.com/sci-tech/icelandic-websites-under-cyber-attack/.

[37] "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/.

[38] Charles Czumski, "Islande: Des Cyberattaques Visent Des Sites Officiels et Des Entreprises Technologiques," *Euractiv*, n.d., 14 June 2023 edition, https://www.euractiv.fr/section/cybercriminalite/news/islande-des-cyberattaques-visent-des-sites-officiels-et-des-entreprises-technologiques/.

[39] Ragnar Tomas, "Minister of Justice: Iceland Not Exempt from Russian Espionage," *Iceland Review*, May 3, 2023, https://www.icelandreview.com/news/minister-of-justice-iceland-not-exempt-from-russian-espionage/.

[40] Darren Adam, "Minister of Justice Thinks Russia Is Spying in Iceland," *RUV*, May 3, 2023, https://www.ruv.is/english/2023-05-03-minister-of-justice-thinks-russia-is-spying-in-iceland.

[41] "Iceland's Comprehensive Approach to Security Is Complemented by a National Focus on Harnessing Natural Resources and Innovation," *NATO Parliamentary Assembly*, May 5, 2023,

Sweden

Since 2014, there has been ample evidence indicating Russian attempts to influence political decision-making in Sweden. A number of pro-Kremlin NGOs have become operational in the country, Russian politicians and diplomats have been reported to proactively intervene in Swedish domestic political affairs, and disinformation campaigns (including fabricated letters and prank phone calls) started to appear in the Swedish information landscape.[42] In 2015, Moscow established a Swedish language Sputnik news website, which – together with Russia Today – fed Russian narratives to vulnerable segments of society. Polarizing topics that Russia has sought to inflame include NATO expansion, (Muslim) immigration, LGBTQ issues, and the elite-general population divide. Pro-Kremlin outlets have also framed Swedish politicians and media as "Russophobe".[43] Compared to Finland, the social media communications of the Russian embassy have been judged as more aggressive.[44]

Following the outbreak of the war – and Sweden's application to join NATO in May 2022 – the country has experienced an increase in both false narratives and cyber interference. To name two examples, on the day of Sweden's general election in September 2022, the Swedish Election Authority was hit by three DDoS attacks,[45] followed by a DDoS attack on the Swedish Armed Forces website in December 2022.[46] As regards espionage, 2023 saw the most serious spy scandal in modern Swedish history, when two intelligence officials were jailed for passing secrets to Russia and the GRU (known as the "Kia brothers case").[47]

Although similar to Finland in some ways – namely that both countries have experienced an uptick in cyber attacks following their NATO bid – Sweden's experience differs in that Russia has sought to upset the accession process by instrumentalizing Islamophobia and suggesting that Sweden is waging war against Islam. More specifically, actors supported by Russia have been found to actively amplify incorrect statements suggesting that the government supported recent Quran burning in an effort to whip up disproportionate anger against Sweden, damage its image abroad, and further delay its NATO bid.[48] In contrast,

https://www.nato-pa.int/news/icelands-comprehensive-approach-security-complemented-national-focus-harnessing-natural.

[42] Anke Schmidt-Felzmann, "More than 'just' Disinformation. Russia's Information Operations in the Nordic Region," in *Information Warfare: New Security Challenge for Europe* (Centre for European and North Atlantic Affairs, 2017), 32–67.

[43] Ibid.

[44] Interview results.

[45] "Swedish Election Authority Hit by Three Cyber Attacks on Day of Vote," *TheLocal.Se*, September 11, 2022, https://www.thelocal.se/20220911/swedish-election-authority-hit-by-three-cyber-attacks-around-election.

[46] "Försvarsmaktens Webbplats Utsatt För Överbelastningsattack" ("Defense Forces website exposed to overload attack"), *Försvarsmakten*, December 2, 2022, https://www.forsvarsmakten.se/sv/aktuellt/2022/12/forsvarsmaktens-webbplats-utsatt-for-overbelastningsattack/.

[47] "Swedish Spy Scandal: Two Brothers Jailed for Passing Secrets to Russia," *The Local*, January 19, 2023, https://www.thelocal.se/20230119/swedish-spy-scandal-two-brothers-jailed-for-passing-secrets-to-russia.

[48] Elisabeth Braw, "How Sweden Became Public Enemy No. 1," *Foreign Policy*, July 28, 2023, https://foreignpolicy.com/2023/07/28/sweden-quran-nato-iran-iraq-russia/.Miranda Bryant, "Russia

disinformation campaigns that have been observed in Finland have been Russia-specific, mostly focusing on the alleged mistreatment of Russians living in Finland.

Finland

Like Norway, Finland has been a test case for Russian hybrid operations since as early as 2015, when the country faced a large influx of asylum seekers from Russia. While information influencing has been largely unsuccessful in Finland, Russian media and proxies have fuelled stories about the alleged maltreatment of Russians (especially children) in Finland, Finns harassing cars with Russian license plates, or false claims about military equipment movements in Finland during the 2022 Arrow exercise. NATO membership, migration and the management of the COVID-19 pandemic add to the list of polarizing topics Russia has sought to exploit. As for cyber interference, the central government, local government actors, and the business community have been targets of cyberattacks, although no attributions have been made publicly by the Finnish authorities. Additionally, the threat of corporate espionage and efforts to infiltrate organizations by various means is on the rise.[49] Critical infrastructure is perceived as most vulnerable to external interference, and foreign property acquisitions close to strategic sites have been more carefully scrutinized.

Following the outbreak of the war, and Finland's bid to join the Alliance, the country anticipated and prepared for aggressive interference during the NATO accession process. Contrary to all expectations, response from the Kremlin has been relatively subdued so far.[50] It is believed that because Russia could not prevent Finland from joining NATO, it might seek to influence what type of NATO member Finland will become and what direction the country's new foreign and security policies will take. In comparison to Sweden, which has been targeted in similar ways, Finland has been found to be less susceptible to hybrid interference – notably in the information domain – and more advanced when it comes to collaboration and intelligence sharing among various security actors.

For a more detailed assessment of the situation in Finland, please see a more extensive country case study on pages 21-26.

Spreading False Claims about Qur'an Burnings to Harm Nato Bid, Says Sweden," *The Guardian*, August 6, 2023, https://www.theguardian.com/world/2023/aug/06/russia-spreading-false-claims-about-quran-burnings-to-harm-nato-bid-says-sweden.

[49] "SUPO Yearbook 2022" (Finnish Security and Intelligence Service, 2023), https://vuosikirja.supo.fi/en/frontpage.

[50] Robbie Gramer, Amy Mackinnon, and Christina Lu, "NATO Countries Begin Ushering Finland and Sweden Into the Fold," *Foreign Policy*, May 16, 2022, https://foreignpolicy.com/2022/05/16/finland-sweden-nato-russia-war-security/.

Four key trends

Since Russia's full-scale invasion of Ukraine in 2022, the Arctic region has been subject to increased information influence operations, malign cyber activity, critical infrastructure interference, cyber espionage, as well as criminal activity as a new element of Russia's hybrid toolbox. While the role of China is also important when considering the big picture of hybrid interference in the Arctic, this report focuses solely on Russia's pattern of malign behavior and sub-threshold activity in the region.

1. Increase in Russian cyber activity

Cyber operations, most of which consist of DDoS attacks, have been on the rise since February 2022. Several ransomware attacks on electoral systems across the Arctic region have been reported – notably in Norway,[51] Alaska, and Finland[52] – as well as a considerable increase in hacking attempts into governmental systems.

In the Kingdom of Denmark, **Greenland** has suffered several serious cyberattacks in recent years. In March 2022, one cyber incident knocked the government network offline, which was followed by another attack on the health care system in May 2022 that severely limited health services.[53] **Iceland**'s websites were subject to a series of sustained DDoS attacks in April 2022, which are believed to have been linked to the planned increase in the country's defense budget. By March 2023, the director of the CERT-IS cybersecurity team Guðmundur Arnar Sigmundsson reported a sixfold increase in suspicious internet traffic scanning of Icelandic cyberspace.[54] Turning to **Norway**, in June 2022 a number of private and public institutions – including the police and the banking ID system – were subject to a DDoS attack.[55] Killnet, a pro-Russian hacker group, claimed responsibility.

Finland and **Sweden** have also been targeted – notably following their NATO membership bid in May 2022. Finland's Computer Emergency Response Team (CERT) reported that as of November 2022, it had received more notifications about DDoS attacks than ever before.[56]

[51] "Norway Says Russia behind Cyberattack against Its Parliament," *Al Jazeera*, October 13, 2020, https://www.aljazeera.com/news/2020/10/13/norway-says-russia-behind-cyber-attack-against-its-parliament.

[52] Naveen Goud, "Finland Election Results Service Hit by Cyber Attack," *Cybersecurity Insiders*, 2019, https://www.cybersecurity-insiders.com/finland-election-results-service-hit-by-cyber-attack/.

[53] Ellis Quinn, "Growing Focus on Arctic Puts Greenland at Higher Risk of Cyber Attacks: Assessment," *Eye on the Arctic*, March 14, 2023, https://www.rcinet.ca/eye-on-the-arctic/2023/03/14/growing-focus-on-arctic-puts-greenland-at-higher-risk-of-cyber-attacks-assessment/.

