From the High North to the Homeland: What Norway's Evolving Risk Assessments Mean for U.S. Homeland Defense

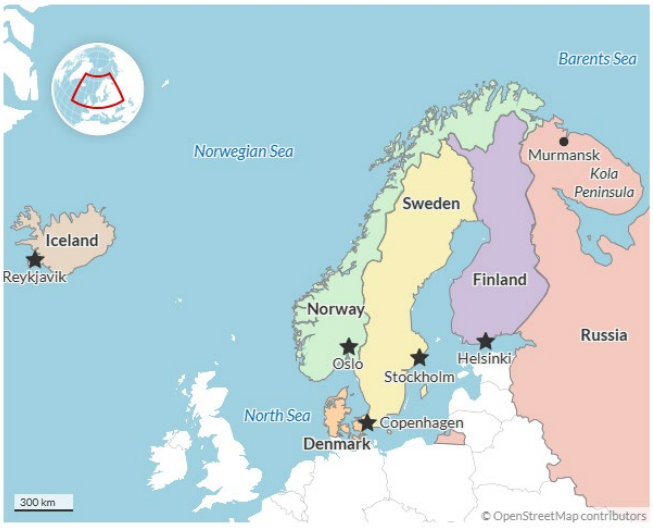
Ria Hanson, Ted Stevens Center for Arctic Security Studies

April 2026

"Global integration" is identified as a central strategic principle in the North American Aerospace Defense Command (NORAD) and United States Northern Command (USNORTHCOM) Strategy document.[1] The document emphasizes "leveraging Allies' and partners' strengths to ensure defense of the continent," and identifying "existing networks for integration." As great power competition reemerges, U.S. decision-making and deterrence is bolstered by allied perspectives and capabilities. In this context, Norway – one of the United States' longest-standing Arctic allies – offers a valuable reference point. Its evolving risk assessment in the European High North may help inform U.S. Arctic planning, while also highlighting opportunities for expanded cooperation in support of homeland defense and broader mission requirements in the Arctic region.

Norway's Perspective

In situ research involving expert panels and perspectives from Norwegian naval operations experts and emergency response practitioners highlighted a specific finding: Norwegian assessments suggest that Russia may consider kinetic activity in the European High North following their conflict in Ukraine, potentially



[1] U.S. Department of Defense, "NORAD and USNORTHCOM Strategy."

aimed at expanding Russian presence around the Kola Peninsula.[2] This concern is particularly evident among military operators, who emphasize the role of Russia's Northern Fleet in its broader defensive posture. While territorial expansion is not the sole or primary risk from Russia identified by Norway, the inclusion of such a scenario reflects a distinct shift in its modern threat perception. The Norwegian Intelligence Service (NIS) publishes an annual threat assessment, "Focus," which provides insight into this evolution. A review of these assessments from 2017-2026 shows a gradual but discernible change in how Norway characterizes Russia as a potential risk to its homeland security.

From 2017 to 2026, "Focus" notes growing Russian distrust of Western intentions, alongside elevated strategic importance of the Northern Fleet in supporting Russia's Arctic posture. The Norwegian assessments increasingly emphasized Russian activity in the High North, including live firing exercises, jamming GPS signals for civilian and allied air traffic over northern Norway, and deploying surface vessels and patrol aircraft to North Atlantic Treaty Organization (NATO) exercise areas. The "Focus" issues also highlight Russian expansion of cyber activities and misinformation campaigns. Simultaneously, Russia continues to build its Arctic operational capabilities.[3]

Gray-zone Risks

Recent Focus assessments highlight cyber-attacks, misinformation campaigns and infrastructure damage, particularly to communication technology, as major risks to Norway

[2] "Naval Activity and Emergency Response Coordination in Norway."
[3] Folland, "Arctic Strategy: Deterrence and Détente."

and NATO in the European High North. After attending the 2025 Arctic Security Round Table, Norwegian Major General Elisabeth Michelsen, Deputy Chief of Staff for Operations at Joint Force Command (JFC) Norfolk, highlighted the calculated and targeted nature of Russian "destabilization operations," which is often classified as "gray zone warfare." Major General Michelsen stated, "These are not accidental, but part of a calculated and targeted strategy to undermine and break down cohesion and stability in both Norway and the West... They affect us in the cognitive domain and carry out covert sabotage operations either against physical "things" or digitally. It's not war, but it's not peace either."[4]

Consider the Russian influence campaign known as "DoppelGänger."[5] It has been running since 2022, operated by the Russian Social Design Agency and Structura National Technologies. DoppelGänger works to promote pro-Russian narratives by infiltrating the western media landscape. The campaign uses generative AI to create and disseminate information through various means including social media manipulation, fake articles and cloned websites, including NATO's website and The Guardian.

