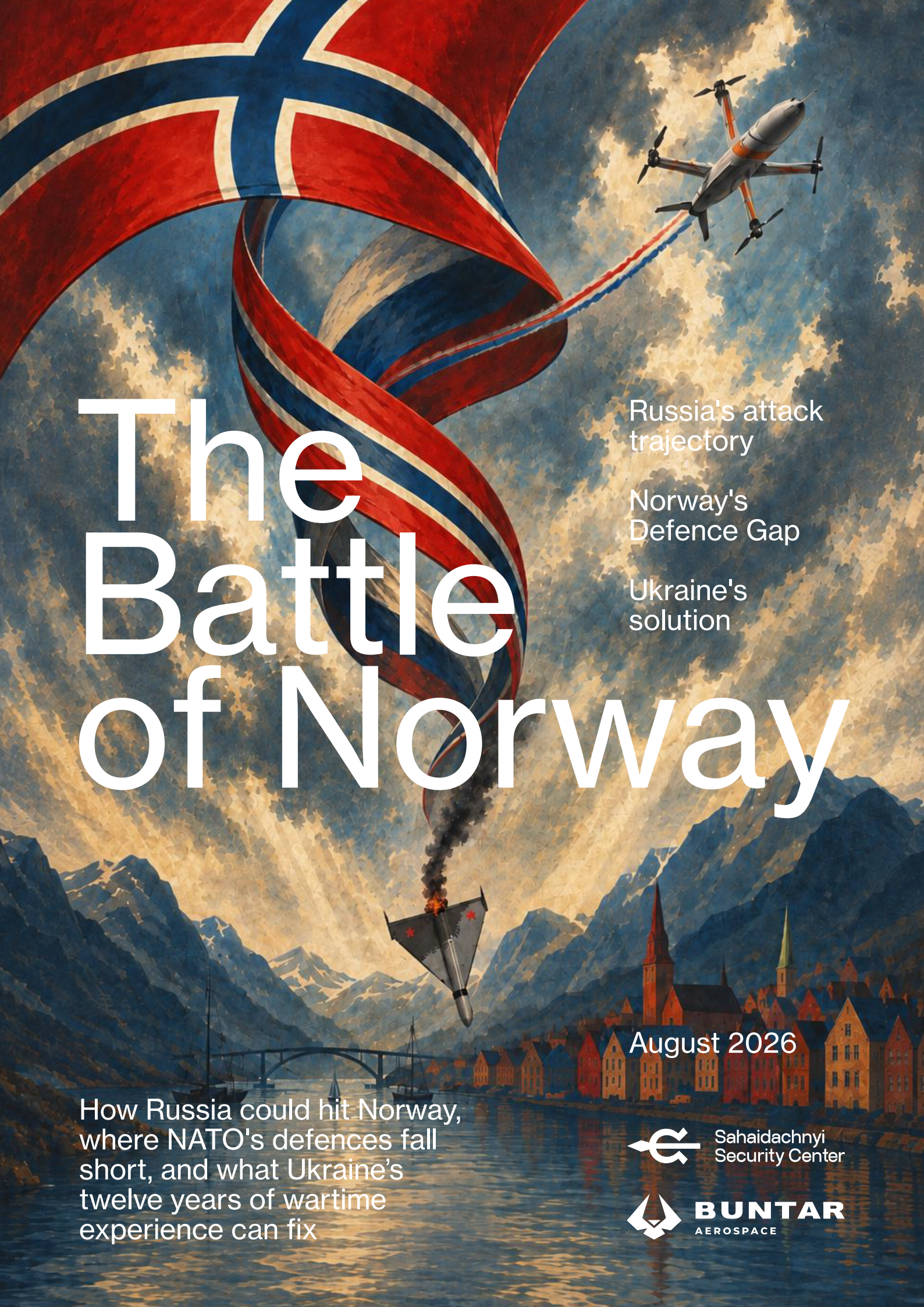


The Battle of Norway

Russia's attack trajectory

Norway's Defence Gap

Ukraine's solution

August 2026

How Russia could hit Norway, where NATO's defences fall short, and what Ukraine's twelve years of wartime experience can fix

Sahaidachnyi Security Center

BUNTAR AEROSPACE

This study was supported by Buntar Aerospace and prepared by the Sahaidachnyi Security Center in support of a stronger Ukraine – Norway Strategic Defence Partnership.

Drawing on twelve years of Ukraine's wartime experience, including more than four years of high-intensity warfare, the study examines how Russia could challenge Norway across multiple domains, identifies critical gaps in Norway's and NATO's existing defence posture, and assesses how Ukraine's combat-tested capabilities, technologies, and operational experience can help address them.

The study is intended to contribute to a forward-looking strategic dialogue between Ukraine and Norway: one that moves beyond assistance to Ukraine towards deeper defence cooperation, joint capability development, and a shared approach to strengthening European security.

Sahaidachnyi Security Center is a Ukraine-based think tank dedicated to the security and defense sector. Its mission is to provide top officials in Ukraine and worldwide with strategic recommendations on security and defense issues in and around Ukraine.

Buntar Aerospace is a Ukrainian defence tech company building the interface between humans and robotic combat systems. It transforms the battlefield from a manual environment into an ecosystem where troops and autonomous systems jointly execute missions.

Sahaidachnyi Security Center

BUNTAR AEROSPACE

Analytical Framework, Sources and Limitations

This paper sets out the original analytical vision and insights of the Sahaidachnyi Security Center. Certain assessments of Norway's current capabilities necessarily rely on publicly available information and may therefore not fully capture capabilities, arrangements or dependencies that are classified or otherwise not publicly documented. Where the discussion concerns the warfare trends and the Russian aggressor's potential, they build on a multi-year research framework exploring both the Russian-Ukrainian war as a prototype of next-generation warfare and the knowledge on military capabilities and fighting doctrine of the Russian aggressor.

The factual data and figures supporting the research claims and conclusions are drawn from credible sources including: Norwegian Intelligence Service, Norwegian Police Security Service (National Threat Assessment 2026), Finnish Defence Intelligence, Ukrainian Defence Intelligence and General Staff assessments, NATO/SHAPE and Allied Maritime Command public releases, Norway's Long-term Defence Plan 2025–2036, including its March 2026 funding revision, Norwegian Ministry of Defence and Defence Materiel Agency releases, the Norwegian Armed Forces' drone strategy white paper, NATO IAMD policy documentation, Norwegian and Ukrainian government and ministry statements on Brave-Norway and the April 2026 Oslo declaration, Kongsberg Group and Kongsberg Defence & Aerospace public releases, European Commission documentation on the Readiness Roadmap 2030, EDDI and the Action Plan on Drone and Counter-Drone Security, Ukrainian military and intelligence statements on Russian drone force expansion, and open-source defence-industrial reporting current to August 2026.

Figures on Russian capability generation and military industry production carry inherent uncertainty and are presented as order-of-magnitude estimates rather than verified numbers.

Procurement timelines are as stated in current government and contractor announcements and remain subject to revision.

Contents

Executive summary	05
Preface	09
1. The Threat Environment	13
1.1. Strategic Vulnerability Window	13
1.2. The “Battle of Britain” Remastered in the Drone Era	16
1.3. Russian War Machine: Bigger Problem Now Than in 2022	22
1.4. Framing the Threat for Norway: Low-Probability Scenarios	26
1.5. High-Probability Scenario: Projected Trajectory	27
1.6. The Defence Challenge	31
2. The Capability Gap	32
2.1. Not “Just Another Weapon”	32
2.2. Countering Massed Combined Air Offensive	35
2.3. Countering Sabotage at Scale	41
2.4. Sea Denial in Full-Scale War	42
2.5. Deterrence on the Ground	44
2.6. Electronic Warfare.	45
2.7. The Quantum Leap from C5ISR to C7ISR Challenge	47
3. The Golden Card of Ukraine	51
3.1. Ukrainian Security-as-a-Service: the New Horizon of Defence	51
3.2. Not Starting From Scratch	55
3.3. “Low-Hanging Fruit” in NO-UA Defence Partnership	57
3.4. From Programs to Partnership	60
Conclusion	61
Addendum. The Battle of Norway. Memories of the Future	63
Intro	63
The Denied War	64
The Trap Snaps Shut	65
The Doomsday	66
Where the Shell Held	69
The Long Grey Water	69

Executive summary

- Through 2025-2026, a growing number of intelligence assessments, including a recent U.S. reassessment in August 2026, converge on a window between late 2026 and 2029 in which Russia may test NATO's Article 5 resolve. This is driven less by Russian readiness than by the closing gap between Moscow's ability to keep its war machine running at full capacity and Europe's still incomplete rearmament. At the same time, almost all major Norwegian modernisation programs mature between 2029 and 2036

- Russia remains Norway's primary and most immediate military threat. But Kongeriket Norge is not a target for Moscow for its own sake. This is its status as a key-holder to European security (energy supply, subsea communications infrastructure, and NATO's principal Atlantic gateway into the Nordic-Baltic theatre) that makes it a primary and imminent object of potential hostilities.

- These specifics define the most probable form of aggression against Norway: it is neither a ground offensive into Finnmark nor a maritime confrontation over Svalbard. Instead, Norway is far more likely to be drawn into a NATO - Russia confrontation in "Battle of Norway" format: a multi-domain contest fought in the air, at sea, on the seabed and in the electromagnetic spectrum, targeting Norwegian offshore and onshore energy infrastructure, subsea cables, and logistics nodes, without Russian forces needing to set foot on Norwegian soil.

- Operationally, the aggression would resemble the Battle of Britain - 1940 rather than Barbarossa - 1941. In a modern setting, this would result in a contest of denial and attrition through mass combined drone-missile deepstrike air offensive, drone-powered autonomous precision strike at the sea and in the littorals, and pervasive cyber, and physical sabotage in all the operational domains including underwater.

- As such a campaign would likely be synchronised for shock effect within a compressed window, NATO's collective decision-making and reinforcement machinery is structurally too slow to prevent the opening blow, even as instruments such as Baltic Sentry and the newly launched Arctic Sentry raise the cost of the succeeding lower-intensity aggression.

- While Norway's own 2026 threat assessments assume this underlying vulnerability picture, they judge that Moscow still prefers to avoid direct war with NATO. Still, given the probability gravity ratio of the threats involved, even with minimum probability, the worst-case scenario leaves no room for complacency given the trajectory of Russian doctrine, capability and risk tolerance.
- The gap concentrates precisely where Russia is most willing and able to exploit it: a near-total absence of ballistic / hypersonic and counter-drone defence in air defence architecture, a naval and coastal sabotage detection architecture still built for warship-on-warship combat rather than mass unmanned threats, a distributed tactical electronic warfare layer that barely exists along with nascent strategic tier, and a ground deterrence model for Finnmark that still assumes manpower Norway does not have and mechanized contest that does not work.
- Norway's capability gaps derive from both chronic lack of attention to Russian military threat since 1990s and the paradigm shift in warfare which makes current force structures optimised for a battlefield that no longer exists in the form it was designed for.
- The change in warfare driven by unmanned and autonomous systems is not an added capability requirement on top of existing force structure. It necessitates a different application architecture: from sensing and command & control to communications and logistics, that existing platforms were not designed for and cannot simply absorb through upgrades.
- On today's complex and progressively "intelligent" battlefield, simply acquiring a drone, robotic system, or artillery platform will be of limited value unless it is embedded within the wider enabling infrastructure of sensors, energy, communications, digital networks, and intellectual capacity.
- This shift necessitates a change in the cooperation model, moving from sporadic transactions to systemic defence industry cooperation and joint capability development.

- Norway's exquisite platforms such as the F-35A fleet, the P-8A Poseidon squadron, the incoming Type 26 frigates and Type 212CD submarines buy real and valuable strategic effects such as air superiority, ASW[1] dominance, deep-water sea denial. None of them, individually or together, is built to survive or economically counter mass, low-cost, attritable asymmetric attack. That is a different capability, and Norway does not yet have it at scale in any domain.

- Almost all major Norwegian modernisation programs mature between 2029 and 2036. This mismatches with the threat window identified as 2027–2029.

- Norway's own assessments already say most of this plainly. The value this report adds is less in identifying the gaps what Oslo has largely done than in showing how they compound across domains, and where strategic partnership with Ukraine can close them faster than the current procurement timeline allows.