[54] Johanna Hjaltadottir, "Suspicious Internet Traffic Increased Sixfold after the Russian Invasion of Ukraine," *RUV*, March 9, 2023, https://www.ruv.is/frettir/innlent/2023-03-08-grunsamleg-netumferd-sexfaldadist-eftir-innras-russa-i-ukrainu.

[55] Thomas Nilsen, "Pro-Russian Hacker Group Says It Attacked Norway," *The Barents Observer*, June 29, 2022, https://thebarentsobserver.com/en/security/2022/06/pro-russian-hacker-group-says-it-attacked-norway.

[56] Alexander Martin, "Finland CERT Reports Record Number of Denial-of-Service Attacks," *The Record*, November 10, 2022, https://therecord.media/finland-cert-reports-record-number-of-denial-of-service-attacks.

The North American Arctic (notably **Alaska)** has also suffered cyberattacks, but very few have been publicized. In May 2021 – amid the COVID-19 pandemic – state-sponsored hackers gained unauthorized access to Alaska's health department. The same month, Alaska's court system was taken down and the country's courts had to operate manually, without Internet, for the month that followed.[57] This follows reporting that in 2020 Alaska's voting system was hacked and personal information (such as birth dates and driver's license numbers) was stolen.[58] More recently, in March 2022, the Permanent Fund division, which is responsible for paying the annual dividend to Alaskans, was attacked more than 800,000 times. The division shut down its computers and no data was stolen.[59] Further, Canada's National Research Council reported a "cyber incident" in March 2022.[60]

Although cyber operations have been on the rise since February 2022, they have been largely unsuccessful and no lasting impacts have been reported. It is possible that other cyber incidents have not been disclosed to the public. When key government websites were taken down, it appears that Western Arctic states were able to re-launch them without much difficulty and without much delay. What is more, no sensitive information was stolen. Overall, very few instances of cyber interference have been publicized, notably in the US and Canada. However, the increase in DDoS attacks on healthcare organizations has become a serious concern across the board. Besides gaining access, the goal of cyber interference may have been to demonstrate an intruder's cyber capabilities and to deter the target country from pursuing a certain policy action.

2. Increase in critical infrastructure interference

The damage to the Nord Stream gas pipelines in September 2022 was a wake-up call and a stark reminder of how structurally vulnerable communications cables, pipelines and other critical subsea infrastructure are to foreign interference. In April 2023, Swedish authorities concluded that it was a state actor that perpetrated the attack but stated that confirming identity would be difficult.[61] While there is no evidence that would prove Russian involvement in the explosions, Russian navy ships were seen operating in the proximity of the blast site,[62] and the country is well-known for maintaining highly advanced subsea capabilities.

[57] Nathaniel Herz, "Months Later, Details of Alaska Cyberattacks Remain a Closely Held Secret.," *Alaska Public Health*, September 30, 2021, https://alaskapublic.org/2021/09/30/months-later-details-of-alaska-cyberattacks-remain-a-closely-held-secret/.

[58] Nathaniel Herz, "Alaska Officials Say Hackers Stole Voter Info, Didn't Compromise Election Integrity," *Alaska Public Media*, December 3, 2020, https://alaskapublic.org/2020/12/03/alaska-officials-say-hackers-stole-voter-info-didnt-compromise-election-integrity/.

[59] James Brooks, "As Cyberattacks Continue, Alaska Lawmakers Consider Millions for Defense," *Anchorage Daily News*, April 17, 2022, https://www.adn.com/politics/alaska-legislature/2022/04/17/as-cyberattacks-continue-alaska-lawmakers-consider-millions-for-defense/.

[60] Steven Chase, "Canada's National Research Council Hit by a 'Cyber Incident,'" *The Globe and Mail*, March 21, 2022, https://www.theglobeandmail.com/canada/article-canadas-national-research-council-hit-by-cyber-incident/.

[61] Johan Ahlander, "State Actor Involvement in Nord Stream Pipeline Attacks Is 'Main Scenario' Says Swedish Investigator," *Reuters*, April 6, 2023, https://www.reuters.com/world/europe/swedish-prosecutor-says-still-unclear-who-behind-nord-stream-sabotage-2023-04-06/.

[62] Gordon Corera, "Nord Stream - Report Puts Russian Navy Ships near Pipeline Blast Site," *BBC News*, May 3, 2023, https://www.bbc.com/news/world-europe-65461401.

The mapping and targeting of undersea cables has been increasingly observed in the Arctic region, too. In early 2022, a communications fiber optic cable connecting the Norwegian mainland with a satellite ground station on the Svalbard archipelago was cut.[63] According to Norwegian authorities, the damage was likely caused by human activity rather than natural phenomena.[64] A few months earlier, in November 2021, the LoVe sea observatory in northern Norway went out of service due to extensive cable-related damage.[65] In addition to monitoring emissions and fish stocks, the observatory was also used to detect passing submarines – including those of the Russian Northern Fleet – which could have been the reason why it was targeted.[66] While attribution has been difficult, the fact that these events occurred within a relatively short time span raises alarms. Damage to subsea communication cables was also reported near the Faroe and Shetland Islands in October 2022, leaving many in the islands without internet access.[67]

The threat of spying on critical infrastructure has similarly increased. In April 2023, following a joint investigation of the public broadcasting companies in Denmark, Finland, Norway, and Sweden, Russia was accused of spying in the waters off the Baltic and North Seas using civilian fishing trawlers, cargo ships and yachts.[68] This alleged mapping of seabed infrastructure was interpreted as an effort by Moscow to plan and prepare possible acts of sabotage that could affect electricity flow to nearby countries.[69] Given that Norway became Europe's largest gas supplier, already in February 2023 the Norwegian Police Security Service (PST) suspected that Russia would seek to collect more intelligence on Norway's energy infrastructure to put pressure on European energy security.[70]

Interference with radio and radar navigation has been on the rise, too, particularly in Norway and Finland. In March 2022, soon after Russia invaded Ukraine, Finland experienced extensive disruption in GPS services, causing flight cancellations and

[63] Malte Humpert, "Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident," *High North News*, September 29, 2022, https://www.highnorthnews.com/en/nord-stream-pipeline-sabotage-mirrors-svalbard-cable-incident.

[64] Ibid.

[65] Stine Hommedal, "Ocean Observatory Temporarily out of Service," *Institute of Marine Research*, November 5, 2021, https://www.hi.no/en/hi/news/2021/november/ocean-observatory-temporarily-out-of-service.

[66] Thomas Newdick, "Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut," *The Warzone*, November 11, 2021, https://www.thedrive.com/the-war-zone/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut."

[67] Malte Humpert, "Fiber-Optic Submarine Cable near Faroe and Shetland Islands Damaged; Mediterranean Cables Also Cut," *High North News*, October 24, 2022, https://www.highnorthnews.com/en/fiber-optic-submarine-cable-near-faroe-and-shetland-islands-damaged-mediterranean-cables-also-cut.

[68] Jari Tanner, "Nordic News Outlets: Russian Yachts, Cargo Ships Spy at Sea," *AP News*, April 19, 2023, https://apnews.com/article/russia-baltic-sea-ships-spying-investigation-07346b954b6de12f03aebd7c9b9ad95e.

[69] Ibid.

[70] Gwladys Fouche, "Russia Likely to Spy More on Norway's Energy Industry, Say Norway Security Police," *Reuters*, February 13, 2023, https://www.reuters.com/world/europe/russia-likely-spy-more-norways-energy-industry-say-norway-security-police-2023-02-13/.

difficulties landing – especially at Savonlinna airport in eastern Finland.[71] Even though the government launched an investigation into both GPS interference and airspace violations of the spring and summer of 2022, the probe was later suspended for lack of available evidence.[72] In Norway, Russian GPS jamming reached “unprecedented levels” following the outbreak of the war: In 2022, the National Communications Authority (Nkom) reported a fivefold increase in the number of days with GPS failures over the airspace of Finnmark.[73] Norwegian authorities were clear in attributing blame to Russia, and tried diplomatic channels to get Moscow to stop. Russia has denied all such allegations.

3. Increase in (cyber) espionage and intelligence operations

Intelligence activities performed by foreign states – notably Russia and China, which have extensive powers to collect information abroad – constitute a significant threat to the seven Western Arctic states. According to a 2023 assessment by the Danish Security and Intelligence Service (PET), “Russia’s invasion of Ukraine and its continued isolation from the international community have increased the need of Russian intelligence services for collecting information that may improve the decision-making basis of the Russian regime.”[74] Areas of particular interest to Russian intelligence include Arctic states’ foreign, security, defense and energy policies, policies concerning the Arctic region, critical infrastructure, military capabilities and plans, military support to Ukraine, positioning/deliberations on sanctions imposed on Russia, and negotiations in relevant international fora of which they are members.[75]

In October 2022, a court in Norway charged Mikhail Mikushin, a Brazilian academic who worked at the University of Tromsø, with espionage for Moscow. Bellingcat, an investigative journalism group, stated that the accused man was linked to Russian military intelligence, the GRU, which Mikushin denied.[76] In addition, several Russian citizens were arrested in Norway for illegally flying drones and taking photographs near sensitive locations.[77] Energy-related intelligence is considered to be a high priority for Russia.