Further, in 2026, NIS reported that it expects Russian espionage and potential sabotage targeting Arctic infrastructure to increase.[6] Legitimizing this expectation, Russia conducted a covert operation in early 2026 with two intelligence gathering submarines from the Main Directorate of Deep Sea Research (GUGI) around critical undersea

[4] Michelsen, "Russian destabilization and NATO's multidomain operations."
[5] Office of Public Affairs, "Russian Disinformation Campaign 'DoppelGänger' Unmasked."
[6] Norwegian Intelligence Service, "Focus 2026: Threat Assessment."

infrastructure in Norwegian and British maritime areas.[7] When the British government released a statement that it had tracked this Russian covert operation in cooperation with allies, Russia responded with a statement claiming Norway is assisting Ukraine in preparing attacks on Russian vessels in the Barents and Norwegian Seas.[8]

Kinetic Risks

Norway is assuming an increased willingness from Russia to take offensive action to reach its long-term goals in the Arctic. As Russia continues feeding military capability into Ukraine, the Northern Fleet increases in importance as Russia's primary defense mechanism still dedicated to the Arctic. Thus, a land grab from Norway to establish a greater buffer around the Kola Peninsula is considered one of the biggest kinetic risks in the region.[9] General Eirik Kristoffersen, Norway's Chief of Defense, states this plainly: "We don't exclude a land grab from Russia as part of their plan to protect their own nuclear capabilities, which is the only thing they have left that actually threatens the United States."[10] He indicated that while there was no expectation of a full annexation attempt, the proximity of high value nuclear facilities on the Kola Peninsula make the European High North a potential flashpoint. The entry of Sweden and Finland into NATO only heightens this risk, as Russia no longer has a buffer against NATO along Russia's western flank.

[7] Nilsen, "UK and Norway Expose Russian Operation near Undersea Infrastructure."
[8] Nilsen, "Russian Propaganda Claims Norway Is Helping Ukraine Prepare Attacks on Vessels in Northern Waters."
[9] "Naval Activity and Emergency Response Coordination in Norway."
[10] Walker, "Norway Defence Chief Says Russia Could Invade to Protect Nuclear Assets."

Russia-China Cooperation

Russia's 2023 *Foreign Policy Concept* discusses "mutually beneficial cooperation with non-Arctic states that pursue a constructive policy toward Russia and are interested in international activities in the Arctic."[11] Russia depends on international partners in the Arctic to achieve its economic potential, due to a lack of resources, technology and knowledge that Russia can put forth independently. In practice, this means a renewed effort by Russia toward cooperation with China in the Arctic.

Russia and China are deepening military and diplomatic ties as relations with the West continue to deteriorate. Russia and China are conducting joint patrols in the Arctic and Pacific, by air and sea, that enter the Alaska air defense identification zone (ADIZ) and U.S. exclusive economic zone (EEZ).[12] Beyond joint patrols near U.S. territory, the current relationships between Russia and China may also provide Russia with opportunities to gather information about China's offensive naval strategies.

Map Source: Åtland, Kristian. (2024). The High North after Russia's Invasion of Ukraine: Military Signaling and East-West Interaction.

[11] Devyatkin and Lipunov, "The Arctic in the 2023 Russian Foreign Policy Concept."

[12] Popeski and Kelly, "Russia Says Its Navy in Joint Patrols with China in Pacific"; Mahadzir, "Russian, Chinese Warships Operated Near Alaska, Say Senators."