- Ukraine's offer to Norway is an integrated, continuously adapting system spanning doctrine, training pipelines, battle management, electronic warfare, unmanned combat operations, ISR, sea denial, military medicine and industrial cooperation in exactly the "missing piece" of its total defence – C-UAS, littoral defence, unmanned naval warfare, and AI-powered automation to reduce critical manpower deficit.

- A real institutional track already exists through Brave- Norway, the April 2026 Oslo defence declaration, Kongsberg's Kyiv office and its investment in Ukrainian-designed naval drone production. It is time to take the next step.

- The line of cooperation with highest value and fast payoff is counter-drone defence built around the Norwegian Heimevernet. This is already Norway's own plan; what it may not yet have is a realistic sense of the scale of distributed systems and trained people – operators, technicians and analysts keeping the entire kill-web running – that a genuine nationwide shield requires. This is the area where Ukrainian involvement is close to non-substitutable, with a set of doctrinal and technical solutions Norway needs to make the systems work.

- Most capability gaps identified in this report trace back to the structural constraint of Norway's vast geography combined with its small population – a dilemma that cannot be reconciled by adding more people. The only realistic path to adequate coverage is deep automation, remote operation and AI-assisted fusion that let a limited number of skilled operators run large distributed sensor-and-effector networks – and this is precisely where Ukrainian combat experience is most directly transferable.
- Relying solely on Brussels is not a strategy. EDDI, the EU's flagship counterdrone initiative, targets full operational capability by the end of 2027, which is an unrealistic horizon. A tighter, faster bilateral or minilateral track, with Ukraine on board, can deliver a working baseline well before the threat materializes at its full potency. There is no need to wait until Norway finds itself in the position that countries in the Near East face in 2026, when the same track would still have to be installed, only under fire.

[1]Anti-surface warfare, a branch of naval warfare that focuses on attacking, suppressing, or destroying an adversary's surface ships and craft.

Preface

By mid-2026, Russia's war against Ukraine continues without any credible prospect of termination, with sporadic rounds of peace negotiations amounting to little more than diplomatic theatre without credible progress. It is being settled into a form of strategic stalemate: neither side is positioned to force a decisive breakthrough this year, as tactical gains on the ground continue to offset one another. The war is mutating into an essentially new phase, better characterised as a "war of cities", waged primarily against rear-area strategic infrastructure and economic assets, aimed less at expanding territorial control than at breaking political will and economic capacity through sustained deep strike pressure. Russia is scaling its lethal capacity both in sheer numbers, and in technical and operational quality: within a year horizon serious breakthroughs are expected in satellite communications (a "Starlink analogue") and in lethal autonomy, specifically in missiles, unmanned naval and aerial systems, electronic warfare, swarming, C-UAS, and AI-driven battlefield management. Some of this is already partially visible on the front line in Ukraine.

On the surface, this appears predominantly a Ukrainian problem. In substance, it is a NATO challenge as well – and a Norwegian one in particular.

For that reason, this paper aims to figure out what the current trajectory in the Russian military capability and intent, set against the broader panorama of revolutionary transformation in warfare, means for Norway. Two other questions discovered in reasonable detail, are whether Oslo is ready to address the challenges, and how a structured partnership with Ukraine can help close the gaps identified.

Norway, despite the security guarantees of NATO membership, arguably faces a threat environment no less serious than Ukraine's own, albeit one of lower actualization probability. Russia continues to "rattle its sabre" along NATO's northeastern flank, and while its economy erodes gradually, its breaking can be expected over a horizon of years, not months (given Ukraine manages to sustain pressure intensity and tempo). Yet Moscow's military capacity is trending in the opposite direction: growing more capable with respect to modern warfare requirements, and more able to inflict damage on NATO states in any future confrontation in the High North. As the Russian playwright Anton Chekhov famously put it: "If you say in the first act that there is a rifle hanging on the wall, in the second or third act it absolutely must go off."

In this respect, Norway's position combines real strength with real vulnerability. It understands the Russian threat with unusual clarity, holds cutting-edge capabilities in select niche domains, including space technologies, missiles and programmed munitions, digital communications, and autonomous underwater systems (though the latter still predominantly oriented toward civilian applications at scale).

It also commands financial resources ample and flexible enough to be redirected toward defence at scale whenever necessary.



At the same time, those strengths are not tailored to compensate for a huge structural imbalance between the geography Norway is responsible for defending and the quantitative and qualitative limits of what it can currently field, particularly in view of the dispersed, decentralized, omnipresent nature of new military threats. And even aside from this numerical gap, Norway (as any NATO member including the U.S. though[2]) also has no operational experience with modern algorithmically-driven drone warfare. Its major combat assets and critical land / maritime infrastructure remain effectively undefended against mass unmanned aerial, surface, and underwater threats. Its C2[3] architecture is undergoing transformation which is not expected to reach operational readiness before 2030. The Heimevernet, Norway's Home Guard, is assigned for the nation-wide counterdrone defence but hardly realizes either the scope of the doctrinal challenges it is to face with zero experience in this domain, nor the full technical magnitude of the problem stemming from its limited numbers.

Ukraine, by contrast, is the only country in the free world to have built a proven operational architecture for next-generation unmanned warfare, backed by a mature and hyperadaptive military innovation ecosystem. Its accumulated expertise sits almost precisely over Norway's gaps: defence against unmanned sabotage at sea, along coastlines, and inland; air defence against combined mass attacks, particularly in the counterdrone segment;

[2] NATO's Combined Resolve-2026 drills stand as the most recent clear testament to this assessment.

[3] Command-and-control.

operational blueprints and technical solutions to optimize small dispersed threat monitoring and neutralisation over huge geographical areas of responsibility with scarce personnel as a constant; and, more broadly, a transition of the entire military capability generation and employment framework toward an AI-native robotic warfare architecture.

Two clarifications are warranted before proceeding.

First, this paper does not claim that near-term Russian aggression against NATO in its northeastern flank, or against Norway specifically, is to materialize for sure. That depends on numerous factors well beyond the scope of any single study. What is not in question is that Russia is actively mastering the inventory and preconditions for such an enterprise, across political-diplomatic pressure and military build-up alike.

The clear historic record of its military politics patterns shows it would very plausibly exploit a favourable window of opportunity (e.g. a European recession, a military crisis around Taiwan etc) should one arise.

Notably, Russia has prioritised precisely those capabilities against which NATO states currently have the fewest answers. It expands ballistic missile production, permanently refines a full-cycle deepstrike drone complex spanning R&D, component supply chains, and operational procedures, trains hundreds of thousands of its children and adolescents as drone operators and engineers, considerably expands number and staffing of elite special units for sabotage and sub-threshold warfare – just few examples relevant for Norway, among many. In any aggression scenario, Russia would almost certainly try to impose the conflict style least comfortable for NATO, politically and militarily.

Second, the analysis deliberately foregrounds a worst-case scenario. This is not intended to alarm, but reflects a basic principle of risk management: where the consequences of a scenario are potentially catastrophic, even the lowest probability of occurrence warrants serious preparation.

To sum up: the threat is real, even if its probability of materialising remains open to debate; the capability gaps are real and not seriously contestable by Norway itself; and the premium opportunity to close those gaps fast through a strategic partnership with Ukraine is real too, but available only within a limited window of time – before a crisis hits.



1. The Threat Environment

Russia and the "Battle of Norway"

Norwegian security is embedded in the wider architecture of European defence under the NATO umbrella. Within this paradigm, Russia is its dominant and most immediate military threat in the near-to-medium term. This is a conclusion of Norway's own Intelligence Service. In the 2026 Report it admits that Russia has entered into a lasting confrontation with the West in which Norway is explicitly counted among Moscow's adversaries[4].

This doesn't mean that Russia is the only long-term driver of the threat environment for Norway. The character of warfare being pioneered in Ukraine, based on cheap, attritable, mass produced unmanned systems, enabled by a digital and communication infrastructure and built upon COTS[5] and open-source software; makes a perfect inventory for asymmetric and hybrid warfare, and is replicable by virtually any state or non-state actor. This creates a universal longer-horizon risk from non-state criminal and terrorist actors.

Yet for the immediate outlook of the next 2-5 years, Russia is the actor with both the capability and a plausible intent to test NATO militarily, with Norway sitting right inside the geography that intent would most efficiently exploit.

1.1. Strategic Vulnerability Window

Russia's four and a half years of Russia's war against Ukraine have not delivered the swift and prestigious victory the invasion was designed to produce.

By 2026, this became explicitly evident to the broader Russian public, as the enormous human toll Moscow pays for making only marginal territorial gains has reached its peak – roughly 1,100–1,400 men per day[6]. Russian losses since February 2022 are assessed as reaching 1.1 million killed, wounded, missing or captured[7].

Along with this, Ukrainian long-range strikes have begun measurably degrading the economic base of the Russian war machine[8].

As a regime that has tied its domestic legitimacy to martial success, and that cannot be seen to have "lost" against an adversary constantly stigmatized by its propaganda as inferior, the Kremlin leadership may need to engineer a cheaper, faster victory elsewhere for a demonstration Russia still dictates the terms of European security.

This is exactly the logic now driving a marked shift in Western intelligence assessments. As of early August 2026, the U.S. intelligence has revised their view that Moscow would avoid provoking NATO while tied down in Ukraine; the new assessment holds that Putin could attempt a limited test of NATO's resolve ranging from a major cyberattack to a small-scale land incursion on the alliance's eastern flank, at any point between autumn 2026 and 2029, with the probability of the worst scenario assessed as low but rising[9]. This aligns with a broader perspective: Harvard's Belfer Center, aggregating public forecasts across Western services, finds 2027–2028 to be the most frequently cited years for Russian intent, while 2030 is the most common year cited for full Russian capability[10].

More important than assessments are facts that dictate clear logic of action. First of all, Moscow has its own pressing time window to sustain opening "a second front" against NATO, and it may close well before 2030. This window is framed by:

Economy

Russia's sovereign wealth fund, a traditional buffer against wartime/financial volatility, has collapsed from 6.5 to 1.8 %[11]. Most researchers converge on that Russia can sustain its war machine fully active for 2-4 years maximum, then the cost becomes unsustainable without dramatic GDP reallocation or demilitarization.

Military Posture

NATO's Readiness 2030 initiative explicitly targets this year as a capability delivery inflection point[12]. Thereafter, a "small victorious war" against NATO becomes progressively less likely to remain either small or victorious.

Demography

Russia already has big problems to replenish manpower losses under present attrition tempo in Ukraine[13]. Even anticipated mobilization of 300,000-500,000 personnel in autumn 2026 (aside from political risks for Putin) alleviates the problem for 8-13 months (given current losses rates preserve), after which the problem gets much graver. The Kremlin may try to make a "cobra strike" against NATO within that year-size window until the manpool sufficient to sustain its war machine starts shrinking rapidly.

[4] Norwegian Intelligence Service (Etterretningstjenesten), "Focus 2026: Assessment of Current Security Challenges," February 6, 2026, Introduction, etterretningstjenesten.no/publikasjoner/focus/focus2026_contents
[5] Commercials-off-the-shelf, dual-use components readily available on open markets.
[6] As of mid-August 2026.
[7] UK Ministry of Defence, "Evidence Shows Russia Continues to Incur Catastrophic Losses for Minimal Gains in an Unsustainable War," UK Statement to the OSCE, April 29, 2026, gov.uk/government/speeches/evidence-shows-russia-continues-to-incur-catastrophic-losses-for-minimal-gains-in-an-unsustainable-war-uk-statement-to-the-osce.
[8] As one example among many, since March 2026, Ukrainian forces have targeted 22 Russian oil refineries, disrupting approximately 40 percent of refining capacity
[9] Gordon Lubold and Warren P. Strobel, "U.S. Intelligence Warns Russia Could Test NATO Resolve with Limited Incursion," The Wall Street Journal, August 5, 2026, wsj.com/world/europe/u-s-intel-finds-putin-could-test-natos-resolve-with-limited-incursion-e3b02e2c
[10] Belfer Center for Science and International Affairs, "Russian Threats to NATO's Eastern Flank: Scenarios, Strategy, and Policy for European Security," Harvard Kennedy School, February 2026, belfercenter.org/research-analysis/russia-nato-baltics-scenarios-europe-security
[11] Becker, Torbjörn; Egorov, Konstantin; García-Herrero, Alicia; Klein, Matthew C.; Korhonen, Iikka; Ribakova, Elina; Risinger, Lucas; Schularick, Moritz. Endgame: The State of the Russian Economy (Kiel Report No. 9). Kiel Institute for the World Economy, June 2026. https://www.kielinstitut.de/ publications/endgame-the-state-of-the-russian-economy-19855/
[12] See North Atlantic Treaty Organization (NATO), "Deterrence and Defence," NATO Topic, last updated June 25, 2026, https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence
[13] Congressional Research Service, Russian Military Performance and Outlook, CRS Product IF12606 (April 2026), https://www.congress.gov/crs-product/IF12606

Second, and most troublingly for the alliance and Norway in particular, "Epic Fury" operation exposed the deep fragility of NATO's military capabilities (through the U.S. as their principal representative) in terms of endurance and tolerance to rising stakes. More tangibly, it exposed shortages of stockpiles of certain precision munitions considered the foundation of the allied defence capacity, primarily long-range precision strike missiles and surface-to-air missile short-range air defence interceptors[14]. A few weeks of the recent U.S. operation in the Middle East depleted these stocks far more heavily than four years of assistance to Ukraine. This has drastically narrowed the West's margin for a powerful and decisive response in the perception of the entire authoritarian axis.