A broad range of actors and targets are subject to the threat of espionage in the Arctic. They include public authorities and decision makers (including politicians and centrally placed public officials), staff from security authorities, companies, research institutions, critical infrastructure, researchers and students, refugees, as well as dissidents.[78] Whether or not Russian intelligence efforts in the Arctic are more

[71] “NBI Suspends Investigation into Aircraft GPS-Jamming,” *YLE News*, February 3, 2013, https://yle.fi/a/74-20016277.
[72] Ibid.
[73] “Strong Increase in GPS Jamming over Finnmark,” *The Resilient Navigation and Timing Foundation*, February 26, 2023, https://rntfnd.org/2023/02/26/strong-increase-in-gps-jamming-over-finnmark-nrk/.
[74] “Assessment of the Espionage Threat to Denmark, the Faroe Islands, and Greenland,” 12.
[75] Ibid.
[76] “Norway Charges Man Accused of Being a Russian Spy,” *BBC News*, October 28, 2022, https://www.bbc.com/news/world-europe-63429520.
[77] Ibid.
[78] Assessment of the Espionage Threat to Denmark, the Faroe Islands, and Greenland.

intense than the general rise in Russian intelligence operations globally presents an interesting avenue for further research.

Western Arctic countries have responded to this threat by expelling a large number of Russian intelligence officers. As early as February 2022, the US expelled 12 Russian diplomats working at the United Nations for allegedly engaging in "espionage activities."[79] Denmark followed suit, sending 15 Russian intelligence officers working under diplomatic cover at Russia's representations in Denmark in April 2022 back to Moscow.[80] In April 2023, Norway barred 15 Russian intelligence officers from the Russian embassy for "engaging in activities not compatible with their diplomatic status," which followed an earlier removal of three intelligence officers a year prior.[81] The same month, Sweden announced it would expel five employees of the Russian embassy in Stockholm. This decision came amid other espionage charges in Sweden, namely the sentencing of two Iranian-born Swedes (the Kia brothers) for passing information to Russian intelligence between 2011 and 2021.[82] Finally, in June 2023, Finland announced plans to send nine intelligence officers operating under diplomatic cover at the Russian Embassy in Helsinki back to Moscow.[83] In contrast, Canada has so far declined to expel Russian diplomats, despite evidence of diplomatic misconduct. As to Iceland, the country decided to close its Embassy in Moscow as of August 2023, and requested Russia to reciprocate and scale back the operations of its Embassy in Reykjavík.[84] While this decision is not related to espionage concerns, it will nevertheless have implications for Russia's ability to collect relevant information in Iceland.[85]

Given that human intelligence (HUMINT) under diplomatic cover was Russia's main intelligence collection method, Moscow's ability to spy will be markedly reduced following the expulsions. It is expected that Russia will try to "compensate" for lost physical presence and use other methods for spying, including cyber espionage and electronic collection.[86] Neither cyber espionage, nor the monitoring of electronic communications (such as mobile phone conversations, text messages, e-mails, and radio communications) require a physical presence in the countries concerned. To illustrate, an assessment produced in Denmark in February 2023, titled "The Cyber Threat to Greenland", observed a large increase in cyber espionage and crime over the last few years in Greenland, and flagged the threat of cyber crime such as ransomware as particularly high. The Finnish Security and Intelligence Service

[79] Richard Roth, "US Is Expelling 12 Russian UN Diplomats," *CNN*, February 28, 2022, https://edition.cnn.com/2022/02/28/politics/us-expels-russian-un-diplomats/index.html#:~:text=The%20United%20States%20has%20asked,continues%20its%20attack%20on%20Ukraine.

[80] "Assessment of the Espionage Threat to Denmark, the Faroe Islands, and Greenland."

[81] Alte Staalesen, "Norway Expels 15 Intelligence Officers at Russian Embassy," *The Barents Observer*, April 13, 2023, https://thebarentsobserver.com/en/2023/04/norway-expels-15-intelligence-officers-russian-embassy.

[82] "Swedish Spy Scandal: Two Brothers Jailed for Passing Secrets to Russia."

[83] "Haavisto on Diplomats' Expulsion: Finland Is Braced for Russian Countermeasures," *YLE News*, June 7, 2023, https://yle.fi/a/74-20035694.

[84] "Iceland Suspends Embassy Operations in Moscow" (Government of Iceland, June 9, 2023), https://www.government.is/news/article/2023/06/09/Iceland-suspends-embassy-operations-in-Moscow/.

[85] Ibid.

[86] "Assessment of the Espionage Threat to Denmark, the Faroe Islands, and Greenland."

(SUPO) also reported that Russian cyber espionage targeting Finland exceeded previous levels by the second half of 2022.[87] Looking ahead, recruitment of civilians, journalists and business people to spy for Russia, as well as deployment of intelligence officers undercover in locations other than the embassies, are likely.[88]

Foreign property acquisitions close to strategic sites are more carefully scrutinized, too. Finland, for instance, experienced an uptick in land and real estate acquisitions by Russians in 2022.[89]

4. Increase in information influence operations (including disinformation)

Once removed from the mainstream, the Arctic region has attracted considerable media attention, coverage and international visibility in recent years. Understanding the potential of the Arctic spotlight, the Kremlin has used the Arctic as a strategic communications tool to shape and modify Russia's image abroad, turn its strategic competition with the US to its advantage, as well as to form public opinion at home.[90] As Dr. Marlène Laruelle of the George Washington University writes, since as early as 2008-2009, Moscow has been focused on crafting a highly cooperative "Arctic brand" and an official narrative that celebrates the Arctic region as a zone of peace and international cooperation – of which Russia is the co-leader.[91]

Whitney Lackenbauer, Adam Lajeunesse, and Troy Bouffard provide an extensive analysis of the Russian disinformation and propaganda ecosystem in the Arctic. In a comprehensive study, published in October 2022, they outline various themes that have been prevalent in Russian narratives from 2016 to 2020. First and foremost, messaging by Russia and its proxies tends to frame the US and NATO as destabilizing forces in the Arctic, and the smaller Arctic states as pawns of the US. Another common theme in the Russian media is that Russia's Arctic military build-up is defensive in nature and that Russia does not pose a threat to its Arctic neighbors.[92] Russian media have also sought to devalue the effect of Western sanctions, suggesting that they are more damaging to Arctic states' economic interests than they are to Russia. Overall, Western Arctic states are generally framed as weak, whether through a lack of icebreakers or bases. Even Western military exercises such as Trident Juncture and Cold Response are reported through a paradigm of weakness.

Since the outbreak of the war in Ukraine, Russian disinformation efforts have significantly increased. However, they have followed the patterns found by

[87] "More Russian Cyberattacks Targeting Finland," *YLE News*, June 9, 2023, https://yle.fi/a/74-20028302.
[88] Ibid.
[89] "Finland Sees Uptick in Real Estate Purchases by Russians," *YLE News*, February 9, 2023, https://yle.fi/a/74-20017150.
[90] Marlène Laruelle, *Russia's Arctic Strategies and the Future of the Far North* (Armonk, New York: M.E. Sharpe, Inc, 2014), 12–13.
[91] Ibid.
[92] See, for example, Katarzyna Zysk, "Myths and Misconceptions around Russian Military Intent: Myth 8: Russia's Military Build-Up in the Arctic Is Defensive" (Chatham House, July 14, 2022), https://www.chathamhouse.org/2022/07/myths-and-misconceptions-around-russian-military-intent/myth-8-russias-military-build.

Lackenbauer, Lajeunesse, and Bouffard. Polarizing topics that Russia has sought to inflame include the role of NATO in the Arctic and the US's behavior. Russian disinformation efforts have also continued to downplay Russia's military build-up in the region and have reinforced the message that Russia does not want the conflict in Ukraine to spill over into the Arctic.

Our research suggests that there is variation in how the seven Western Arctic states are targeted via disinformation, with Russia producing a uniquely tailored content to influence audiences of each Western Arctic state. For example, while populations of both Finland and Sweden have long been exposed to anti-NATO and anti-US information campaigns, there are contextual differences in how Russia targets each country. Anti-NATO narratives saw a significant increase in the wake of February 2022 when both countries applied for NATO membership. However, as one example, Swedish journalist Chang Frick, closely affiliated with Russia Today, paid for Danish far-right activist Rasmus Paludan to publicly burn the Quran near the Turkish embassy in Sweden – an event that directly led to Turkish President Erdogan saying Sweden should not expect Turkish support for NATO membership.[93] Sweden being portrayed as an anti-Muslim and anti-immigrant country is yet another example of a country-specific targeted campaign. By contrast, Canada, which has the world's second-largest Ukrainian diaspora, has had to grapple with narratives aimed at stoking anti-Ukrainian sentiments. Another example is Russian claims that Finnish social workers were taking Russian-born children into custody and selling them to gay couples in the US.[94]

[93] Anna Mikhailova, "Russia-Affiliated Journalist Paid for Quran Burning in Sweden," *I24 News*, January 24, 2023, https://www.i24news.tv/en/news/international/europe/1674639619-russia-affiliated-journalist-paid-for-quran-burning-in-sweden.

[94] "Jussi Toivanen: Learning from Finland's Society-Wide Approach to Countering Disinformation," *CDA Institute*, December 4, 2020, https://cdainstitute.ca/jussi-toivanen-learning-from-finlands-society-wide-approach-to-countering-disinformation/.