In the South China Sea, China is currently creating several overlapping bastions to pursue its geopolitical goals in the Pacific. Meanwhile, Northern Fleet activity around or through the Bear Island and GIUK gaps is recognized as a key warning sign to NATO of Russian operations and sea-denial efforts, and sea denial south from the Bear Gap to the GIUK Gap is one of the operational effects Russia must achieve for success in armed conflict with NATO.[13] Additionally, Russian submarine technology is continuing to improve. Together, these realities create an environment where Russia may try to employ methods from China's offensive bastion strategies to achieve sea denial through the Bear-GIUK gap region. It is unlikely that China would be directly involved in conflict in the European High North, nor that Russia would want it to be involved, but this does not preclude Russia from learning Chinese strategies to apply in the North.

Impacts on the U.S. Homeland Defense Mission

Continued risks of gray zone activity, including cyber-attacks, misinformation campaigns and sabotage of communication infrastructure as identified in the NIS "Focus" assessments have implications for the security of the United States as an Arctic nation, neighbor of Russia and member of NATO. If Russia's war on Ukraine subsides, Norway is concerned about kinetic activity in the European High North, specifically, a land grab around the Kola Peninsula. The possibility of Russia moving away from the defensive

[13] Halsne, "Competitive Strategies in the European High North"; Black et al., *Enhancing Deterrence and Defence on NATO's Northern Flank*.

bastion strategy toward more circumpolar naval activity is also gaining more attention. These risks relate directly to the U.S. homeland defense mission.

Cyber-Attacks

Consider the November 2020 cyber-attacks on Estonia. The operation included three attacks on Estonia's national information technology (IT) infrastructure and an attack against the Foreign Ministry's external website servers.[14] In 2022 another attack hit Estonia, Ukraine and the United States, as well as 23 other NATO nations who were providing support to Ukraine.[15] The hackers' goal was to deposit a cyberweapon on targeted Ukrainian computers that would destroy the target computer and related data before the Russian invasion of Ukraine. The attackers also exfiltrated sensitive data and offered it for sale on the internet. After national and international investigations, six Russian hackers were charged, five of whom were officers in Unit 29155 of the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces.

A cyber-attack against a government system leads to reduced security of that system until the breach is confined and all impacted areas are identified and addressed. In the interim, certain network capabilities may not be available, reducing operability and slowing communication within the system. Any new information sharing must be restricted

[14] ERR, "Russian Military Intelligence Organized Cyberattacks against Estonian Institutions."
[15] Office of Public Affairs, "Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government."

or done over alternative channels. This is a significant disability in an environment that relies on quick decision-making over vast distances, like the Arctic. Additionally, any information shared on an attacked network is at risk of discovery by the adversary. In the case of a cyber-attack on Norway, the U.S. might experience a reduced ability to cooperate or communicate with Norway, a key Arctic ally, or be at risk of having sensitive information from or about the U.S. exposed.

Misinformation Campaigns

As an Arctic nation, the U.S. benefits from the support of NATO allies in the Arctic, especially now that Sweden and Finland have joined the organization. NATO deters Russia in the Arctic far more effectively than seven fragmented nations could. Thus, Russia's efforts to use misinformation to undermine the cohesion of NATO nations internally and as an organization is dangerous to the U.S.

Misinformation campaigns involve circulating false information that confuses or undermines the intentions or capabilities of a state or an organization such as NATO. If successful, misinformation campaigns can undermine citizen support and state commitment to an organization or mission. This can fracture the governing body and distort mission focus, reducing efficacy and power projection. Even if misinformation campaigns are not entirely successful in directly undermining the cohesion of NATO or Norway, they can still act to slow decision-making processes by introducing the need to filter for false information and narratives. This challenge continues to grow as

technological innovation and AI integration make it increasingly easy to generate and disseminate false narratives in a convincing manner.

Infrastructure Damage

Undersea telecommunication cables carry about 99% of transoceanic digital communications including phone calls, online communications and financial transactions.[16] Infrastructure damage, particularly to communications infrastructure like undersea cables, is a major risk to the U.S. because it can shut down entire systems that take significant time, expertise, and investment to repair. Many undersea telecommunication cables land in the U.S. and support government communications including for the military, diplomatic, and national security agencies. A cable break could lead to the inoperability of financial markets or transactions between nations for goods as impactful as oil and gas or make military coordination across regions significantly more challenging. In the Arctic, and particularly the U.S. Arctic, infrastructure is sparse. There are usually few back-up options to keep operations running.