Finally, Russia operates a clear doctrinal logic that Western discourse frequently misreads. Russian military theory treats "hybrid warfare" not as a distinct type of hostilities but rather as a specific, advanced stage of escalation within the holistic warfare spectrum, the point at which use of a limited conventional force is synchronised with sub-threshold warfare – non-conventional pressure of a broad spectrum. Under this framework, many years of propaganda, economic intrusion and political interference efforts in Europe were neither hybrid nor sub-threshold warfare, but rather an essentially grey-zone investment strategy to consolidate Russian influence in Europe. However, the pattern explicitly changed over the past two to three years: sabotage of critical infrastructure, repeated unexplained drone incursions, direct airspace violations by combat aircraft plausibly signals a shift to a distinctly antagonistic approach of hybrid warfare. It is no longer aimed at gradually shaping European politics, but at actively degrading European governance and defence readiness to prepare the operational environment for a probable military aggression. Notably, Russia's own 2023 Foreign Policy Concept explicitly frames the "collective West" as having already launched a "hybrid war of a new type" against Russia[15]. This is actually a formal admission, inverted in a typical Russian manner, that the Kremlin already considers itself in a state of overt confrontation with NATO and the EU.

The hypothesis for Oslo is the following: the shaping phase is already under way, and regarding Norway, rather than ground troop concentrations, it would prioritize massed air raids and similarly massed sabotage attempts, now substantially amplified by its enhanced drone, electromagnetic, and direct sabotage capabilities.



[14] Zachary Cohen, Jim Sciutto, and Haley Britzky, "Nearly 80% of Interceptors for a Key Missile defence System Depleted, Sources Say," CNN, August 4, 2026, https://www.cnn.com/2026/08/04/politics/us-iran-key-missile-interceptors-low

[15] Ministry of Foreign Affairs of the Russian Federation, "The Concept of the Foreign Policy of the Russian Federation," March 31, 2023, https://mid.ru/en/foreign_policy/fundamental_documents/1860586/

1.2. The “Battle of Britain” Remastered in the Drone Era

Russia’s strategic calculus regarding a NATO confrontation could fluctuate in detail, but presumably follows some general political logic. At minimum, Moscow would seek to force the Alliance to recognize Ukraine as part of Russia’s sphere of interest and to halt all military assistance to Kyiv. At maximum, it would aim to deliver a political shock the Alliance could not survive, by presenting it with a military dilemma that cannot be resolved for political reasons — yet whose non-resolution would negate NATO’s core reason for existence.

Such political logic in turn can have different operational manifestations. This can be a fully remote operation – or an escalating set of such operations based on synchronized combined sabotage acts and kinetic deep strikes of different magnitude, designed to inflict political and economic pain without seizing territory.

In August 2026, for instance, Lithuania’s military intelligence warned that Russia is actively considering false-flag drone operations using captured Ukrainian unmanned systems to trigger NATO crisis without direct attribution[16].

Another option includes a territorial gambit with a ground component, and can take the form of a limited seizure of territory combined with sustained remote pressure to create a negotiating asset that Russia can firmly hold. Aside from logic, this option aligns with Putin’s emotional fixation on imperial restoration and self-perception as “Rus’ lands gatherer”. Last but not least, this second option is more costly, more risky, and more dangerous to NATO: as recent military incidents show (including the “Epic Fury” in Iran), NATO member states became incredibly averse to place their “boots on the ground” anywhere outside their own national territory.

In the latter case, evidence suggests Baltic states – not Norway – remain Russia’s preferred and most strategically efficient axis for a “quick win” against the Alliance – a theatre offering the most rapid, decisive, and humiliating effect for NATO cohesion at the lowest Russian cost. Moreover, Russia considers it has a legitimate ground for this, as the Baltics lie within its sphere of historical influence and strategic interest. Crucially, it recently moved from rhetoric to making a formal legal pretext for intervention: in May 2026, President Putin signed a law[17] authorizing the deployment of Russian armed forces abroad for the purpose of protecting Russian citizens from detention, arrest, or armed aggression.



[16] Milda Seputyte, “Lithuania Warns Russia Weighs False-Flag Drone Attack on Baltic Infrastructure,” Bloomberg, https://www.bloomberg.com/news/articles/lithuania-warns-russia-weighs-false-flag-drone- attack-on-baltic-infrastructure

[17] “Putin Signs Law on Use of Army to Aid Russians Abroad,” Bloomberg, May 25, 2026, https://www.bloomberg.com/news/articles/2026-05-25/putin-signs-law-on-use-of-army-to-aid-russians-detained-abroad

In such circumstances, as we agree the likelihood of a major land offensive on Norwegian territory is low, a fair question may arise:

Why should Norway expect to be drawn into NATO's limited war with Russia at all, beyond the role of a remote provider of ISR, area denial, precision strike and logitics capabilities to allies?

This is because Norway's centrality to Euro-Atlantic security rests not on its territory but on what runs through and beneath its waters.

As of 2026, Norway is the European single largest supplier of pipeline gas: around 54% of the EU pipeline gas imports in 2025, 55% in the first quarter of 2026[18]. Combining pipeline and LNG, it supplies roughly 30% of the EU's total gas imports[19]. This position is beginning to shift as U.S. LNG expands its European market share, but Norwegian pipeline supply remains structurally embedded, non-substitutable in the short term, and irreplaceable for continental heating and industrial demand through at least the remainder of this decade. Norway is also host to, or transited by, some of the most sensitive subsea data infrastructure in the Euro-Atlantic space, including the cable systems serving the Svalbard satellite ground station – one of only two facilities globally capable of full-orbit communication with polar-orbiting satellites. A Norwegian naval researcher called Norwegian gas pipelines "probably the highest-value [sabotage] target in Europe"[20]. Russian military affiliated commentaries are far more explicit in this respect.

> NATO's Achilles' heel isn't its airfields, HQs, aircraft carriers, or frigates, but rather its energy sector and underwater infrastructure. 95% of internet traffic, power and telecommunication cables, as well as oil and gas pipelines, all rest at shallow depths on the seabed of the Baltic and North Seas... Just three oil refineries serve all of Northern Europe (Sweden, Norway, and Finland), while the entire Baltic region relies on a single one.
>
> Russian military think-tank "Ramzai & his team". 26 April 2026

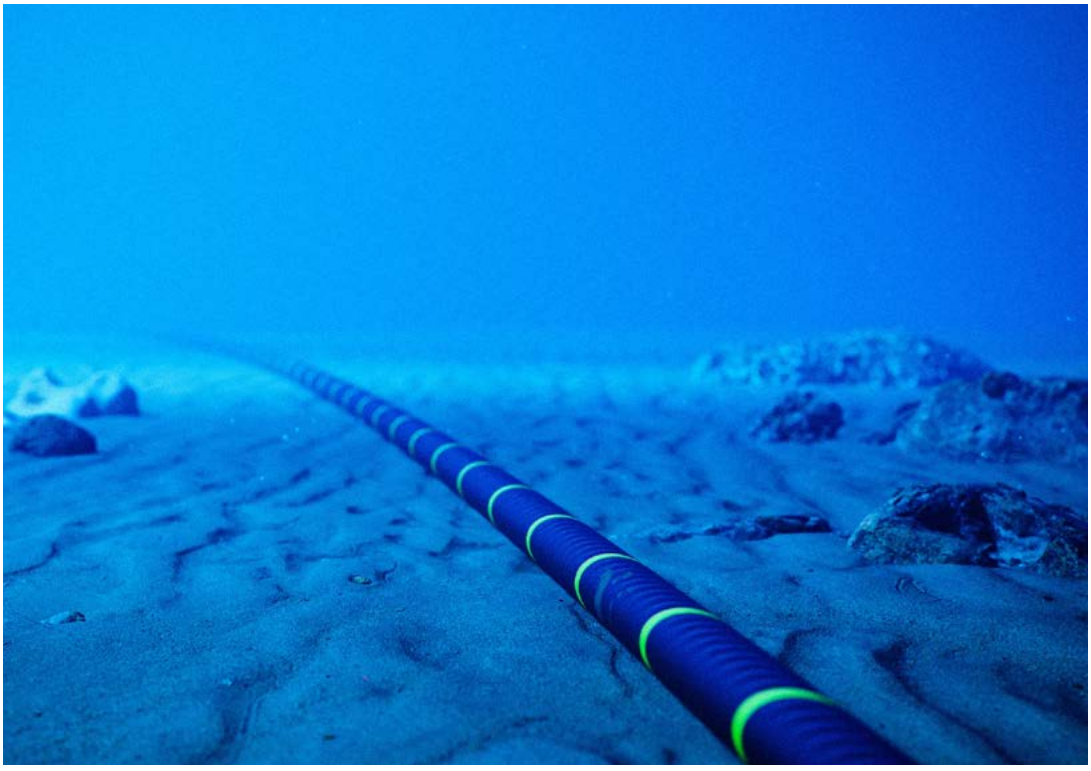
[18] IEEFA, EU Gas Flows Tracker, ieefa.org/eu-gas-flows-tracker

[19] Council of the European Union, Where Does the EU's Gas Come From?, https://www.consilium.europa. eu/en/infographics/where-does-the-eu-s-gas-come-from/

[20] Ståle Ulriksen, Senior Instructor, Norwegian Naval Academy (Sjøkrigsskolen), quoted in VOA News, "Fears Over Russian Threat to Norway's Energy Infrastructure," October 23, 2022, https://www.voanews.com/a/fears-over-russian-threat-to-norway-s-energy-infrastructure/6801621.html

In addition to that, through 2025-2026 Norway has further consolidated its role as NATO principal Atlantic reception and reinforcement gateway into the Nordic-Baltic theater. Along with air bases and ports, this includes stockpiling of allied equipment. The long-standing U.S. Marine Corps Prepositioning Program - Norway was validated at scale during exercise Cold Response ‘26, where U.S. and Norwegian logistics commands stood up their first fully integrated joint headquarters and tested logistical operational procedures, including a cross-border logistics convoy running through Sweden into Finland[21]. Norway’s bilateral defence pact with France (the “Narvik Agreement”) in May 2026 further institutionalises this reinforcement role, and NATO’s own Arctic Sentry initiative launched in February 2026 under Joint Force Command Norfolk, modelled on the Baltic Sentry mission, now maintains a constant enhanced readiness across the High North, from Greenland to northern Finland[22].

Together, this is why Norway would inevitably be pulled into a Baltic-centered NATO–Russia war, should one materialize. Even setting aside NATO obligations, Norway would be targeted whether its troops are in or not, because it is a “keyholder” to European (and Allied) sustainability. Disabling or credibly threatening Norwegian energy exports and subsea infrastructure, and disrupting the logistical architecture that would otherwise allow allied reinforcement north and east, delivers strategic effect against NATO without requiring Russia to fight (and even threaten) a land campaign it can hardly resource or a conventional naval campaign it can hardly win.



[21] Norwegian Armed Forces, Cold Response 2026, (Mar. 25, 2026) forsvaret.no/ en/exercises-and-operations/exercises/cr26

[22] NATO Joint Force Command Norfolk, “Arctic Sentry to Enhance NATO’s Presence in the Arctic and High North,” (February 12, 2026). jfcnorfolk.nato.int/activity/nato-jfc-norfolk-leads-arctic-sentry-to- bolster-nato-posture-in-the-arctic-and-high-north.aspx

Information Sheet

Norwegian infrastructure of high interest to Russian attack.