Case study: Finland

Threat and vulnerability landscape

Instrumentalization of migration

As early as 2015 and 2016, Finland became a test case for Russian hybrid operations, when Russia allowed an increasing number of asylum seekers to cross into Finland (and Norway) with a destabilizing effect on Finnish society.[95] In the words of Charly Salonius-Pasternak of the Finnish Institute of International Affairs (FIIA), this orchestrated flow of asylum seekers constituted "a proof of concept aimed at Finland and the European Union", demonstrating that Russia can "transfer people [and] fully control the flow of migrants across its border."[96] The 2021 refugee crisis at the Belarusian-Polish border demonstrated that weaponization of migration is still part of Kremlin's influencing toolbox. According to one of our interviewees, "now that our relations with Russia are adversarial, we cannot exclude that [Russia] would not do it again." Based on its experience in 2015, Finland has developed its preparedness for and capability to respond to a mass influx of migrants.[97] This includes the border barrier fence, which is currently under construction along Finland's border with Russia, as well as improved surveillance.

Information influence activities and polarizing topics

Historically concerned about NATO's eastward expansion, Russia had attempted to divide public opinion on NATO membership long before Finland formally applied to join the Alliance in response to Russia's invasion of Ukraine.[98] Other notable examples of information influencing include disinformation campaigns about the alleged maltreatment of Russians (especially children) in Finland, Finns harassing cars with Russian license plates, exaggerations of Finnish energy dependence on Russia, or false claims about military equipment movements in Finland during the 2022 Arrow exercise.[99] Migration and the management of COVID-19 pandemic add to the list of polarizing topics Russia has sought to exploit. Since 2014, Finland has made significant advances in dealing with Russian operations in the information domain. As a result, the level of Russia's information activities, political or election interference is considered "low" and ineffective.

[95] Interview with Dr. Matti Pesu, Finnish Institute for International Affairs (FIIA), April 28, 2023, Helsinki, Finland.
[96] "Flow of Migrants into Finland from Russia Dries up: Helsinki," *Reuters*, March 17, 2016, https://www.reuters.com/article/us-europe-migrants-finland-russia-idUSKCN0WJ1NP.
[97]"Government Report on Changes in the Security Environment" (Finnish Government, 2022), https://julkaisut.valtioneuvosto.fi/handle/10024/164002.
[98] See, for example, Sijbren de Jong et al., "Inside the Kremlin House of Mirrors" (The Hague Centre for Strategic Studies, 2017), https://hcss.nl/wp-content/uploads/2021/01/Inside-the-Kremlin-House-of-Mirrors-How-Liberal-Democracies-can-Counter-Russian-Disinformation-and-Societal-Interference.pdf.
[99] Matthew Holroyd, "Ukraine War: False Claims Spread about Military Movements in Poland and Finland," *Euronews*, May 6, 2022, https://www.euronews.com/my-europe/2022/05/06/ukraine-war-false-claims-spread-about-military-movements-in-poland-and-finland.

Weaponization of energy

In May 2022, Russia stopped electricity and gas exports to Finland.[100] The move was preceded by an earlier Finnish decision to halt Russian crude oil imports, which was later substituted by increased imports from Norway, the US, and the UK.[101] These steps put an end to Finland's energy ties with Russia.[102] Breaking energy ties with Russia was easier for Finland than it was for other European countries (especially those in Central and Eastern Europe) as natural gas constitutes only 5% of Finland's energy mix and most of the country's electricity is produced from alternative sources of energy (namely nuclear, biomass, hydro and wind power). Large-scale energy collaboration with Russia also included nuclear power. Imports of uranium fuel from Russia, which presently remain untouched by EU sanctions, could be an issue down the line. As regards the overall vulnerability of the Finnish energy sector, the Finnish Security Intelligence Service (SUPO) considers it unlikely that another state would seek to incapacitate the Finnish energy sector. Limited and temporary disruptions in electricity distribution, however, *can* be achieved and may be a future threat that Finland ought to prepare for.[103]

Cyber interference

The central government, local government actors and the business community have all been targets of cyber attacks in Finland.[104] SUPO assessed that the volume of Russian cyber activity targeting Finland decreased before the war started, as Russia focused its resources on Ukraine. However, cyber activities started to grow again and returned to their normal levels by the summer of 2022. By the second half of 2022, Russian cyber espionage efforts targeting Finland had become even more active than before.[105] To mention two examples of cyber interference targeting Finland, Finnish government websites suffered hacking attempts while Ukrainian President Zelensky was delivering a video address to the Finnish parliament in April 2023,[106] and the most recent significant DDoS attack was reported on 4 April 2023, the day Finland acceded to NATO. Additionally, the threat of corporate espionage and efforts to infiltrate organizations by various means is on the rise.[107] Cyber interference is cheap, easy, and difficult to attribute, enabling Russia both to gain access and to demonstrate its cyber capabilities. While there has been no lasting damage from the attacks, Russian cyber interference is occasionally effective in the way it signposts Russian capabilities and causes disruption in the everyday lives of Finns. The aim is presumably to deter Finland from pursuing certain foreign policy and security actions. Interviews conducted for the purpose of this study suggest that

[100] "Russia Has Cut off Its Natural Gas Exports to Finland in a Symbolic Move," *NPR*, May 21, 2022, https://www.npr.org/2022/05/21/1100547908/russia-ends-natural-gas-exports-to-finland.

[101] "Finland Replaces Russian Urals with Oil from Norway, UK and US," *Reuters*, May 15, 2023, https://www.reuters.com/business/energy/finland-replaces-russian-urals-with-oil-norway-uk-us-2023-03-15/.

[102] "Russia Has Cut off Its Natural Gas Exports to Finland in a Symbolic Move."

[103] "SUPO Yearbook 2022."

[104] "Government Report on Changes in the Security Environment."

[105] "SUPO Yearbook 2022."

[106] "Finland Says Government Websites Hacked as Ukraine President Spoke," *Reuters*, April 8, 2022, https://www.reuters.com/world/europe/finnish-government-websites-hit-by-cyberattack-2022-04-08/.

[107] "SUPO Yearbook 2022."

cyberattacks targeting Finland have not been disruptive – probably as a result of Finnish enhanced investment in cyber defense.

Critical infrastructure interference

Critical infrastructure is perceived by our interviewees as vulnerable to external interference. The 2022 Nord Stream sabotage attack raised fears of possible Russian interference in Finland's energy infrastructure. On the one hand, technological developments and digitalization equip malign actors with additional means of inflicting harm and exerting influence. Simultaneously, Russia could seek to interfere through the purchase of property close to strategic sites. Since 2016, the Finnish Defence Ministry has been paying closer attention to land and real estate acquisitions by foreign entities near military facilities and critical infrastructure, fearing they could be taken advantage of in a crisis situation – to accommodate troops, or to close transport routes, for example.[108] In 2020, the Defence Ministry was given powers to grant property sales to Russian entities and reject them on national security grounds, as happened in 2022, when three Russian citizens sought to purchase a former elderly care home near the Finnish army garrison out of which the joint Finnish and NATO exercise Arrow 22 was run.[109] The government is also paying closer attention to the amount of information it shares online concerning 3D GIS data of buildings and energy sites.[110]

Targets and audiences

According to Statistics Finland, there are around 93,000 Russian-speakers permanently living in Finland (less than 5% of the overall population), 33,000 of which have Russian nationality.[111] Russian speakers are dispersed across the country, are considered to be well integrated into Finnish society, and have access to Russian-language news produced in Finland.[112] According to a 2022 survey, over a third of Russian speakers take a critical stance towards the Russian invasion of Ukraine.[113] Thus the minority is small and the divides within this minority are not strong enough, which makes it difficult for Russia to drive wedges, or to use the "compatriots abroad" policy as a tool of influence.

While Russian-speakers residing in Finland might not be vulnerable to outside influence, our interviewees suggested that Russian narratives can hold sway over other immigrant populations – those from the Middle East or Africa, for instance – which tend to be less integrated, have less confidence in Finnish media and institutions, and continue to follow the news in their native languages. For example,

[108] Gabriel Samuels, "Finnish Government 'Suspects Russia of Buying Property to House Soldiers' in Case of Future Invasion, Tabloid Claims," *The Independent*, November 2, 2016, https://www.independent.co.uk/news/world/europe/finnish-government-suspects-russia-of-buying-property-to-house-troops-a7392841.html.

[109] Charlie Duxbury, "Russians Hunting Property in Finland Hit a New Wall of Suspicion," *POLITICO*, February 23, 2023, https://www.politico.eu/article/russia-finland-property-buy-homes-ukraine/.

[110] Interview with Brigadier General Sami Nurmi, Ministry of Defence of Finland, April 28, 2023.

[111] "Population and Society" (Finland in Figures, 2022), https://www.stat.fi/tup/suoluk/suoluk_vaesto_en.html.

[112] "Spike in Interest in Yle's Russian-Language News; HS Offers Articles in Russian," *YLE News*, March 10, 2022, https://yle.fi/a/3-12352547.

[113] "Survey: One Third of Finland's Russian Speakers Think Russia Violated Ukrainian Sovereignty."

Finnish public broadcasting company (Yle) found in 2022 that pro-Russian trolls had created discourse around an imminent Russian invasion on Arabic TikTok and shared videos claiming that war would break out in Finland or that the US was forcing Finland to join NATO.[114] Other segments of society that are likely to be targeted include extremist groups, political elites and right-wing populists, and local populations that feel removed from the capital and decision-making. Here, establishment of NATO presence could be portrayed as harmful to their environment and livelihoods.[115] Companies that are responsible for critical infrastructure, as well as digital government services and platforms, also constitute an attractive target audience.