Such infrastructure sabotage is also particularly impactful because it is directly and immediately felt by civilian populations. When civilians are victims, the shockwaves of damage travel further, faster. For example, in February of 2024, multiple cables were cut in

[16] Carter et al., "Protection of Undersea Telecommunication Cables."

the Red Sea which caused internet traffic to slow between Asia, Africa and Europe impeding civilian use of Microsoft, Google and Amazon.[17]

In April 2026, China's Ministry of Natural Resources reported that the research vessel, "Haiyang Dizhi 2," completed a deep-sea scientific mission that included a cutting test of a deep-sea electro-hydrostatic actuator at a depth of 3,500 meters (11,483 feet).[18] The device is presented as a tool to aid in the construction and repair of deep-sea pipelines. However, it is also capable of severing the most fortified undersea fiberoptic cables. With or without cooperation with Russia, this increases the risk posed to undersea infrastructure that the U.S. and allies rely on.

There is an additional challenge in that some infrastructure sabotage may be disguised to look like a natural event. In June 2023, naturally shifting ice severed an undersea cable serving the North Slope of Alaska, affecting internet and cell service for residents in the U.S. Arctic region. As tensions rise in the Arctic, events such as these could be used to excuse future cable damage even though current estimates place only 14 percent of cable damage events as having natural causes.[19]

Beyond blaming deliberate sabotage on a natural event, there is also the possibility of using winter storms, typhoons, tsunamis, flooding or wildfires as a window of opportunity to cover infrastructure sabotage, hidden behind the noise and confusion of

[17] Monaghan et al., *Red Sea Cable Damage Reveals Soft Underbelly of Global Economy*.
[18] Tong, "China Tests Submarine Cable Cutter at 3,500-Metre Depth."
[19] Carter et al., "Protection of Undersea Telecommunication Cables."

humanitarian or disaster response efforts.[20] Constant surveillance for adversary activity and a deep understanding of natural events are required to ensure natural risks are minimized and sabotage is identified for what it is. The emergence of drones as a mechanism for damage to surface infrastructure is another significant development. Long-term planning must now account for defense against drone damage as well as natural and human-effected damage.

Kola Land Grab and the Northern Fleet Bastion

If Russia were to make a land grab near the Kola Peninsula, it would invoke NATO's Article 5, requiring an allied response. The Supplementary Defense Cooperation Agreement (SDCA) between the U.S. and Norway increases the probability that U.S. troops might be involved in these efforts from an early stage. The challenging operating environments of the Arctic and near-Arctic stretch response times and infrastructure capabilities. The high tempo of modern warfare places a heavy burden on the credible threat of rapid and lethal response. A poor initial response increases the probability of a protracted conflict and unnecessary costs incurred for all allies. Limited Arctic resources and infrastructure make sustained conflict challenging, increasing the importance of NATO's initial ability to respond.

Lastly, the advent of new technology also increases the importance of the Arctic as a strategic center of gravity. Russia and China are at the forefront of developing long-range and high-speed precision guided weapons.[21] The capabilities of these modern weapons

[20] Moerbe, "Hybrid Threats in the Arctic Pacific."
[21] Halsne, "Competitive Strategies in the European High North."

significantly increase access to North America over the pole, from the Kola Peninsula or elsewhere.[22]

Offensive Bastion Concept and Circumpolar Naval Operations

As of early 2026, Russia has modernized its Pacific Fleet of SSBNs more than its Northern Fleet of SSBNs. Thus, an offensive bastion strategy from Russia may be exercised in the Pacific before it is employed in the Arctic.[23] This poses a risk to the Bering Strait region in its unique role as the Pacific entrance to the Arctic. There is also potential spillage of conflict in the Pacific traveling north, or the possibility that Russia may attempt to secure the Bering Strait before instigating any kinetic activity in the European High North. A more robust Russian navy with methods learned from China may increase the latter possibility.

A more active and capable Russian navy in the Arctic makes Arctic allied air and naval capabilities increasingly more important. As Russia becomes less tied to bastion defense and more of an offensive player in the Arctic, the Alaskan coastline in the Arctic becomes more vulnerable. Additionally, the probability that the Bear Island and GIUK gaps become potential flashpoints increases, bringing conflict with Russia closer to the U.S. homeland.