The following list is not exhaustive; it is not intended to serve as a targeting resource for hostile actors. It is to illustrate the depth of vulnerability in the new warfare realities having smashed borders between frontline and rear.

Category	Key Assets	Vulnerability Profile
Energy Export Infrastructure		
Gas processing & export terminals	Kårstø (Rogaland), Kollsnes (Øygarden), Nyhamna (Aukra)	Handle the majority of Norwegian gas exports to Europe. Kårstø is Europe's largest NGL export facility
Crude oil terminals and LNG plants	Sture, Mongstad, Melkøya (Hammerfest LNG)	Melkøya is the only large LNG facility and lies closest to Russia (in Barents Sea)
Major export pipelines	Europipe I & II, Franpipe, Langeled, Zeepipe, Statpipe, Norpipe, Polarled	8,800 km of subsea pipelines linking the Norwegian Continental Shelf to the UK and continental Europe.
Offshore platforms & subsea systems	Troll, Ormen Lange, Åsgard, Snøhvit, Johan Castberg (the list in not exhaustive)	Platforms and subsea templates are vulnerable to long-range strike, drones, or special forces' sabotage.
Subsea Infrastructure		
Gas pipelines	8,800+ km network	Vulnerable to physical sabotage (anchors, explosives, underwater systems)
Telecom / fibre optic cables	Svalbard cables, North Sea cables (e.g. NO-UK, Havfrue), Arctic routes	Repeated mapping by Russian vessels; previous incidents already in place (Svalbard cable damage)
Power cables	Interconnectors and domestic subsea links	Lower priority than gas/ telecom but still relevant
Logistical Architecture for Allied Reinforcement		
Ports	Narvik, Trondheim area, Bodø, Tromsø, Haaknsvern	Primary Atlantic entry points for reinforcements flowing north and east (Sweden, Finland, Baltic nations)
Air bases	Evenes (F-35 Quick Reaction Alert & U.S. joint area), Ørland (main F-35 base), Bardufoss, Andøya, Rygge, Sola	Critical for air reinforcement, rapid reaction, and logistics airlift. Evenes and Ørland are especially high-value

Prepositioning sites	MCPP-N caves (primarily Trøndelag region: Frigaard, Tromsdal, Bjugn and others)	U.S. Marine Corps equipment stored there. It directly supports rapid force generation.
Cross-border logistics corridors	E6, E10, Ofotbanen (Narvik–Kiruna rail), and similar road/rail links into Sweden and Finland	Susceptible to 24/7 middlestrike operations with autonomous drones akin to current "logistical lockdown" in Crimea
Space Ground Infrastructure		
Commercial polar ground stations	SvalSat (Platåberget mount, near Longyear city)	World's largest commercial satellite ground station, critical for Earth observation, maritime surveillance. Along with soft physical protection on exposed plateau, it has high cyber vulnerability. Russia has publicly flagged it as dual-use.
	Tromsø Network Operations Centre (TNOC)	Central 24/7 control hub for the entire KSAT global network, including remote operation of SvalSat, single point of failure for commanding and routing polar satellite data.
Military ground stations	Defence Satellite Station Eggemoen (Ringerike), Andøya ground statio	The former is Norwegian Armed Forces' primary military satellite communications station, the latter is critical for missile warning, tracking and situational awareness
Spaceports	Andøya Spaceport (Andøya island, Vesterålen archipelago)	Europe's first operational orbital launch site for small satellites into polar and sun-synchronous orbits. Limited local protection contrasts to high value for both commercial and military space access.
Military ground stations	Kongsberg Defence & Aerospace (KDA) sites, Nammo Raufoss industrial park	Primary Norwegian production capacity for naval strike missiles, joint strike missiles, NASAMS components, remote weapon stations, medium and large calibre ammunition

Archetypally, the potential Russian offensive against Norway is better understood through the lens of the Battle of Britain which was a confrontation between a continental power and a nation whose key military capabilities are concentrated rather in maritime and air domain. In such a scheme, neither side can hence decisively enter the other's domain of strength – Russia cannot directly contest Norwegian and allied air and undersea dominance, while Norway and NATO together cannot cheaply project decisive force on the Russian ground. What plays out instead, as in 1940, but in a new technological setting, is an extended campaign of strategic-to-tactical precision strike, pervasive drone-powered sabotage, littoral blockade pressure and electromagnetic contest. This is the reign of denial and attrition – denial at sea and airborne attrition against infrastructure on the land and at sea, with minimum to no ground manoeuvre and territorial conquest. The pattern has been visible, in lower-intensity form, for years. Since 2022, Norwegian offshore and onshore energy sites faced growing unidentified drone activity, alongside parallel undersea cable incidents since 2021. In April 2026, a joint UK-Norwegian operation disrupted a GUGI-coordinated deployment of an Akula-class attack submarine and two deep-sea reconnaissance submarines near their waters[23]. Norway's 2026 intelligence assessment distinguishes between shallow-water infrastructure—exposed to unsophisticated sabotage using anchors, trawls or small vessels—and deep-water infrastructure, precisely the target GUGI's submarines exist to reach[24]. Both channels are already live.

Russia would presumably use a different deep-strike approach to soft and hardened targets to maximize effectiveness in derailing Norway's infrastructural resilience.

Target Type	Example	Engagement approach
Soft targets and soft elements of hardened targets with critical value	Combat and support military aircraft and vessels in open sites, fuel trucks, bowsers, above-ground fuel storages, ground-based air defence radars, above-ground pipeline manifold areas, high-capacity power transformers, outdoor switchyards, transmission substations, soft satellite and space ground infrastructure, railway signalling systems, key switches, locomotives, critical telecom masts, oil production support vessels	Mesh-networked remotely controlled and autonomous small sabotage drones and swams
Hardened targets with critical value	Target Type Example Engagement approach Soft targets and soft elements of hardened targets with critical value Combat and support military aircraft and vessels in open sites, fuel trucks, bowsers, above-ground fuel storages, ground-based air defence radars, above-ground pipeline manifold areas, high-capacity power transformers, outdoor switchyards, transmission substations, soft satellite and space ground infrastructure, railway signalling systems, key switches, locomotives, critical telecom masts, oil production support vessels Mesh- networked remotely controlled and autonomous small sabotage drones and swarms Hardened targets with critical value Offshore oil and gas production complexes (Troll, Oseberg, Johan Sverdrup, Heidrun, Statfjord, Gullfaks), major gas processing & export terminals, critical high-voltage transformers & major substations, Nammo and Kongsberg defence industrial facilities, military airbases and sites, port infrastructure (primarily those critical for allied seaborne reinforcement in Narvik, Trondheim, Bergen, and Stavanger), satellite and space ground stations, onshore facilities supporting transatlantic cables Cruise and ballistic missiles combined with Shahed-type drone mass.	Cruise and ballistic missiles combined with Shahed-type drone mass

[23] British Ministry of Defence & Norwegian Ministry of Defence, "Joint Statement on Russian Submarine Activity in the Atlantic," April 9, 2026, norway.no/en/missions/osce/norway-and-the-osce/ statements/norwegian-statements-2026/ joint-statement-on-russian-submarine-activity-in-the-atlantic/

[24] Etterretningstjenesten (Norwegian Intelligence Service), Focus 2026 – The Intelligence Service's Assessment of Current Security Challenges, Feb. 2026, etterretningstjenesten.no/ publikasjoner/fokus/focus-in-english/

1.3. Russian War Machine: Bigger Problem Now Than in 2022

Four and a half years into the war, Russia has rebuilt, modernised, and expanded in the most meaningful domains of a war machine, including industrial footing that total European production does not match. The precise figures move month to month and are contested even between Ukrainian intelligence services, but the order of magnitude, and the trend, are clear.

Given that the aggression scenario of greatest relevance to Norway, the following suite of lethal systems offers a useful illustration of a trend.

Category	Approximate 2026 output	Trend by August 2026
Iskander-M ballistic missiles (9M723)	50-70 / month	65 actual vs 60 planned in July
Repurposed S-300/S-400 (RM-48U) missile	40 / month	According to the plan
Zircon (3M22) hypersonic missile	30 / year	33 for the last 7 months
Oniks (P-800) supersonic missile	8-9 / month (compared to 5 / month as of April)	60 for the last 7 months
3M14 “Kalibr” cruise missile	25-30 / month	29 actual vs 26 planned in July[25]
Kh-101 cruise missile	40–70 / month	87 actual vs 72 planned in July
Kh-35 cruise missile	20 / month	July plan outperformed 200%
Long-range attack, ISR and decoy drones (Geran / Gerbera family)	140–400+ per day as of early 2026, industry plans 110,000 units for the year	11,000 for August, refocusing toward jet-powered Geran-3, 4, 4 “Seeker” (with remote control)
Radio-controlled strike tactical FPV drones	450,000 / month (30-fold increase since 2023)	11,000 for August, refocusing toward jet-powered Geran-3, 4, 4 “Seeker” (with remote control)
Fiber-optic (EW-immune) FPV	No direct output figures, but Russia consumed 10.5% of global optical fiber output in 2025 only	11,000 for August, refocusing toward jet-powered Geran-3, 4, 4 “Seeker” (with remote control)
Naval strike drones (USV)	No serial production yet (prototype/small-batch stage)	Rapid maturation, industrial capacity for scaling built, first confirmed combat use a year ago (August 2025)

Note. Figures are drawn from Ukrainian military intelligence assessments.

[25] Most newly produced Kalibr missiles are currently not used for strikes against Ukraine but allocated to equipping new surface ships and submarines, as Ukrainian air defences currently intercept nearly 100% of this type of missiles.

Therefore, even a degraded Russian war economy currently sustains a material base for thousands daily drone-powered sabotage ops and monthly long-range drone and missile output production to provide aggregate daily strike capacity at roughly 310–380 munitions – and even further increases this rate. This comfortably exceeds anything the European defence-industrial base can currently generate for collective defence, independent of what is expended in Ukraine.

Moreover, the quantitative dimension is only half the picture, and its impressively high figures may hide a more important qualitative dimension, a systematic scaling of effectiveness of Russia's weapons based on combat adaptation.

The most perilous trend is combat autonomy it successfully develops and deploys backed by solid funding and combat data datasets it possesses just as Ukraine[26].

For example, Moscow develops the S-71M "Monokhrom" cruise missile for the Su-57, capable of autonomously reaching a search area, selecting a target by priority, and striking without operator involvement against both stationary and moving objects. AI trajectory is clearly visible in "Italmas" UAV and some "Geran" family modifications (Geran-4 "Seeker" and SEAD version of Geran-2 in particular), where the operator's role is limited to initial target identification, after which the onboard computer flies the terminal leg of the route itself. At the tactical level, Russia effectively tested and now actively scales deployment of an autonomous version of a cheap fixed-wing "Molniya" UAV completely immune to radio-frequency detection and EW suppression. The Iskander-M received active in-flight maneuvering to complicate interception even for the Patriot PAC-3 system.

[26] CSIS, Kate Bondar, How Russia Is Building a Sovereign Drone Ecosystem for AI-Driven Autonomy (April 13, 2026), csis.org /analysis/how-russia-building-sovereign-drone-ecosystem-ai-driven -autonomy

This material capacity is matched by force restructuring on Russia's north-western flank. The new 44th Army Corps of the Leningrad Military District (LMD), headquartered at a reactivated Soviet-era garrison at Petrozavodsk in the Republic of Karelia, has been under active construction since late 2025, with Russian officials confirming the project in May 2026; the corps is projected to reach 15,000–16,000 personnel. Part of a longer-term ambition, assessed by Finnish military intelligence as realistically a 2030s prospect, is to raise total Leningrad MD troop levels facing Finland and Norway from roughly 30,000 to as much as 80,000. Progress remains slow and resource-constrained by the continuing drain of Russia's war against Ukraine. That is the reason a near-term ground threat to Finnmark should not be prioritized in the near term, yet it cannot be fully discounted either.

However, the LMD's newly formed Iskander-M brigade, confirmed operational in Karelia and Murmansk regions[27], represents the ground-based ballistic threat to Norwegian territory from this direction. Beside that, K-300P "Bastion-P" complexes deployed on the Rybachy Peninsula – fewer than 100 km from Norway's Vardø radars, are prepared to launch supersonic Oniks anti-ship missiles, with launch positions geolocated just 77 km from the Norwegian border[28].