In the past, Russia sought to maintain close contacts with influential individuals and decision makers in Finland. Gift offerings were not uncommon either.[116] As people-to-people contacts diminished and Russian intelligence activities in Finland "significantly weakened" over the past two years[117] – following the expulsion of intelligence officers working at the Russian Embassy – traditional human intelligence operations have become more difficult for Russia. This may explain why Russia has become more active in cyberspace.

Level of preparedness and resilience

Our interviewees unanimously agreed that Finnish society is *inherently resilient* to Russian hybrid influencing. This high level of resilience is underpinned by the long and complex history of Russo-Finnish relations – which have resulted in a "healthy dose of realism and caution"[118] – high education standards which have nurtured a critical and active civil society, active and impartial media, strong democratic traditions, social cohesion and trust in the government. As noted in one of our interviews, Russia knew that an aggressive campaign aimed at dissuading Finland from joining NATO would be futile and that efforts to misinform or otherwise sway public opinion were not going to succeed. Although the success of disinformation campaigns is not guaranteed, Russia has nevertheless persisted with other forms of hybrid activity. Finnish stakeholders interviewed for the purpose of this study acknowledged that no one is immune from the threat and that it is important to remain prepared and vigilant. Enhancing social cohesion, and increasing the resilience of more vulnerable and susceptible target audiences – including marginalized groups, which may feel that policies have left them behind – is key.

Finnish approach

Comprehensive security lies at the heart of the Finnish approach to countering hybrid threats.[119] Last updated in 2017, the concept denotes a whole-of-society approach to

[114] "Disinformation Campaigns Target Finland's Foreign Language Speakers, NATO Fears," *YLE News*, accessed August 8, 2023, https://yle.fi/a/3-12525251.
[115] Interview results.
[116] Interview results.
[117] Interview results.
[118] Interview with Amb. Petteri Vuorimäki, Finnish Ministry of Foreign Affairs, April 27, 2023, Helsinki, Finland.
[119] "Comprehensive Security" (The Security Committee, n.d.), https://turvallisuuskomitea.fi/en/comprehensive-security/.

addressing a broad array of threats to national security. It is rooted in an understanding that conventional/military might alone is insufficient to ensure national survival, and an emphasis on the importance of information sharing and collaboration between the authorities, the business community and organizations – even citizens.[120]

Senior representatives from all sectors, including NGOs, businesses and parliament, are invited to attend prestigious National Defence Courses, in which participants discuss comprehensive security and practice responding to different types of crises.[121] Four national and 1-3 specialized courses are offered annually, with the aim of facilitating networking and improving cross-sector cooperation in national defense. Response to hybrid threats forms part of the curriculum.[122]

On Finland's initiative, a European Center for Countering Hybrid Threats was established in Helsinki in 2017. Supported by 33 states from across the EU and NATO, the Center provides expertise and training for countering hybrid threats and serves as a platform for the sharing of best practices among its Participating States.[123] In addition, Finland is a contributing nation to the NATO Cyber Defense CoE, the NATO StratCom CoE and the NATO Energy Security CoE, all of which help enhance Helsinki's capabilities in the cyber, information and energy domains.

Finland has also taken important legal steps. As mentioned above, the government has tightened property ownership policy and it has also amended national legislation governing border security, with the aim to better respond to possible instrumentalization of migration.[124]

Looking ahead: Thoughts on Russian objectives

According to our interviewees, Russia seems to be assessing how to define its relations with Finland post-NATO accession, and what type of narrative to craft for its domestic audience. It is expected that the Kremlin's reaction will remain restricted, muted and rhetorical only. As noted in one of the interviews, Russia does not perceive Finland as negatively as it perceives its other NATO neighbors. "Moderate NATO member states are not the hardliners," one of the respondents added.[125] Given the history of Finland's pragmatic relationship and experience of dealing with Russia, the biggest threat for Russia is that Finland aligns its rhetoric or policies with those of the Baltic states and Poland.

Unpredictability will likely remain Russia's operating model moving forward, which represents a possibly dangerous situation. Because Russian conventional power has

[120] Vesa Valtonen and Minna Branders, "Tracing the Finnish Comprehensive Security Model," in *Nordic Societal Security: Convergence and Divergence*, ed. Sebastian Larsson and Mark Rhinard, Routledge New Security Studies (London; New York: Routledge/Taylor & Francis Group, 2021).
[121] Elisabeth Braw, "We Can All Learn from the Finnish Approach to Defense," *The Financial Times*, February 9, 2023, https://www.ft.com/content/7c8cebc4-8107-45d8-8f58-2382277fdd0c.
[122] Interview with Brigadier General Sami Nurmi, Ministry of Defence of Finland, April 28, 2023.
[123] "What Is Hybrid CoE?" (The European Centre of Excellence for Countering Hybrid Threats, n.d.), https://www.hybridcoe.fi/who-what-and-how/.
[124] "Government Report on Changes in the Security Environment."
[125] Interview results.

declined, the country is more likely to resort to other means, such as hybrid activities or even nuclear deterrence. Simply put, Russia will need to get more creative with the means and tools it has at its disposal. It is expected that Finland will see an increased number of strategic bomber patrol flights near its border, Russia regrouping forces and placing more hardware along its border with Finland, more surveillance and more symbolic actions. The possibility of sabotage in the maritime domain cannot be excluded. Given its determination and will to act, the overall assessment is that at some point, Russia will be able to regain its military capability.

As regards Russian objectives – beyond efforts to destabilize Finnish society – it is believed that because Russia could not prevent Finland from joining the Alliance, it might seek to exert control over the formation and substance of Finnish NATO policy, as well as over Finland's new foreign policy and security approach. Given that Finland raised its military budget by 25% in 2023, exceeding 2.2% of GDP, Russia is likely to try to influence defense spending-related decisions in Finland.[126]

[126] Interview with Brigadier General Sami Nurmi, Ministry of Defence of Finland, April 28, 2023.

Regional Approach: Assessing the viability of a joint response mechanism towards hybrid threats

Addressing hybrid threats effectively requires – first and foremost – a common understanding of what precisely constitutes "hybrid" interference and how such threats manifest themselves.[127] So far as we know, there is no common definition of hybrid threats in the Arctic. Additionally, there is no shared understanding of who the aggressor is. As a study produced by the Hybrid CoE in 2021 confirms, "there is no consensus on the nature and extent of hybrid threats to the Arctic, nor on their use by adversaries. [...] The absence of consensus on these challenges can result in real policy differences between Allies, and Arctic states. This gap is exploitable and inhibits responses, particularly in the hybrid threat space."[128] While opinions on the threat that Russia poses have shifted since the outbreak of the war, Canada and the US continue to consider China as the number one threat to their Arctic interests.

Additionally, each Arctic country prioritizes responding to hybrid threats differently, considering its national specificities and societal vulnerabilities. Consider the Nordic countries, for example. The approach to hybrid threats appears fairly homogeneous across Finland, Sweden and Norway, in the sense that all three countries have adopted a "Total Defense" approach to security, which consists of *military* defense and *civil* defense. This concept relies on societies' overall emergency readiness, and combines the armed forces and civil society in a comprehensive whole-of-society approach.[129] But while the organizations that are responsible for total defense are in discussion with each other, they do not pursue a uniform approach.

The inability to replicate the Finnish comprehensive security model in the remaining Arctic countries stems first and foremost from national legislative and regulatory limitations. For example, in countries like Sweden, the law forbids police and defense forces from collaborating with the secret service. As such, the collaboration of – and intelligence sharing between – the security actors that is commonplace in Finland would not be possible to replicate across the board.[130] Similarly, in Norway, there are important restrictions on the scope of actions that can be undertaken by certain security actors, including the armed forces. More specifically, the Constitution prevents the military from acting domestically other than in warfare (and a few other exceptional cases).[131] Population size matters, too. The Finnish comprehensive

[127] See, for example, European Commission and Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model: Public Version.* (LU: Publications Office, 2021), https://data.europa.eu/doi/10.2760/44985.

[128] "Security and Hybrid Threats in the Arctic: Challenges and the Vulnerabilities of Securing the Transatlantic Arctic" (The European Centre of Excellence for Countering Hybrid Threats, December 2021).

[129] See, for example, James Kenneth Wither, "Back to the Future? Nordic Total Defence Concepts," *Defence Studies* 20, no. 1 (January 2, 2020): 61–81, https://doi.org/10.1080/14702436.2020.1718498.

[130] See, for example, Mikael Lohse, "Sharing National Security Information in Finland," *Information & Communications Technology Law* 29, no. 3 (September 1, 2020): 279–90, https://doi.org/10.1080/13600834.2020.1759277.

[131] Dick Zandee and Adaja Stoetman, "Countering Hybrid Threats: The Role of the Joint Expeditionary Force" (Clingendael, March 2023).

security model – which works well in a country of 5.5 million inhabitants – would be harder to accomplish in a populous country like the US.[132]

As regards conceptual variations, Finland offers an interesting case in point. Instead of hybrid influencing – which the government considers "too narrow" a definition[133] – Finland focuses on preventing and countering the threats of "broad-spectrum influencing".[134] This definition expands the notion of hybrid influencing to include military means as well as the threat of using them.

In addition, each Arctic country examined in this study has its own **structures** for dealing with hybrid threats, which complicates regional cooperation further when it comes to formulating common responses to hybrid threats.