Options for Further Consideration

[22] Special Operations Association of America, "The Power of Allies: Continuing U.S.-Norway Partnership in the High North."

[23] Kjellén, "The Russian Northern Fleet Bastion Revisited."

Russia is a permanent presence in the Arctic, and as it builds up its military forces and continues its assault on Ukraine, credible Arctic deterrence is non-negotiable for the U.S., Norway and NATO. Cooperation between the U.S. and Norway can improve planning and response capabilities for both nations and the broader NATO alliance. Both nations are direct neighbors to Russia and guardians of the two major sea entrances to the Arctic region, the Bering Strait and the GIUK gap. Norway controls sea lanes and air approaches that any actor in the Arctic must account for, and the U.S. brings firepower that Norway could not provide alone.[24] Options for burden-sharing could range from military exchanges where Norway comes west to gain experience with Chinese naval tactics, to improving intelligence, surveillance and response (ISR) networks through integrated models like the Canadian Rangers, or strengthening information campaigns facilitated by professional and cultural exchange programs through entities like the National Guard or State Department. More research is needed to fully understand the long-term implications of Norway's changing risk assessment toward Russia for U.S. homeland defense, and how resources should be targeted in response.

Author's Disclaimer: The views expressed in this Brief are those of the author and do not reflect the official policy or position of the U.S. Department of Defense or of the U.S. Government.

[24] Special Operations Association of America, "The Power of Allies: Continuing U.S.-Norway Partnership in the High North."

References

Black, James, Stephen J. Flanagan, Gene Germanovich, et al. *Enhancing Deterrence and Defence on NATO's Northern Flank: Allied Perspectives on Strategic Options for Norway*. 2020. https://www.rand.org/pubs/research_reports/RR4381.html.

Carter, Nicole T., Laura B. Comay, Patricia Moloney Figliola, et al. "Protection of Undersea Telecommunication Cables: Issues for Congress." Congress.Gov, August 7, 2023. https://www.congress.gov/crs-product/R47648.

Devyatkin, Pavel, and Nikita Lipunov. "The Arctic in the 2023 Russian Foreign Policy Concept." *The Arctic Institute - Center for Circumpolar Security Studies*, May 30, 2023. https://www.thearcticinstitute.org/arctic-2023-russian-foreign-policy-concept/.

ERR. "Russian Military Intelligence Organized Cyberattacks against Estonian Institutions." With Valner Vaino and Marcus Turovski. Estonia, September 5, 2024. https://news.err.ee/1609445381/russian-military-intelligence-organized-cyberattacks-against-estonian-institutions.

Folland, Maj Gen Rolf. "Arctic Strategy: Deterrence and Détente." Senior Leader Perspective. *Journal of Indo-Pacific Affairs*, October 2022.

Halsne, Sigbjørn. "Competitive Strategies in the European High North." *Scandinavian Journal of Military Studies* 5, no. 1 (2022). https://doi.org/10.31374/sjms.93.

Kjellén, Jonas. "The Russian Northern Fleet Bastion Revisited." *Journal of Advanced Military Studies* 2025, no. SI (2025): 7–27. https://doi.org/10.21140/mcuj.2025SI001.

Mahadzir, Dzirhan. "Russian, Chinese Warships Operated Near Alaska, Say Senators." *USNI News*, August 6, 2023. https://news.usni.org/2023/08/06/russian-chinese-warships-operated-near-alaska-say-senators.

Mason, Shane. "Battle of the Bastions." *War on the Rocks*, January 9, 2020. https://warontherocks.com/2020/01/battle-of-the-bastions/.

Michelsen, Elisabeth. "Russian destabilization and NATO's multidomain operations." LinkedIn, February 2025. https://www.linkedin.com/in/elisabeth-michelsen-15426313/recent-activity/all/.

Ministry of Local Government and Regional Development. "Norway in the High North – Arctic Policy for a New Reality." Pressemelding. Government.No, Regjeringen.no, August 27, 2025. https://www.regjeringen.no/en/whats-new/norway-in-the-high-north-arctic-policy-for-a-new-reality/id3116990/.