At sea, the Northern Fleet based on the Kola Peninsula, a short flight from Norwegian territory, retains its function as the bedrock of Russian strategic deterrence and is the one component of Russian military power that has continued to modernise steadily throughout Russia's war against Ukraine. Three Severodvinsk-class (Yasen-M) multirole submarines and three Admiral Gorshkov-class frigates are already deployed, and by the end of 2026, the modernised Admiral Nakhimov battlecruiser is expected[29]. This force maintains operational reach of Norway through Kalibr subsurface cruise missiles and Zircon hypersonic missiles.

A further modernised Akula-class attack submarine and six Kalibr-armed Kilo-class conventional submarines are expected in the coming years. Most significantly for this assessment, the Northern Fleet hosts Russia's Main Directorate for Deep-Sea Research (GUGI) – a special sabotage unit under the General Staff, whose specialised submarines, capable of operating against critical undersea infrastructure at extreme depth, are based exclusively on the Kola Peninsula and therefore on Norway's doorstep. They constitute presumably Russia's most asymmetric threat vector against Norwegian critical infrastructure.

The air component operates Tu-22M3 bombers from Olenya carrying Kh-32 cruise missiles and Kinzhal hypersonic air-launched systems with a 2,000 km range that can reach Norwegian military airfields within minutes of launch (most of it currently intensely engaged against Ukraine, but using Kinzhals is minimized), as well as Su-24M/Su-34 strike aircraft from Monchegorsk armed with Kh-35U anti-ship missiles. Coastal air defence consists of S-400/S-300 layered systems, Pantsir-SA and Tor-M2DT point defence, and Bastion-P coastal batteries.

[27] Yle News. "Russia sets up missile brigade in Karelia in 'adequate response' to NATO expansion," April 22, 2024 yle.fi/a/74-20084963

[28] [2] The Barents Observer. "Russia deploys missile system 70 km from Norway's Vardø radar," Aug. 7, 2019. https://www.thebarentsobserver.com/security/russia-deploys-missile-system-70-km-from-norways- vardo-radar/158070

[29] Army Recognition, "Russian nuclear battlecruiser Admiral Nakhimov enters final sea trials to challenge US in the Arctic," (Jun. 6, 2026). https://www.armyrecognition.com/news/navy-news/2026/admiral- nakhimov-sea-trials-russian-nuclear-battlecruiser

What can Norway set against this?

Overall, its Royal Navy and Air Force, especially if backed by its allies, can in theory deny most of the Russian aircraft and frigates within their missiles launch radius, effectively counter surface combatants and Kilo-class submarines at periscope depth (and not that easily – quite Yasen-M submarines). GUGI sabotage assets and unattributed small drone swarms deployed from the shadow fleet require much more nuanced intelligence, surveillance and denial response, especially while operating in the gray zone between peace and war.

A true challenge (especially given its scale and Moscow capacity to sustain it) are mobile Iskander and Bastion launchers highly resistant to targeting due to their shoot-and-scoot deployment profile. Yet fundamentally, the dense air defence umbrella around the Kola Peninsula creates a suppression requirement that could be a challenge for Oslo to overcome. Unlike the Baltic theatre, where NATO force density more equally distributes this burden, the northern axis presents a more operationally demanding problem.

NATO has more member states around the Baltic (Sweden, Finland, the Baltics) contributing radars, airfields, and SEAD-capable platforms, so no single country's assets have to carry the suppression job alone. Around Kola, Norway remains the only axis that actually reaches the target set with acceptable risk (Finland borders the problem but not the target set), which makes it rely here actually on its own.





1.4. Framing the Threat for Norway: Low-Probability Scenarios

Public and even some professional discussion of a Russian threat to Norway tends to default to two familiar narratives evoking World War II and the Cold War: ground hostilities directed at Finnmark, or a maritime stand-off centred on Svalbard. Given the new warfare realities, both deserve to be explicitly deprioritised (not ignored but placed in the correct proportion).

A land offensive into Finnmark is operationally unattractive for Russia on every axis that matters. The terrain, a narrow, road-poor, easily-interdicted corridor, offers no operational advantage that compensates for the exposure involved. More decisively, Russia simply does not have the spare manpower: the formations that would notionally execute such an operation, the Leningrad MD's northern brigades and the nascent 44th Army Corps, remain substantially committed to and drained by the Russia's war against Ukraine, and reconstitution to a scale sufficient for a serious offensive is realistically a matter of quite a few years even under the most pessimistic Finnish and Norwegian intelligence assessments[30]. Although now powered with tactical drone mass and ground robotics, a demonstrative probing ground movement toward the Finnmark cannot be excluded, but as a tool of diversion and disruption of Allied forces, not as a serious bid to seize and hold Norwegian territory.

A classical Arctic maritime confrontation as a contest for control of the sea and airspace around Svalbard, echoing Cold War bastion-defence thinking, is similarly a poor fit for present conditions. Two developments make it so. First, the operational environment has become radically more transparent: persistent satellite, airborne and surface multisensory ISR coverage of the Norwegian and Barents Seas makes any large-scale, sustained Russian surface, and even subsurface concentration difficult to conceal and correspondingly easy to target should conflict erupt. Second, Norway and its allies field capability tuned to deny Russia an easy contest in exactly this domain: the fully-delivered Norwegian F-35A fleet (52 aircraft) provides a credible area denial across the High North, while five P-8A Poseidon maritime patrol aircraft supported by Finnish and other allied assets represent a solid capability for classical (manned) anti-submarine warfare in precisely these waters. Combined with the severe logistics burden the Arctic environment imposes on any large-scale force, this makes a conventional bid for sea control around Svalbard a high-cost, low-payoff proposition for Moscow relative to the alternative discussed below[31].

1.5. High-Probability Scenario: Projected Trajectory

Drawing together current Russian fighting doctrine, its newly acquired and battle-hardened capabilities of modern warfare, and the pattern of incidents already observed against Norway and its immediate neighbours, a plausible (though not the only possible) sequence for the actualisation of this threat can be sketched.

The described pattern is offered as an analytical construct to inform planning, not as a prediction of a concrete operation. Also, it is - the reminder – deliberately framed as the worst-case scenario.



[30] Barents Observer, “Kola and in Karelia likely to get tens of thousands of new soldiers,” January 24, 2025 https://www.thebarentsobserver.com/news/kola-and-in-karelia-likely-to-get-tens-of-thousands-of-new-soldiers/423579

[31] Russia’s war against Ukraine proves this as well. Seizing an island is trivial compared to holding it under pervasive ISR and long-range precision strike. Snake Island fell to Russia in the war’s opening hours only to become untenable and be abandoned within months, because a garrison in the open sea cannot be sustained or defended once the enemy can see and reach it at will. The same logic has long kept the United States from “boots on the ground” in Kharg Island despite the disparity in raw capability.

Zero Phase

Continuous intelligence collection through such lines of effort as: GUGI seabed mapping of cable and pipeline routes; recurring deniable drone overflight of energy infrastructure, ports, airbases and other critical facilities, deployed mostly via shadow-fleet vessels; cyber-espionage and embedding dormant AI-powered cyber agents against Norwegian defence, energy and government targets; placing sleeper cells ready for sabotage missions by a pre-arranged signal; cognitive operations contesting Norwegian consensus on defence policy issues. This phase would also plausibly include the technical groundwork for false-flag intrusions and attacks sourcing or replicating Ukrainian-pattern drone components, markings and flight-planning signatures well in advance, so that they are ready for use rather than improvised at the moment of employment.

Phase 1

Once Moscow commits to limited aggression against NATO, zero-phase measures would be radically intensified, with reconnaissance and sleeper cell placement (both human and cyber), as well as pre-positioning other assets for the main synchronised effort. At the same time, overt sabotage against subsea cables and other critical infrastructure would plausibly remain at some median level (to make the crisis feel trivial or routine for allies) but without serious escalation, to avoid triggering their premature galvanization ahead of the actual “D - day”. GNSS jamming and cyberattacks would be conducted at a deniable level to test Russian respective capabilities before further scaling. Some limited, demonstrative Russian ground force movement in the Finnmark border area may or may not occur, depending on the aggressor’s concept and operational design (if it envisages ground phase in the Baltics, this could be useful to distract and disperse allied attention and force), but in any case, its comparable significance would be marginal.

Phase 2

This is “D - day” hybrid culmination, opening the overt aggression (right as it was in Ukraine on the 24th February 2022). Extensive synchronized cyber, cyber-physical, and physical sabotage operations would aim to produce the maximum disruptive impact across the critical strategic domains of Norwegian and Norway-based NATO defence in the first hours of an operation, as well as to generate a psychological “everything is collapsing” effect across Norwegian society and command architecture. Russian sleeper networks inside Norway would activate pre-placed sensory and communication infrastructure, enabling the operation of hundreds of remotely controlled or autonomous small UAVs, massively deployed from the Russian shadow fleet, unmanned surface vehicles and ground homepoints in Kola Peninsula. A portion of this package could carry Ukrainian-pattern markings or spoofed origin data designed to suggest a Ukrainian or rogue launch rather than a Russian one.

The purpose would not be durable deniability, which Moscow could not sustain once forensic attribution runs its course, but the shorter and more valuable prize of confusion during exactly the hours when NATO's own consultation mechanisms are already too slow to act: a contested first attribution narrative gives Russia additional time on top of the institutional delay already built into Article 5 decision-making, and opens a secondary line of effort aimed at Norwegian and European public and political opinion. These drones, equipped with AI networks trained for specific categories of targets, would strike soft, high-signature, visually distinctive and hard-to-replace objects.

Two target classes deserve explicit attention alongside the infrastructure and command targets identified. First, defence-industrial sites tied to weapons production or assembly for Ukraine as a target category Russian officials have repeatedly signalled in public rhetoric as a legitimate military objective wherever located, and one a mass cheap-drone raid can reach even where such sites sit inside otherwise well-defended NATO territory. Second, undefended civilian logistics infrastructure (food-storage and distribution warehouses in particular) which costs Russia a fraction of a single Geran to strike, requires no precision, and is disproportionately effective at generating exactly the panic, uncertainty and pressure toward a negotiated settlement this phase is designed to produce; a foodstocks warehouse fire achieves more psychological effect per dollar spent than almost any other target on this list.

The phase would be designed to make simultaneous effects, for triggering panic, blackouts, communications collapse, and general disorder as a side effect. GUGI sabotage groups would try to damage Norway's subsea power interconnectors to the UK, Germany, and Denmark along with other deep-water infrastructure. This phase might also (not necessarily) extend to attempts against Allied satellite systems. In the Norwegian context, priority targets would likely include the SvalSat ground station on Svalbard, as well as early warning radar and tracking sites.

[32] Unmanned Aerial Vehicles.

Phase 3

Rather than succeeding Phase 2 in a discrete sequence, this phase would partially coincide with and extend across it, being focused on a compressed in time combined drone-missile kinetic deep strike attack(s). It would aim to maximize the Phase 2 effects, but with a focus on target classes that are significantly harder to reach and / or hit with small-class loitering munitions. The key asset would be Iskander-M missile capability as the one harder to track and engage (operated by 152nd Missile Brigade in Kaliningrad, 112th Guards Missile Brigade in Shuya, 448th Rocket Brigade in Kursk and 26th Missile Brigade in Luga), along with cruise and quasiballistic missile carrier aircraft and naval combatants (much more exposed to F-35/P-8 fleet) and a massive employment of Geran/Gerbera long-range drones.

Phase 4

Afterwards, Russia would likely seek to extend its Kola-based electronic warfare and air defence "dome" seaward and establish sea-denial conditions in the Norwegian and Barents Seas sufficient to delay or degrade allied reinforcement. But given Norwegian and allied strong conventional maritime capability, it would hardly succeed in this. Therefore, Moscow would likely shift to an indefinite, elastic campaign of sea denial attrition across the Barents sea, partly reaching Norwegian Sea, in a rolling, open-ended condition bleeding Norwegian and allied defence capacity. The backbone of this concept would be persistent unmanned harassment based on small, cheap, mesh-networked uncrewed surface vessels and loitering munitions (with a big portion of EW immune autonomous and fiber optic drones) launched from Kola peninsula, and conducting patrols to jam, strike, threaten, mine-lay or pre-position in dormant "zhdun"[33] state against Norwegian and allied shipping, offshore installations and port infrastructure. Under permanent unmanned satellite and ISR coverage, this line of effort would activate in waves timed to Norwegian or allied military and logistics activities. Norwegian and NATO efforts to interdict these vessels would themselves become a target set: helicopters and warships are perfect targets for unmanned systems, while jet-powered aircraft and submarines are not tuned to counter such LSS[34] objects. Only a matching unmanned capacity is capable of dealing with this threat. Broad sea and coastal mining, delivered by unmanned systems, would target choke points and approach corridors at Vestfjorden, the Andøya/Bodø/Tromsø approaches, and the Bear Island gap. Combined with periodic air raids combining missiles, deep-strike drones and decoys, against high-value targets – by this stage plausibly including renewed strikes on strategic and logistics infrastructure – as a standing pressure instrument – Russia would aim to sustain attrition tempo in "as long as it takes" manner.