The North Atlantic Treaty Organization (NATO)

NATO provides its members with tools to counter hybrid campaigns. When Sweden joins the Alliance – following Finland's lead – the seven Western Arctic states will all be members of NATO. Since as early as 2015, NATO has had a strategy for countering hybrid warfare. While it can be difficult to reach consensus and officially invoke Article 5 in the face of hybrid aggression,[135] a stricken Ally can always invoke Article 4 consultations to discuss its security concerns and available options when facing a hybrid campaign. Furthermore, Article 3 commits Allies to enhancing their resilience. In fact, all seven Western Arctic states already participate in NATO meetings and symposia on resilience.[136]

In addition to serving as a platform for consultation, NATO has consistently broadened its toolbox to help its members prepare for and respond to hybrid threats.[137] In 2016, NATO identified seven "baseline requirements" for resilience, against which all Allies can assess their level of preparedness. They include 1) government continuity, 2) resilient energy supplies, 3) effective handling of uncontrolled population movements, 4) resilient food and water resources, 5) ability to deal with mass casualties, 6) functioning of civil communications systems, and 7) resilient civil transportation systems.[138] These "baseline requirements" provide the added value of creating a more coherent system of resilience and preparedness for Western Arctic states (as well as other NATO members).

[132] Interview with Brigadier General Sami Nurmi, Ministry of Defence of Finland, April 28, 2023.
[133] Ibid.
[134] "Government's Defence Report" (Finnish Government, September 9, 2021), https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163407/VN_2021_80.pdf.
[135] Invoking Article 5 in response to hybrid threats is possible, as stated in the 2016 Warsaw Summit Communiqué and reiterated in the 2021 Brussels Summit Communiqué. See Michaela Prucková, "Cyber Attacks and Article 5 — a Note on a Blurry but Consistent Position of NATO," NATO CCDCOE, March 10, 2022, https://ccdcoe.org/incyder-articles/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/.
[136] See, for example, "NATO Resilience Symposium, 25-27 April 2023,"
[137] Michael Rühle and Clare Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats" (NATO Review, March 19, 2021), https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html.
[138] Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defence" (NATO Review, February 27, 2019), https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

In order to counter hostile information activities, NATO has over the past decade heavily invested in setting up its own approach to strategic communications, both processes and capabilities. The StratCom function enables full coordination between the NATO HQ and the military commands, and it helps coordinate efforts with and between Allies. To this end, NATO developed a StratCom handbook, the Narrative Development Tool, and a system to better assess the information environment.[139] In 2023, NATO also published the Allied Joint Doctrine for Strategic Communications, which established the doctrine fundamentals for a NATO-wide approach to strategic communications and a reference resource for commanders.[140] NATO further counters disinformation by setting the record straight – online, on air and in print – and through proactive communications.

NATO has similarly taken important steps in cyber defense. In 2016, Allies recognised cyberspace as a domain of military operations and in 2018, NATO stood up the Cyberspace Operations Centre (CyOC). A year later, in 2019, NATO produced a guide that sets out different response options and tools at member states' disposal to respond to malicious cyber activities. Through the Cyber Defence Pledge, Allies also continue to enhance the cyber defenses of national networks and infrastructure.[141] The Counter Hybrid Support Team (CHST), which NATO members agreed to set up in 2018, can be deployed on short notice to any Ally requesting NATO support, either to prepare against hybrid activities by building national counter-hybrid capacities, or in a crisis.[142]

Prompted by the sabotage of the Nord Stream pipelines, NATO created a Critical Undersea Infrastructure Coordination Cell in 2023. This brings key military and civilian stakeholders together with industry representatives to share best practices, leverage innovative technologies, and boost the security of Allied undersea infrastructure.[143] As an additional step to improve critical undersea and energy infrastructure security, NATO and the Allies increased their maritime presence and patrols in the North and Baltic Seas.[144] Finally, since Finland and Sweden secured their invitee status at NATO in the summer of 2022, all Western Arctic states have been comprehensively involved in the civilian intelligence sharing at NATO.[145] Sharing of intelligence about domestic developments is key to developing a shared picture and understanding of hybrid threats.

[139] Lieutenant Colonel Lothar Buyny, "Implementing Stratcom," *The Three Swords Magazine* 28 (2015): 39–63.

[140] "Allied Joint Doctrine for Strategic Communications" (Ministry of Defence, March 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146501/20230328-AJP_10_EdA_V1_Strategic_Communications-O.pdf.

[141] "Cyber Defence" (NATO, June 22, 2023), https://www.nato.int/cps/en/natohq/topics_78170.htm.

[142] Rühle and Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats."

[143] "NATO Stands up Undersea Infrastructure Coordination Cell," *NATO*, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

[144] "NATO Maritime Assets Play Key Role in Offshore Critical Infrastructure Security," *NATO*, February 14, 2023, https://mc.nato.int/media-centre/news/2023/nato-maritime-assets-play-key-role-in-offshore-critical-infrastructure-security."

[145] "SUPO Yearbook 2022."

The European Union (EU)

Denmark, Finland and Sweden are also part of the European Union (EU), which has developed a wide range of tools to help its members coordinate their responses to hybrid threats and campaigns – should they choose to invoke the assistance of the EU. These include the **Cyber Diplomacy Toolbox**, adopted in 2017 to counter cyberattacks and cyber criminality, and the **Foreign Manipulation and Interference (FIMI) Toolbox**. The EU also established the East StratCom Taskforce in 2015 to address Russia's ongoing disinformation campaigns.[146] The EU Strategic Compass, which recognizes the need to counter hybrid threats and deal with them comprehensively, launched the development of an **EU Hybrid Toolbox (EUHT)**, which was completed in December 2022. The Toolbox is intended to serve as an "umbrella" framework that brings together all relevant civilian and military instruments, and seeks to ensure that their application – and EU responses to hybrid campaigns – is coherent and coordinated.[147] At the EU level, over 200 measures and tools have so far been identified as suitable for countering hybrid threats.[148] The **EU Hybrid Fusion Cell,** for example, plays a central role in enhancing strategic foresight and situational awareness, particularly with regard to the origin and features of hybrid threats and campaigns. Finally, following the example of NATO's Counter Hybrid Support Team (CHST), the EU also set out to establish "stand-alone" **EU Hybrid Rapid Response Teams**. These teams would not only support EU members, but also assist Common Security and Defence Policy (CSDP) missions and operations, as well as third countries, in countering hybrid threats.[149] As such, they can be deployed Arctic-wide. Regarding the resilience of critical infrastructure, in 2022 the EU adopted the **Critical Entities Directive (CER)**, which introduced EU-wide obligations on entities providing essential services in terms of their physical protection. This Directive is binding for EU member states – including Denmark, Finland and Sweden. While there is currently no foreign direct investment (FDI) screening at an EU level, a coordinated approach is sought after and may be in the works.[150] A unified EU toolkit on sanctions with specific talking points to respond to Russian disinformation could also prove useful.[151] Overall, given the extent of the EU's competencies and powers, as well as the multitude of instruments it has at its disposal, some would argue that the Union is better suited to play an active role in the civil domain than NATO.[152] However, states that are members of both EU and NATO certainly can use both sets of tools.

[146] "Questions and Answers about the East StratCom Task Force" (European Union External Action, October 27, 2021), https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232.

[147] "Countering Hybrid Threats" (European Union, March 2022), https://www.eeas.europa.eu/sites/default/files/documents/2022-03-28-countering-Hybrid-Threats_NewLayout.pdf.

[148] See Kenneth Lasoen, "Realising the EU Hybrid Toolbox: Opportunities and Pitfalls" (Clingendael, December 2022).

[149] "The Strategic Compass of the European Union," 2022, https://www.strategic-compass-european-union.com/2_Secure_Strategic_Compass.html.

[150] Tobias Heinrich et al., "Foreign Direct Investment Reviews 2023: Europe," *White and Case*, March 20, 2023, https://www.whitecase.com/insight-our-thinking/foreign-direct-investment-reviews-2023-europe.

[151] Personal communication with Agathe Demarais, Global Forecasting Director of The Economist Intelligence Unit (EUI), July 17, 2023.

[152] Zandee and Stoetman, "Countering Hybrid Threats: The Role of the Joint Expeditionary Force."

NATO-EU collaboration

The EU and NATO seek to ensure that their efforts are complementary and they are exploring further avenues for counter-hybrid cooperation. The Joint Declarations of Warsaw (2016) and Brussels (2018) identify hybrid threats as one of the priority areas for EU-NATO cooperation. At least 20 out of the current 74 EU-NATO "proposals for common action" are related to countering hybrid threats.[153] The 2023 Joint Declaration noted "unprecedented progress" since 2018, with "tangible results in countering hybrid and cyber threats". The two organizations are also stepping up their collaboration when it comes to protecting critical infrastructure. In early 2023, they agreed to establish a new taskforce on resilience and critical infrastructure protection which will focus on making "[Europe's] critical infrastructure, technology and supply chains more resilient to potential threats" as well as taking action to mitigate potential vulnerabilities.[154] Making critical entities more resilient – including by scrutinizing FDI into critical infrastructure and networks, especially from potential adversaries like China – is another area that could benefit from enhanced EU-NATO collaboration in the future.[155]

The Nordic Defense Cooperation (NORDEFCO)

When it comes to addressing cyber interference/cyber resilience in particular, a common regional cyber security approach is emerging within the framework of the **Nordic Defense Cooperation (NORDEFCO)** – the primary vehicle for joint military collaboration between Sweden, Denmark, Finland, Iceland and Norway.[156] NORDEFCO already possesses the capacity to liaise with national cybersecurity agencies and military cyberthreat units in Nordic states. As part of its Defence Vision 2025 project, NORDEFCO's role will expand to also advance the deepening of cross-border cyber security collaboration, enhanced intelligence sharing, and the development of more effective joint cyber defense capabilities to respond to attacks against targets across the Nordic states.[157] In the words of Iceland's minister of higher education, science and innovation Áslaug Arna Sigurbjörnsdóttir, "the time is now right for a joint cyber security strategy."[158] In parallel to deepening their cyber security collaboration, all NORDEFCO members are individually increasing their defense and hybrid threat cybersecurity investments.[159]

[153] "Countering Hybrid Threats."