Moerbe, Wes. "Hybrid Threats in the Arctic Pacific." *Executive Briefs*, April 4, 2025, 3.

Monaghan, Sean, Michael Darrah, Eskil Jakobsen, and Otto Svendsen. *Red Sea Cable Damage Reveals Soft Underbelly of Global Economy*. March 7, 2024. https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy.

"Naval Activity and Emergency Response Coordination in Norway." January 2026.

Nilsen, Thomas. "Russian Propaganda Claims Norway Is Helping Ukraine Prepare Attacks on Vessels in Northern Waters." April 9, 2026. https://www.thebarentsobserver.com/security/russian-propaganda-claims-norway-is-helping-ukraine-prepare-attacks-on-vessels-in-northern-waters/448337.

Nilsen, Thomas. "UK and Norway Expose Russian Operation near Undersea Infrastructure." April 9, 2026. https://www.thebarentsobserver.com/security/uk-and-norway-expose-russian-operation-near-undersea-infrastructure/448299.

Norwegian Intelligence Service. "Focus 2017: Threat Assessment." Accessed March 17, 2026. https://www.forsvaret.no/en/news/publications/Focus_2017_2002_English_v2.pdf/_/attachment/inline/387ad7df-f4ad-477b-bda7-9cfc469702c5:6fd3d3056a6ee63cfe521ab912e7736db91203f2/Focus_2017_2002_English_v2.pdf.

Norwegian Intelligence Service. "Focus 2024: Threat Assessment." Accessed March 17, 2026. https://www.etterretningstjenesten.no/publikasjoner/fokus/focus-in-english/Focus2024%20-%20EN%20-%20Printer-friendly%20v4.pdf/_/attachment/inline/9ed8c4d1-a368-4b40-91b8-c6e2af87aefb:1be4c6860a051d7177386285600ebe6e526a55ba/Focus2024%20-%20EN%20-%20Printer-friendly%20v4.pdf.

Norwegian Intelligence Service. "Focus 2026: Threat Assessment." Etterretningstjenesten. Accessed March 13, 2026. https://www.etterretningstjenesten.no/publikasjoner/focus/focus2026_contents.

Office of Public Affairs. "Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government." U.S. Department of Justice, September 5, 2024. https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government.

Office of Public Affairs. "Russian Disinformation Campaign 'DoppelGänger' Unmasked: A Web of Deception." U.S. Cyber Command, September 3, 2024. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/.

Office of the Prime Minister. "Government to Provide Additional NOK 115 Billion to Strengthen Long-Term Defence Plan." Pressemelding. Government.No, Regjeringen.no, March 27, 2026. https://www.regjeringen.no/en/whats-new/government-to-provide-additional-nok-115-billion-to-strengthen-long-term-defence-plan/id3155063/.

Popeski, Ronald, and Lidia Kelly. “Russia Says Its Navy in Joint Patrols with China in Pacific.” World. *Reuters*, September 15, 2022. https://www.reuters.com/world/russian-chinese-navies-conduct-joint-patrols-pacific-russian-defence-ministry-2022-09-15/.

Special Operations Association of America. “The Power of Allies: Continuing U.S.-Norway Partnership in the High North.” January 7, 2026. https://soaa.org/us-norway-partnership/.

Tong, Zhang. “China Tests Submarine Cable Cutter at 3,500-Metre Depth.” South China Morning Post, April 15, 2026. https://www.scmp.com/news/china/science/article/3350174/china-tests-submarine-cable-cutter-3500-metre-depth.

U.S. Department of Defense. “NORAD and USNORTHCOM Strategy.” Accessed March 22, 2026. https://www.northcom.mil/Strategy/.

U.S. Intelligence Community. “2026 Annual Threat Assessment of the U.S. Intelligence Community.” Site page. Office of the Director of National Intelligence, March 22, 2026. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2026/4141-2026-annual-threat-assessment.

Walker, Shaun. “Norway Defence Chief Says Russia Could Invade to Protect Nuclear Assets.” World News. *The Guardian*, February 10, 2026. https://www.theguardian.com/world/2026/feb/10/norway-defence-chief-russia-nuclear-assets.