[33] "The one being in a waiting mode" (rus.)

[34] Low-slow-small.



1.6. The Defence Challenge

The central operational problems this scenario poses for Norway and NATO are those of tempo and attritable mass. Russia would try to execute the key phases 2-3 within a window probably measured in hours, which is definitely shorter than NATO's collective response cycle. Instruments such as Baltic Sentry, operational since January 2025, and the newly launched Arctic Sentry operational since February 2026 under JFC Norfolk, have measurably raised the cost and reduced the frequency of deniable sabotage in the region waged within the sub-threshold warfare format. By providing persistent surveillance and military presence across the Baltics and the High North, it is helpful, but still not sufficient in the case of surprise attack which largely relies on traditional and new asymmetric assets.

But even Russian conventional assets alone are most likely to generate substantial strike effects against Norway, as the Kola-based force sit geographically outside the footprint of NATO's standing rapid reaction forces present in the region.

What would suffice is the early reconstitution of the entire capability architecture in line with the renewed threat profile – and its timely scaling.

2. The Capability Gap

Force Design for the New Warfare

Given the threat profile for Norway, its Armed Forces indisputably possess a range of brilliant capabilities to counter a substantial portion of this threat — but, regrettably, not all of it. The "missing piece" for Norway's Totalforsvaret[35] includes: comprehensive air defence capability tuned to counter combined saturated drone-missile attacks; effective sea denial and littoral defence against modern asymmetric threats; and, above all, the "connective tissue" for the entire combat effectiveness – a new highly resilient, autonomous and adaptive command & control architecture, capable of connecting enormously diversified sensors, processors and effectors in real time across the entire battlespace and bringing a bridge over a chasm between geographical vastness and demographic scarcity of Norway.

Sensors – in military terminology, devices and systems that detect, locate, track, and characterize objects or activities across the battlespace (radar, electro-optical/infrared, acoustic, electronic intelligence, open-source feeds etc).
Processors – the computational and analytical layer that fuses, correlates, prioritizes, and interprets sensor data in near-real time, generating actionable tracks, threat assessments, and targeting solutions (battle management systems, AI/ML fusion engines, and command applications).
Effectors - the means of influence or destruction that act on the battlespace in response to processed information – kinetic (missiles, guns, loitering munitions), non-kinetic (electronic attack, cyber), or soft (deception, information operations).

The origin of this gap is twofold: chronic lack of attention to the Norwegian defence since the 1990s, and, most of all, the warfare revolution of the 2020s.

2.1. Not "Just Another Weapon"

Russia's war against Ukraine is the first full test of a warfare model in which unmanned systems replace networked manned platforms as the core of combat power. This is not about drones being added to existing arsenals as "just another type of weapon", because unmanned systems, especially in their autonomous incarnation, fundamentally alter the modus operandi on the battlefield. Their transformational impact is comparable to that of firearms having replaced the multi-millennial combat paradigm based on cold weapons in the late XVII century.

35 Total Defence (nor.)

A drone (or a robot) as a piece of hardware is only a small, while architecturally critical, element of the entire picture. Using unmanned systems at scale provides a chain effect of transformation of every part of military capability generation and deployment, from sensing and command & control, to kill-chain, fortification, and logistics.

This means, on today's complex and progressively "intelligent" battlefield, that simply acquiring a drone, robotic system, or artillery platform will be of limited value unless it is embedded within the wider enabling infrastructure of sensors, energy, communications, digital networks, and intellectual capacity.

Perhaps one of the most radical changes relates to the personnel. AI-powered robotized warfare with a high level of operational autonomy – a kind of a "Terminator embedded in the Matrix" – holds the promise of reducing quantitative demand for manpower in the foreseeable future. However, at the current stage of a transition the reverse is true: extensive use of unmanned systems reduces manpower attrition rate but necessitates bigger numbers of qualified manpower, not fewer. Greater staffing is needed to manage advanced capabilities until processes become fully automated and optimized, particularly in operating, maintenance, technical support, repairs, troubleshooting, data analysis, quality control, and decision-making tasks.

Smartphonization of Warfare – the term coined by the SSC research team, to reflect the transition from a hardware-centric through software-defined to AI-powered warfare paradigm. Just as commercial IT evolved from mainframes to personal computers and finally to smartphones, military technology is undergoing a similar shift of MilTech individuation at the expense of size and price, powered by the conceptual evolution from mechanization to digitization, and now to intellectualization (autonomy).

'Matrix' & 'Terminator' – the original concept developed by the SSC research team describing the emerging hybrid network–atomic warfare model where a unified digital situational awareness and decision-making space ('Matrix') coexists with an autonomous effects execution loop immune to comms disruption, based on forward-deployed unmanned (autonomous) combat systems and their swarms ('Terminator'). The critical technical backbone for the former is resilient satellite communications, and for the latter – AI fed by structured combat big data.

Some other most meaningful features of this new paradigm include:

The distinction between front and rear has collapsed. Persistent surveillance and nearly unlimited cheap tactical precision strike now reach deep into what used to be secure rear areas. Nothing operating within drone-powered kill web range is permanently safe, regardless of distance from the line of contact.

The mainstream of drone evolution changed its trajectory since the 2020s (and perhaps for good) towards prioritizing small UAV classes. This means, attritable mass is favored over sophistication (with some balance to be found in the mid-term perspective as counterdrone technology matures). The proliferation of cheap, small, expendable, easily replaceable and adaptable systems flooded the battlespace in numbers no "big-and-beautiful" platform was built to absorb.

Small remotely controlled and progressively autonomous loitering munitions are gradually dwarfing the roles of artillery and other crew-served tactical strike systems as the kill zone expands. A drone with terminal guidance autonomy is to become soon the default means of precision fires across the close and deep battlefield.

A drone also becomes the foundation of mass and maneuver. As the battlefield is now transparent, and persistent sensing makes any concentration of force immediately visible and targetable, massed manned formations, the organising principle of land warfare for centuries, are no longer survivable. Dispersion is now a survival requirement at every echelon. This did not make mass and maneuver obsolete, it is just provided by “drone / robotic cross-domain fists”.

Operational planning on the tactical level and in part mission level has largely shifted from prediction to processing – absorbing and acting on a near-complete real-time operational picture faster than the enemy can act on his own.

Direct fire platforms have lost their centrality. Beyond-line-of-sight precision strike is now the norm. Main battle tanks and other direct-fire systems remain useful for certain surgical operations requiring special application conditions.

Industrial-scale production of small drones, and a corresponding comprehensive counter-drone architecture, are now baseline military capability category, genuinely new and comparable in significance to the rise of aircraft and air defence rising in the mid-20th century.

Long-range precision strike now combines missile systems and cheap unmanned mass, necessitating a layered and algorithmic air and missile defence architecture. Missile systems are themselves being “dronified”, enhanced with CV, maneuverability and frequency hopping algorithms.

Adopting this model by any nation, with no exception for Norway, requires four things to converge: a maturity of a new military technology, its economically appropriate scalability, military necessity to deploy it, and the cognitive willingness to recognise that necessity. NATO states generally have the first two. Ukraine (and alas Russia) were the first to have all four, partly by circumstance and partly because there was no alternative. Norway seems to have the first three, and the cognitive shift of understanding is actually the pillar needed to reorganize force structure, doctrine and procurement around this new paradigm and meet upcoming threats in all arms.

The following section examines Norway’s capability profile against its key threat vectors.

2.2. Countering Massed Combined Air Offensive

A modern synchronised raid combining ballistic and cruise missiles with mass, cheap drones that Russia mastered (and continues to) for years – with week-to-week technical adaptation and operational upgrade – is designed less to be individually survived than to overwhelm and exhaust whatever defends against them. Meeting that threat requires several distinct tiers to work together, and Norway currently has a part of the top of the pyramid and very little of the base.

NATO's current doctrinal language centered around the IAMD concept[36] obscures the true scale of the challenge, and would not survive contact with what Norwegian current capability in this domain is actually capable of. In particular, the word "integrated" pretends to provide a comprehensive coverage against aerial threats that the present architecture already fails to provide, given the changed composition and scope of a typical air raid. Within that composition, hyper/supersonic cruise missiles and ballistic missiles, subsonic cruise missiles and mass cheap drones are separate, although connected problems, each with a different answer, and in the attrition warfare Norway's current inventory based on F-35A, P-8A, NASAMS and NOMAD systems, adequately answers only one of the three.

Foundational observation:

Norway's critical advantage is that most of Norway's critical infrastructure, particularly southern and central energy export facilities, MCPP-N prepositioning sites, and production centers lies beyond the effective range of Iskander-M (500 km), which is the key conventional aerial threat Oslo has no immunity against. This would force Russia to rely here on hypersonic and supersonic cruise missiles (Kinzhal, Zircon) produced in severely constrained numbers, or standard cruise missiles (Kh-101, Kh-555) falling within NASAMS effective engagement envelope. The real vulnerability threshold Russia will exploit is the sustainable employment of Geran/Gerbera drones. Current Norwegian air defence architecture lacks the saturation tolerance to absorb simultaneous multi-hundred drone waves over weeks or months. This is the decisive capability gap in air defence – degradation through attrition via mass unmanned systems. Accordingly, counter-drone architecture must become a priority ASAP.

The part of a problem that has a formal answer is subsonic cruise missiles. Kh-35, Kh-101 and Kalibr along with their carriers make a more tractable problem, where Norway's current assets are well matched. Norwegian native NASAMS is a battle-tested interceptor against exactly this class of missiles, and Ukrainian operational data puts its effectiveness at over 90 %. Norway continues to modernise the system based on the lessons learnt in Ukraine, including experimentation of heterogenous launchers adapted for differentiated response to cruise missiles and drones with separate types of interceptors.

The problem is not NASAMS' quality but its overall quantity. Norway has only two batteries currently operational. Certainly, it relies on joint allied capability in the Nordic-Baltic Region. Also, the ground-based component would be supported by F-35 and P-8 aircraft spotting and hunting missile carriers (Russian fighters, bombers, submarines and warships, along with ground-based launchers wherever possible), which they would fulfill with a certain extent of success (in contrast to the highly outdated Ukrainian F16s).

[36] Integrated Air and Missile Defence (IAMD) – an air defence concept of networked architecture that unifies separate sensors, command nodes, and weapon systems to protect territories, population, and forces from airborne threats.

[37] International Institute for Strategic Studies (RUSI), "Iskander: An Improved Russian Missile Tests Ukraine's Air Defence," Nov. 18, 2025 https://www.rusi.org/explore-our-research/publications/ commentary/iskander-improved-russian-missile-tests-ukraines-air-defence .

Still, the open question is how successful Russia could be in disrupting radar coverage at the sabotage phase, and what if it attacks several countries simultaneously, saturating the raid with many hundreds of attritable drones and decoys, and making allies preoccupied with their own airspace protection.

At a sufficiently high saturation of cruise missiles and jet powered attack drones within a broader framework of massive combined attack, the number of batteries actually deployed may simply run out of interceptors before the raid runs out of missiles. That is a quantitative problem rather than a qualitative, and it is the one scenario where Norway may have to consider adapting F-35 for the atypical role of missile interception itself (as it currently works in Ukraine), exactly for the moments when ground-based air defence is saturated and there is nothing else to fill the gap. At the same time, air defence against the supersonic & ballistic missile problem is non-existent. Oslo may count on Sweden's arsenal of approximately 200 Patriot PAC-3 interceptors, but in Norway's own current inventory nothing intercepts a ballistic missile. NASAMS fires interceptors of air-breathing targets (AMRAAM, AIM-9X, IRIS-T-SL), none rated against terminal velocity and trajectory of Iskander and P-800 Oniks warheads[37]. Arsenal capable of dealing with this type of threat, including Patriot's PAC-3 MSE, the Franco-Italian SAMP/T NG with Aster 30 B1NT (formally, with no battle-tested proof), or Israel's Arrow 3 (Germany's choice for procurement), is not being currently procured by Norway.