[154] "NATO and the EU Set up Taskforce on Resilience and Critical Infrastructure," *NATO*, January 11, 2023, https://www.nato.int/cps/en/natohq/news_210611.htm.

[155] Interview results.

[156] Gerard O'Dwyer, "Nordics Move towards Common Cyber Defence Strategy," Computer Weekly, March 21, 2023, https://www.computerweekly.com/news/365533113/Nordics-move-towards-common-cyber-defence-strategy#:~:text=The%20Nordic%20countries%20have%20adopted,threats%20from%20the%20cyber%20domain.

[157] Ibid.

[158] Ibid.

[159] Gerard O'Dwyer, "Nordic States Join Together to Bolster Cyber Defenses," *C4ISRNET*, October 6, 2017, https://www.c4isrnet.com/international/2017/10/06/nordic-states-join-together-to-bolster-cyber-defenses/.

The Joint Expeditionary Force (JEF)

Multinational formats such as the **Joint Expeditionary Force (JEF)** could also play a role in harmonizing national approaches to countering hybrid threats in the Arctic.[160] Launched in 2014, the JEF is a UK-led military coalition of like-minded countries, consisting of Denmark, Finland, Estonia, Iceland, Latvia, Lithuania, the Netherlands, Sweden, and Norway. As its membership composition suggests, the JEF focuses its activities on the High North, the North Atlantic and the Baltic Sea regions. Since 2019, the JEF has increasingly focused its activities on the hybrid domain. In their policy direction, published in July 2021, the JEF nations acknowledged the increasingly hybrid character of conflicts and the need to adapt "to be able to respond effectively to competitors operating in the space below the threshold of conventional conflict."[161] At the most recent JEF leaders meeting in Amsterdam in March 2023, the JEF nations reaffirmed their commitment to cooperating on addressing hybrid threats and stated that they have agreed to "accelerate cooperation [...] to detect, deter and respond to threats against our critical undersea and offshore infrastructure."[162] In their latest report, Dick Zandee and Adája Stoetman of the Clingendael Institute explore the opportunities and difficulties that might come along with a military cooperation format, such as the JEF having to operate in the hybrid domain. According to their analysis, one of the biggest advantages of the JEF is its flexible format of decision-making and deployment, which enables rapid action – particularly when compared to NATO, where consensus among 31 Allies is required to deploy forces. Zandee and Stoetman add that the JEF can also act as a "gap filler" – or a first responder force – in crises short of an open armed attack, before NATO takes over. Moreover, given the JEF's regional focus on Northern Europe, its members already have – to a great extent – shared threat perceptions and aligned security interests. Zandee and Stoetman consider information and intelligence-sharing – in order to optimize situational awareness on the character and nature of the hybrid threats – as a key area in which the JEF can add value.[163]

According to the interviews conducted for the purpose of this research, finding a unified approach to addressing hybrid threats in the Arctic would be challenging. Any such effort remains a delicate issue as it would inherently touch on issues of national sovereignty, and could result in push-back. A regional approach should neither dictate how states should act nor rule over decisions that are for the member states to take at the national level. Instead, the focus should be on the sharing of best practices, so as to better understand what has worked and what has not. The Western Arctic states can learn from each other in order to harmonize their whole-of-government arrangements, as well as to rely on existing frameworks to optimize their national approaches to the maximum extent possible. Currently, the Western Arctic states are not joined up on how they prioritize hybrid threats, which leads to an

[160] See Zandee and Stoetman, "Countering Hybrid Threats: The Role of the Joint Expeditionary Force."
[161] "Joint Expeditionary Force (JEF) – Policy Direction" (Ministry of Defence, July 12, 2021), https://www.gov.uk/government/publications/joint-expeditionary-force-policy-direction-july-2021/joint-expeditionary-force-jef-policy-direction.
[162] "Joint Statement by Joint Expeditionary Force Ministers, June 2023," GOV.UK, June 13, 2023, https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-june-2023.
[163] Zandee and Stoetman, "Countering Hybrid Threats: The Role of the Joint Expeditionary Force."

inconsistent response to malign interference. Changing the status quo to a regional approach that emphasizes sharing best practices would rely heavily on trust but would ultimately lead to a better and more unified approach.

Conclusions and recommendations

Designing an effective deterrence strategy to deal with hybrid threats is difficult: with gray zone aggression, perpetrators avoid detection and – in most cases – confident attribution. Unless an attacker wants to signal a provocation in order to demonstrate its capabilities so as to frighten the target country, it can very easily remain hidden. As a result, it is difficult for the target country to identify and punish the perpetrator. It is equally difficult – if not impossible – to measure the cumulative impact of hybrid warfare, which makes it harder to devise effective countermeasures.

There is no "one-size-fits-all" solution to countering hybrid aggression. It may also not be possible to entirely deter Russian hybrid aggression. Hybrid threats are tailor-made to exploit the weak points of the target state. The seven Western Arctic states have been targeted differently because of differences in their political cultures, pre-existing social, economic and demographic conditions, differing threat perceptions and relationship with Russia (both historic and present), and because current measures, organizational structures, and national strategies in place vary from one country to another.

Whole-of-government and whole-of-society approaches are best suited for dealing with the multidimensional threat that malign actors (including but not limited to Russia) pose. Transparent, open, and well-coordinated international, national, and local policies are required to effectively address this challenge.

Below, we outline our thoughts and recommendations:

1. Know one's weaknesses and improve situational awareness

At present, there is no common definition or understanding of hybrid threats across the Arctic region, which complicates cross-border cooperation and harmonization of national responses to hybrid threats. Establishing a unified understanding and definition of the threat is key to building resilience to hybrid interference. The conceptual model generated by the Hybrid CoE in Helsinki could serve as a model for an Arctic-wide typology of threats. It is equally important that Western Arctic states carry out risk and vulnerability assessments to better understand where their weaknesses lie in order to create preventative strategies, and evaluate what the future targets may be so as to design effective strategies to counter hybrid aggression proactively. In addition to developing a joint assessment of potential targets of hybrid activities, it may be useful to develop an inventory of actors – comprising both government actors as well as key private entities in vulnerable sectors – that can be reached in case a hybrid attack occurs.[164] Further, the cross-border sharing of information and joint intelligence efforts – across the EU, between the EU and NATO, and bilaterally – are essential in order to identify threats early on, understand how they are linked, and improve overall situational awareness, risk assessment and planning of counter-hybrid measures. Improving intelligence

[164] See Zandee and Stoetman.

sharing and cooperation should go hand in hand with the bolstering of regional intelligence, surveillance and reconnaissance (ISR) assets.[165]

2. Enhance transparency and public communications

It is important that governments clearly state when they uncover – or are targeted by – a hybrid campaign, and make the goals and activities of any particular malign actor visible to the broader public. Engaging in a debate and clearly stating when false arguments are being used can help raise public awareness of disinformation activities. But governments also have other options at their disposal, such as mechanisms for screening foreign investments or foreign funding disclosure. Strict and clear rules on financial transparency should be in place for political parties, research institutes, media and non-governmental organizations (NGOs) alike. Mandatory financial disclosures can help deter and disrupt alliances between foreign hybrid aggressors and domestic proxy groups.[166] If the origins of the funding can be tied to foreign security or intelligence organizations, the governments should be in a position to close down the recipient organization.[167] Collective attribution – arguably one of the strongest means of punishing a hybrid aggressor – remains a difficult issue, as it touches on national sovereignty.[168] Despite these challenges, Allies need to determine an effective messaging strategy that shows that hybrid activities will not be tolerated and that they will come at a cost that attackers may not be willing to pay (i.e. clearly signal to Russia that retaliation is feasible if attacked). Communicating successes is also critical. As above, this may entail enhancing transparency when hybrid activities are detected and shut down through official channels.

3. Establish good governance structures

Strong democratic institutions, a culture of democratic participation, and societal trust – not only towards the government and parliament but also the security authorities – are important ingredients of a whole-of-society and whole-of-government approach to countering hybrid threats. Good governance itself reduces the level of vulnerability, helps enhance social cohesion, and increases citizens' trust in public authorities.[169] While hybrid warfare seeks to exploit legal thresholds and gaps, liberal democratic governments must ensure that their counter-hybrid responses remain within the bounds of the rule of law, transparency, and democratic oversight.[170]

[165] Douglas Barrie et al., "Northern Europe, The Arctic and The Baltic: The ISR Gap" (IISS, December 19, 2022), https://www.iiss.org/research-paper/2022/12/northern-europe-the-arctic-and-the-baltic-the-isr-gap.