Oslo formally requested Patriot pricing in 2024 and has still not selected a system under the 2025–2036 Long-term Defence Plan. The government even proposed postponing the start of procurement until 2033, but the parliament rejected this and demanded to make a technical decision by spring of 2027 and an investment decision by spring of 2028 – still unacceptably late.

In July 2026 Norway joined nine other states and Ukraine as a founding member of a new Anti-Ballistic Missile Coalition in Paris. Certainly, there is a strong hope that NATO collective defence mechanisms would work impeccably, and a large portion of Russian missiles, once having attacked, would be intercepted by the U.S. Aegis and UK Sea Viper systems capable of countering supersonic and ballistic missiles. However, as the situation in the Middle East in summer 2026 showed, systemic attacks in attrition warfare make even partially successful attacks very painful. Besides, this component also depends on the goodwill of partners, as Oslo's component of Aegis is not tuned to counter ballistic threat.

While Norway's Fridtjof Nansen-class frigates are equipped with the Aegis Combat System, but unlike larger U.S. ships that carry heavy ballistic missile interceptors, Norwegian ships are optimized for localized air defence and anti-submarine warfare, using Evolved Sea Sparrow Missiles (ESSM) to intercept enemy aircraft and cruise missiles only[39].

Another part of the counter-ballistic solution lies in the left-of-launch concept – neutralization prior to missile launch (opposed to right-of-launch, i.e. missile interception. This implies, for instance, hunting Iskander or Bastion transporter-erector- launchers (TEL) before or after they fire, presumably based on F-35s fleet capability. However, this practice historically proves to be ineffective. A mobile launcher displaces, fires and disappears inside minutes which makes it a fundamentally hard targeting problem which total air superiority does not solve.

[38] Norskluftvern, "A Decade at the Oars Without Rowing – Norway's long-range air defence requirement," July 27, 2026 https://norskluftvern.com/2026/07/27/a-decade-at-the-oars-without-rowing- norways-long-range-air-defence-requirement/

[39] Seaforces.org, "Fridtjof Nansen class Frigate Royal Norwegian Navy," https://www.seaforces.org/marint/ Norwegian-Navy/Frigate/Fridtjof-Nansen-class.htm

[40] National Interest, "The First Gulf War Shows How Hard It Is to Stop an Enemy's Missile Launches," March 11, 2020 https://nationalinterest.org/blog/buzz/first-gulf-war-shows-how-hard-it-stop-enemys- missile-launches-and-north-korea-knows-it

In the 1991 "Great Scud Hunt" in the Middle East, roughly 2,500 coalition sorties against Iraqi mobile launchers ended with few dozens of claimed kills, while a postwar Gulf War Air Power Survey could not confirm a single one, most or all of the "kills" turned out to be decoys or unrelated vehicles.

The more recent, partially successful example is Israel's campaign against Iranian launchers in June 2025, when Israeli officials claimed 60 - 80% of Iran's mobile launchers destroyed or disabled over twelve days. But the mechanism was not open-space hunting of dispersed TELs on the move, but largely strikes on the fixed underground storage and tunnel-access points TELs had to return to, combined with air dominance so complete that Israeli aircraft could loiter for extended reattack windows deep inside Iranian airspace with minimal contest. Iran's launchers were also far less dispersed, far less practiced in shoot-and-scoot discipline (compared to Russia), and operating without a layered air defence system of their own to contest the hunters.

None of those conditions apply to a Bastion and especially to an Iskander unit operating from inside the Leningrad Military District or the Kola Peninsula, under Russian EW, S-400/S-300 and fighter coverage, with an OPSEC discipline around mobile-launcher displacement that Russian forces have refined in wartime condition. Norwegian and allied F-35s would be hence hunting inside quite a contested airspace against a harder target than either 1991 Iraq or 2025 Iran presented.

The honest conclusion is that Norway currently has no reliable answer to the ballistic threat, and building one in short terms potentially runs through the new Anti-Ballistic Missile Coalition and collaboration on Ukraine's Freya project (see Chapter 3.4).

Finally, countering the drone component is the new segment concealing most of the pitfalls for Oslo. It cannot be addressed by scaling up anything already deployed in the Norwegian Armed Forces. While most of their air defence systems are technically capable of intercepting both cheap $20,000–80,000 propeller-driven drones such as Geran-2, and their more costly jet-powered modifications, against the quantitative scale of this threat, would by a cost-exchange absurdity, leading to arsenal exhaustion in days or weeks. The use of NASAMS missiles can be arguably justified in rare cases against the minority of raids of jet-powered Geran-4 aimed at critical strategic targets, where the value being defended clearly exceeds the interceptor's cost. But for the mass of the threat, a completely different set of cheaper, purpose-built systems is required – the one barely existing in Norway's current force.

Ukraine's own architecture built under fire shows what that layer actually looks like. Some of the key pillars include the following.



[41] Understanding War, "Iran Update Special Report: June 24, 2025, Evening Edition," June 24, 2025 understandingwar.org/research/middle-east/iran-update-special-report-june-24-2025-evening-e/

Ground-based mobile fire groups (MFG) equipped with machine gun systems

Ukraine now runs nearly 1000 such MFGs armed with automatic cannon or heavy machine guns, the most optimal tool for intercepting low-slow-small Shahed-type targets and their decoys. In practice, the current state in Ukraine is not yet state-of-the-art, as a big fraction of those groups still operate systems with manual aiming (improvised truck-mounted heavy machine guns like Soviet DShK or American Browning M2s, or ZU-23-2). The trend where the system moves and which radically increases efficiency is installing advanced aiming powered by thermal optics, searchlights, and laser rangefinders for night operations. Self-propelled anti-aircraft gun (SPAAG) systems, such as the Gepard, or advanced automated systems like Skynex (utilizing highly efficient programmable airburst ammunition) show significantly higher efficiency but require a more complex supply chain. A growing number of MFGs also operate low-cost guided rocket effectors (such as the laser-guided APKWS Hydra 70 and modernised Soviet R-60 and R-73 air-to-air missiles adapted for ground launch), which provide effective engagement at greater ranges and against higher altitude targets while remaining far cheaper than conventional SAMs. What is really the future transforming the capability and leading to its utmost efficiency is AI-based automation, where a neural network paired with a weapon station to conduct real-time autonomous acquisition and tracking. These are such solutions as Ukrainian Sky Sentinel, a 12.7mm remote weapon station with engagement out to two kilometres. Norway's current inventory includes tested in Ukraine Kronsberg's CORTEX Typhon C-UAS on Dingo 2 armored vehicles with PROTECTOR remote-controlled turrets.

Inter-ceptor drone operator crews

Having started in Ukraine in late 2024, this trend scaled extremely fast, and in February 2026 Ukraine's Air Force already reported some 6,300 interceptor-drone sorties, destroying over 1,500 Russian drones. Unit costs run $1,000–5,000, and Ukrainian training pipelines bring an operator to roughly 50% engagement effectiveness in about 4-6 weeks (5 months for a full operational capability). Washington has taken this seriously enough to start fielding a scaled version of the Merops interceptors, while Great Britain opted for industrial scaling of the Octopus system. Still, this capability is only at dawn of its ripening; as Russia started fielding and scaling jet-powered Geran-3/4 specifically to outrun interceptor drone, Ukraine's own interceptor fleet is now racing to go jet-powered in response. A country adopting this capability today has to adopt the racing cycle with it, not a fixed piece of hardware.

[42] As far as we know, there are no direct operational analogues deployed in Norwegian forces at scale, but the technological and industrial base is more than sufficient to back up deployment if needed.

[43] Surface-to-Air Missile

Aerial mobile fire groups

As technical characteristics of a Shahed-type drone allow it to proceed until the terminal stage at high altitudes above the effective engagement envelope for machine gun systems, this necessitates a specific type of MFG – aerial crews on helicopters and slow-pace jets used for shooting down Geran/Gerbera with door-mounted machine guns or as homepoints for drone interceptor operators. This is a low-cost tactic which is fast to field in Norway as it requires no new procurement, only doctrine, training and a permissive rules-of-engagement framework. Norwegian 18 Bell 412 utility helicopters, half of them recently upgraded and life-extended by 15 years, as well as expected 6 Sikorsky MH-60R Seahawks, would be extremely vulnerable at FEBA in the new realities, but may find a new incarnation as a Shahed-hunting fleet capable day and night.

Electronic warfare & deception measures

EW against drone navigation and terminal guidance is quintessential for countering drone threat since 2022. Ukraine has fielded GPS-jamming and spoofing belts, along with decoy emitters and even physical decoy sites, to degrade Shahed, and later Geran navigation accuracy or lure them off target. Russia continuously responds by retrofitting its drones with progressively complex CRPA systems, beginning with the 8-element Kometa-M and escalating to 16- and 32-element configurations, making Ukraine adapt by complementary increasing density of EW pressure. It is currently one of the least visible but most cost-effective tiers of the whole architecture, and there is no indication Norway has an equivalent program in place.

A diverse sensing network

None of the above effectors work without sensing layer feeding one shared operational picture. In Ukraine, the growing network of passive 3D radars (Israeli RADA and analogues) is complemented by electro-optical coverage and “Sky Fortress” network of acoustic sensors, with 10,000+ of microphones tuned to a distinctive engine note of different Geran and Gerbera modifications. Norway would hardly go without this new acoustic layer, given drones’ reduced radar signature, and especially given the trend towards fully autonomous, AI-guided drones without radio emission such as the Russian “Molniya” type.

Digital battle management architecture

The layer that closes the kill web is a battlefield-management platform that fuses radar, optical, acoustic and open-source feeds into a single shared picture and pushes tracks down to operators in near-real time. In the case of Ukraine, this role is performed by the Delta system as a kind of joint all-domain command-and-control (CJADC2/JADC2) architecture NATO states are still largely prototyping. Norway needs an equivalent, and whether its Mime program meets these requirements is best addressed through separate, primarily Norwegian research.

[44] The Forward Edge of the Battle Area

[45] Controlled Reception Pattern Antenna

Civilian alert networks

Alongside, Ukraine has institutionalised a civilian early-warning layer based on dozens of Telegram and Signal channels, some with millions of subscribers, that translate the military's operational picture into real time and plain language alerts civilians can act on more meaningfully and in advance than a generic siren allows. Channel operators rely on military and intelligence sources. This is a zero-cost, high-trust dissemination tier, and it perfectly fits into the total defence concept of Norway (Oslo currently uses LTE messaging via national mobile operators which is more centralized and fragile for the lack of redundancy).

The Norwegian command already designated Heimevernet (Home Guard) to become an organisational home for the counter-drone segment of the air defence, although strictly defining its role around tactical, low-altitude ground-based sensing and defence, while high-altitude or wide-area air defence remains the domain of the Royal Norwegian Air Force. Given the above capability structure tested in Ukraine and current Air Force arsenal for air defence, if this would work remains a big open question. A further open question is whether Oslo has fully grasped the manpower requirements involved in fielding and sustaining an effective C-UAS capability with credible coverage across Norway's terrain and littorals, especially at the initial phase until operating procedures are tested, streamlined and optimized. Without ambitious comprehensive automation and incorporation of AI agents, the current 40,000–45,000 Heimevernet personnel (with as many as 3,000-strong rapid-reaction element) would never suffice.

For Norway, the maritime dimension compounds this calculus exponentially. Russian naval drone platforms, if deployed at scale as planned by 2027, would not be like the first-generation strike USVs focused on direct strike. Those will be autonomous USV motherships for aerial drone swarms (and launchers of SAMs against Norway's helicopter fleets as well). The distinction is operationally critical: while a handful of kamikaze USVs represents a containable tactical problem for Royal Navy, yet swarms of aerial drones launched from dispersed, mobile maritime platforms across the Barents and Norwegian Sea represent an air defence problem for both Navy and Heimevernet of fundamentally different magnitude. Such swarms would not require deep penetration inland—coastal bombardment of Norway's littoral infrastructure, radar sites, and dispersed military positions across Finnmark and Troms would remain achievable within platform ranges and redundancy margins. This would require from Reitan to consider not just Ukrainian counter-drone architecture expertise outlined above, but also the tactical-level C- sUAS which is only just taking shape on the Ukrainian frontline, requiring tactical EW saturation, shotguns and all-encompassing physical protection along with interceptors and MANPADS.

[46] Norwegian Government, Drone Strategy for the Defence Sector, December 1, 2025, regjeringen.no/en/documents/drone-strategy-for-the-defence-sector/id3141461/?ch=3

[47] HQ of Norwegian military command.