[166] Mikael Wigell, Harri Mikkola, and Tapio Juntunen, "Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats" (European Parliament, 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf.

[167] De Jong et al., "Inside the Kremlin House of Mirrors."

[168] Rühle and Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats."

[169] Matej Kandrik, "Assessment of the Approach of the Slovak Republic Towards Countering Hybrid Threats" (STRATPOL, 2020), https://stratpol.sk/wp-content/uploads/2021/05/Assessment-Slovakia.pdf.

[170] See De Jong et al., "Inside the Kremlin House of Mirrors."

4. Foster quality education and critical media literacy

A well-educated and informed population, media literacy programs, and proactive messaging can make a society more resilient to hybrid threats, particularly in the information domain. Governments need to ensure that both the general public and civil servants are wary of malign interference and that they understand that hybrid threats go beyond disinformation and cyberattacks, and constitute a broader strategic issue. Efforts should be undertaken to educate and train government officials, journalists, civil society representatives and the general public alike to understand how to navigate the online environment (as well as how it works), how social media posts are generated and paid for, as well as how to critically analyze the content they consume.[171] They have to be able to digest, analyze, make informed opinions about the news, and understand what they are dealing with. Governments bear a special responsibility to instill media literacy courses in primary and secondary school curricula.

5. Training and exercising

Consistent training and exercising is another important tool to deter and mitigate the effects of hybrid threats. Exercises can help identify possible hybrid threat scenarios, test hypotheses, as well as tactics and procedures (such as contingency plans). On the whole, they can help improve incident response mechanisms, prepare participating entities for the full range of potential contingencies that they might face, and enable them to work together to identify best practices and lessons learned.[172] NATO's 2018 Trident Juncture exercise, for instance, enabled Norway to exercise and validate different aspects of its approach to resilience, notably enhanced civil-military cooperation.[173] Hybrid warfare tabletop exercises developed by the Hybrid CoE, Finland's National Defence Course for leaders in every sector, or Sweden's "total defense" exercise[174], are among initiatives that other Arctic states could replicate. Such training and exercises should be conducted at the national, regional, and international level so as to better counter sub-threshold threats that can occur at different levels. Training and exercising is an area where the EU-NATO cooperation could be deepened, in order to complement and reinforce capabilities of both organizations.

[171] See, for example, a UK strategy: "Minister Launches New Strategy to Fight Online Disinformation," July 14, 2021, https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation.

[172] See, for example, Shino Rybski, "Comprehensive Security Together #6: The Role of Exercises in Countering Hybrid Threats" (The Security Committee, 2021), https://turvallisuuskomitea.fi/en/comprehensive-security-6-the-role-of-exercises/.

[173] "Norway Uses Exercise Trident Juncture to Strengthen Its National Resilience," *NATO*, November 6, 2018, https://www.nato.int/cps/en/natohq/news_160130.htm?selectedLocale=en.

[174] "Total Defence Exercise 2020" (Swedish Civil Contingencies Agency, December 3, 2020), https://www.msb.se/en/training--exercises/ovningar/total-defence-exercise-2020/.

6. Crisis preparedness

Related to training and exercising is **crisis preparedness**. The governments ought to enhance civilian preparedness and ensure that both civilian authorities and citizens are familiar with different worst case scenarios and know how to function in the event of a serious crisis (e.g. a power outage, disruption of communications systems, etc.). According to Elisabeth Braw, the public needs to be constantly updated about prospective crises and how to prepare for them. "Thinking about crises is not enjoyable, but COVID and the Ukraine War have painfully demonstrated that thinking about events before they occur trumps having to collectively improvise while the crises are occurring," Braw writes.[175] Sweden provides a good example to follow. In 2018, the Swedish government sent every household a pamphlet titled "If Crisis or War comes", with the aim to educate its citizens on how to function in the event of an emergency – be it caused by a cyber or terror attack, natural disaster, disinformation campaign or any other crisis.[176]

7. Break down silos and encourage horizontal coordination

Information sharing is still considered to be too vertical, with different entities operating in "silos". Other limiting factors include resource competition between governmental agencies, general lack of trust between actors, and unclear administrative responsibilities at times. What is more, hybrid threats are designed to make coordinated countermeasures difficult.[177] To strengthen a whole-of-government and whole-of-society response to hybrid threats, it is important to break down silos inside governments, between different government agencies, between institutions, and between the government and the private sector. Greater integration of military and non-military discussions on Arctic vulnerabilities is equally important to better understand the extent to which Arctic communities are exposed to harm.

8. Cooperate within coalitions and capitalize on existing frameworks

Given the nature of hybrid threats, it is essential to work across agency boundaries and geographical borders. Governments must recognize the added value of regional as well as international cooperation in dealing with Russian hybrid operations – rather than believing it is sufficient to respond unilaterally – and capitalize on existing frameworks. The JEF, NORDEFCO, the EU and NATO already provide Western Arctic states with a wide range of tools to respond to hybrid campaigns. The sharing of best practices (what has worked) and lessons learned (what needs improving) within existing frameworks is essential. We need to deepen the cooperation at the EU and NATO level, between the EU and NATO, as well as between public and private entities. It is equally important that counter-hybrid

[175] Elisabeth Braw, "Murky Threats: Why Defense Against Gray-Zone Aggression Needs a Whole-of-Society Approach," *49security*, January 9, 2023, https://fourninesecurity.de/2023/01/09/why-defense-against-gray-zone-aggression-needs-a-whole-of-society-approach.

[176] "The Brochure If the Crisis or the War Is Coming" (Swedish Civil Contingencies Agency, 2018), https://www.msb.se/sv/rad-till-privatpersoner/broschyren-om-krisen-eller-kriget-kommer/.

[177] Mikael Wigell and Emma Hakala, "Towards a Greener Defence: An Introduction," in *Innovative Technologies and Renewed Policies for Achieving a Greener Defence*, NATO Science for Peace and Security Series C: Environmental Security (Springer, 2022).

responses at the local, national and international level are well coordinated and optimized to effectively address this challenge.

9. Avoid unintentional escalation in the Arctic

Given the visible increase in military activity in the Arctic region, and the number of close encounters with Russian aviation and naval units, it is particularly important for the Arctic states to have mechanisms in place to reduce the risk of unintended escalation. Even though the trust is gone, we still need confidence in military stability in the Arctic. Basic risk reduction mechanisms *can* be agreed even when there is a high degree of distrust. While it is difficult to imagine that a new agreement will be negotiated in a multilateral format, those states that currently lack an agreement equivalent to the INCSEA or DMA – all while maintaining military forces in the proximity of Russia – might consider replicating existing agreements on a bilateral basis. Here, the US-Russia INCSEA agreement, and the US-Russia DMA agreement are broadly considered as best examples to replicate. In the next step, all INCSEA and DMA agreements could be complemented with real-time hotlines between military commanders to deal with accidents as they happen.

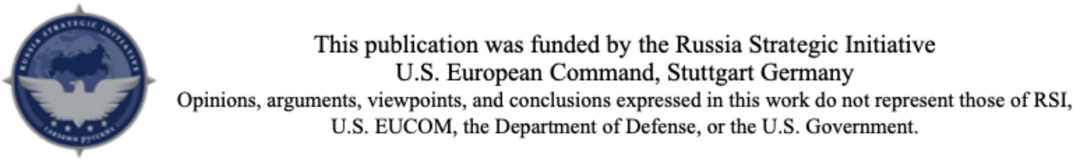
10. Broaden social inclusion

Arctic governments should pay equal attention to implementing targeted programs focusing on the integration of marginalized diasporas and minorities. Such programs could specifically engage with Russian speakers in their own language. In many cases, Arctic communities have a history of reckoning with colonialism, and forced assimilation into Western communities both through schooling programs for children as well as other forced “Western” educational systems. These legacies contribute to distrust towards decision-making centers. Additionally, ensuring that the economic and social needs of these communities are addressed would go a long way in enhancing their resilience to outside interference.

11. Invest effort in understanding Russian intent

Understanding Russian intent and what Moscow hopes to achieve may be key in planning effective mitigation and defense. For example, what is Russia’s intent in conducting hybrid campaigns in the Arctic? Is the primary aim to destabilize individual Western Arctic countries or to create a general incoherence in the region? Both possibilities have different strategies and thus different mitigations that go along with them. Furthermore, Arctic countries that have land or sea borders with Russia may well be placed to help others in understanding Russian intent and capability.

The opinions articulated above do not necessarily reflect the position of the ELN or any of its members. The ELN's aim is to encourage debates that will help develop Europe's capacity to address the pressing foreign, defence, and security policy challenges of our time.



This publication was funded by the Russia Strategic Initiative
U.S. European Command, Stuttgart Germany
Opinions, arguments, viewpoints, and conclusions expressed in this work do not represent those of RSI,
U.S. EUCOM, the Department of Defense, or the U.S. Government.

EUROPEAN
LEADERSHIP
NETWORK

The European Leadership Network (ELN) is an independent, non-partisan, pan-European NGO with a network of nearly 200 past, present, and future European leaders working to provide practical real-world solutions to political and security challenges.

European Leadership Network
8 St James's Square
London, UK, SE1Y 4JU

secretariat@europeanleadershipnetwork.org
@theELNeuropeanleadershipnetwork.org