[48] Counter-small UAS.

2.3 Countering Sabotage at Scale

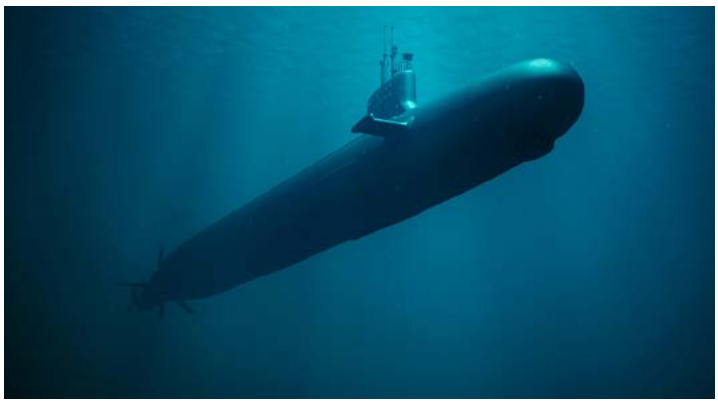
Given Russia's demonstrated reliance on sabotage and other forms of sub-threshold activity, increasingly augmented by AI-enabled and unmanned technologies, Norway's extensive network of subsea cables, pipelines, and other critical infrastructure represents a significant vulnerability. The scale and sophistication of Norway's counter-sabotage capabilities should therefore be commensurate with both the magnitude and rapidly evolving character of the threat. Moreover, it is not a purely wartime capability – it needs to provide all-encompassing detection, denial and neutralization continuously, in peacetime as much as at war, against both conventional and new "smartphonized" (mass, cheap, low signature, algorithmized) and deniable threats with a very complicated attribution.

However, Norway's current answer to this challenge is disproportionately limited and structurally misaligned. Moreover, this is caused by a lack of organizational agility rather than a lack of relevant technology. The problem is that capability generation in this domain, is centered around Royal Norwegian Navy's glory: a Frigate Squadron of four Fridtjof Nansen-class ships pending replacement by five Type 26s from 2030, six Skjold-class fast attack corvettes now receiving a combat-system upgrade, and a submarine arm being rebuilt around the Type 212CD – all backed by the F-35 and P-8A fleets as well as NATO's Boeing E-3A Sentry AWACS. In other words, it is built and sensor-tuned to find and fight other warships and submarines, not naval and aerial drones, autonomous underwater vehicles, remote mining systems or small sabotage groups deployed via formally civilian carriers such as a tanker fleet.

While still vital for deterrence of such threats as GUGI deepwater submarines, these assets are incredibly expensive, slow to build, almost impossible to replace in operational tempo and too few in number to provide ISR and denial coverage of all the offshore, littoral and undersea infrastructure over thousands of kilometres.

The response required is a substantial, attritable and highly autonomous (powered by agentic AI) forward unmanned / uncrewed maritime capability that includes both an offensive component and layered counter-UAS/USV/UUV defence based on thousands of distributed but fused sensors and effectors. Physical security of naval bases, and especially surface assets in open waters, against small drone attacks is demonstrated by Russia's Black Sea Fleet.

The irony is that Norway is arguably better positioned than almost any NATO state to close this gap on its own (with measurable aid from Ukraine). Decades of managing complex offshore oil and gas infrastructure have made Norway a global leader in marine robotics, remote operations, and subsea autonomous technology. Such companies as Kongsberg and various smaller marine tech clusters constantly pioneer cutting-edge unmanned / autonomous surface and underwater vessels for civilian and industrial applications. This potential has simply not yet been converted for military application based on Ukrainian best practices and operational blueprints with anything like the urgency applied to the frigates and submarines. However, this is the only way to provide a response to sabotage threats at the needed density, speed, and cost-effectiveness.



2.4 Sea Denial in Full-Scale War

Countering offshore and littoral hostilities from the water and the sky in case of overt Russian aggression would presumably require a different extent of effort and endurance compared to neutralizing deniable sub-threshold sabotage activities. The former needs extensive, pervasive ISR coverage backed by a comparatively limited arsenal capable of a fast, precise, point-to-point reaction. The latter dictates massed and sustained coverage on both the sensor and the effector side, able to absorb continuous attrition. It shifts the requirement from remote monitoring and rapid reaction to something closer to a standing kill web and killzone.

This capability also implies full-scale contesting the Northern Fleet's submarines and surface combatants, and keeping the sea lanes open for NATO reinforcement to reach Norway and, beyond it, the Baltic. This naval warfare in the traditional sense is where Norway's high-end procurement is currently focused – and this is exactly the reason why Russia is likely to try to avoid or minimize it. In a symmetric contest in this theatre, Norway's capabilities backed by allied regional naval and airpower would eventually hold a real advantage over most of Russian capacity in the region: F-35 fleet would probably suppress most of Russian naval aviation and even surface combatants operating from Kola; while 212CD submarines, once fielded, together with P-8A's are potentially capable of neutralizing even Russian most protected Yasen-M class fourth-generation nuclear-powered multi-purpose attack submarines (the Kalibr and supersonic Oniks carriers), let alone the remaining force. Given standing NATO submarine forces in the region (currently substituting the lack of Norwegian capability expected only by 2029), Russia would very likely lose a conventional fight for control of the Norwegian and Barents Seas, and Moscow knows it.

The hypothesis, therefore, is that in a potential conflict Russia would apply against NATO and Norwegian naval forces precisely the same approach Ukraine has employed against the Russian Black Sea Fleet since late 2022. Moscow is already actively constructing this capability, centered on a distributed unmanned maritime and aerial kill-web.

Russia's naval drone program is considerably further than is generally appreciated in Western threat assessments, and a meaningful share of its development and testing runs through the Baltic region. Russia has established both its key centers for naval drone development close to Baltics (not Ukraine): the Kingisepp Machine Building Plant near St. Petersburg (a serial production hub for sUSV), and the 'Ushkuyanik' R&D center in Veliky Novgorod, (R&D of USV/UUV and their fleet integration).

During the FLOT-2026 exhibition, Rosoboronexport displayed an expanding family of unmanned naval platforms including the Briz, Orkan and BEK-6 strike and multipurpose USVs, the MMT-300 and Klavesin-1RE autonomous underwater vehicles, explicitly marketed around AI-enabled autonomous naval combat.

The Kingisepp-built Oduvanchik kamikaze USV, ordered into trials by the Ministry of Defence in December 2023, can reportedly carry a 600 kg warhead over 200 km at up to 80 km/h and, notably, has no visible communications antenna, designed to run on inertial navigation corrected by satellite positioning against fixed targets, sidestepping the need for a live control link.

[49] Assessment of the allied capacity for countering Russia's strategic nuclear triad in the region is beyond the research scope of this paper.

The key constraint currently holding back the Russian naval drone fleet from full-scale employment is the same visible in Russia's aerial drone campaign: a resilient long range connectivity analogous to Starlink global satellite internet service. But this is not a permanent Russian weakness, and it is closing fast. Moscow's answer, the Rassvet satellite constellation built by Bureau 1440 and launched from the Plesetsk Cosmodrome, moved from sixteen satellites in March 2026 to a second batch in July, already delivering several hours of stable daily connectivity to Russian units at the front by August 2026. Ukrainian military intelligence has publicly confirmed Rassvet is being deployed faster than Russia's own stated schedule, which itself targets 250–300 satellites by 2027 and over 900 by 2035. Once that scaling reaches minimum relevant density, the connectivity constraint currently limiting Russia's unmanned naval power in the High North will disappear.

It can actually partly disappear even earlier, as Russia makes rapid progress baked by substantial effort in mesh radio technology combined with optical modules (fielded on the Geran-4 "Seeker") and full combat autonomy (demonstrated in the last "Molniya" modification), with no need for continuous connectivity at all.

Moreover, with a capability set Russia already possesses, even with no naval drone at all, it can create a serious problem for a state that depends, as Norway does, on undefended commercial and coastal maritime traffic (as illustrated by current drone terror of naval traffic around Odesa and Chornomorsk).

In this respect, while Norway's high-end naval and air assets remain the right tool against the traditional Northern Fleet contest, what it should actually be building along with that is the kill-web layer on a more capable and resourced basis, than a current counter-sabotage framing implies. The logic of the latter is reflected in deployment of Kongsberg-built HUGIN autonomous underwater vehicles in the Navy (since 2017), for mine detection, classification and identification. This is a good solution for sub-threshold warfare, but still a bit unsustainable for heavy attrition one, given its cost per unit (ranging from $5 to $15+ million). For the war of attrition, especially a prolonged one, these important reusable platforms with premium sensory payload need to be supplemented with a mass of much simpler (but effective for their mission), COTS-built one-way intelligence, minelaying and strike platforms like the Ukrainian Marichka or Toloka ($100,000 – $500,000 per unit). The same logic applies to unmanned surface vehicles and the Navy's UAV architectures.

That is the correct model and its "low-end" segment needs to – and can – be deployed along with Norwegian premium unmanned systems with greater urgency than multi-year big surface and subsurface legacy systems. This is because they would shape the core of the next-generation autonomous joint warfighting capability.

[50] Defence Star, "Stepping Into The Autonomous Era: Russia To Debut AI-Driven Naval Drones at Fleet 2026," June 8, 2026 defencestar.in/military/navy/russia-rosoboronexport-fleet-2026-stealth -autonomous-underwater-drone/11807

[51] EDR Magazine, "Fleet 2026 – Rosoboronexport presents a line of Russian USVs and UUVs," June 13, 2026 edrmagazine.eu/fleet-2026-rosoboronexport-presents-a-line-of-russian-usvs-and-uuvs

[52] Ukrainian Defence Intelligence (GUR), cited in Kyiv Independent, "Russia launching its own answer to Starlink faster than planned," August 12, 2026 kyivindependent.com/russia-accelerating- deployment-of-starlink-like-satellite-system-ukraines-military-intelligence-says/

2.5 Deterrence on the Ground

While any substantial ground offensive into Finnmark is a low-probability scenario, Norway still needs to be ready for countering a limited, disturbing and most probably dispersed, drone-backed Russian maneuver at its borders aimed at dispersing and pulling allied attention away from the primary axis of effort.

Norway will have only a single brigade fully operational by 2030, and two more by 2036, thus it does not seem to be prepared once such a scenario materializes. The powerful Air Force and Royal Navy would not suffice to deal without at least a limited – but fully ready for combat in the modern killzone – ground component.

Certainly, under the NATO umbrella Oslo might place hopes for the Finnish Jaeger Brigade and NATO's Forward Land Forces (FLF) based in Lapland to lend a helping hand for dealing with this sort of a challenge. But as we consider the worst-case scenario, an option where Norway would have to act on its own on the ground cannot be fully discarded.

The challenge is that even FLF may prove less effective than expected due to the battlefield architecture being transformed by robotization, and necessitating a completely new set of capabilities Russia have mastered in the war with Ukraine. But this is also good news, actually. This means that even two currently combat-ready battalions of the Brigade Nord, and border forces of the emerging Brigade Finnmark, with a timely bet placed on robotization and automation instead of mechanized mass, would be potent in deterring this threat by 2027.

A set of capabilities to be generated and deployed are exactly those that constitute the core of combat efficiency of mechanized and assault brigades of the Land Forces of Ukraine. This includes: kill-chain largely based on 24/7 drone-powered pervasive ISR and tactical precision strike, as well as digital battle management architecture and long-range artillery for massing fires (K9 and K239 Chunmoo systems Norway is currently fielding would suffice); robotized last-mile logistics and MEDEVAC; unmanned remote mining and demining, modular fortification adapted to the drone threat and long-lasting quartering, and prepositioned minefields and non-explosive barriers; autonomous robotized firing positions; combat robotized escort for infantry and armoured vehicles; tactical and individual counterdrone protection (in addition to the strategic-level C-UAS); tactical R&D innovation; layered SIGINT and EW tuned for drone warfare and brought down to the tactical level as well. The 54 Leopard 2A8 NOR tanks with Trophy active protection Norway is fielding can also be of a limited use, but plausibly most of them would be lost until those narrow use cases for modern killzone become recognized by the command[54].



[53] Barents Observer, "NATO activates forward land forces presence in Lapland,". June 7, 2026
hebarentsobserver.com/security/nato-activates-forward-land-forces-presence-in-lapland/452108

2.6 Electronic Warfare

The significance of EW enormously grew in the drone warfare age: the dominance on the battlefield is increasingly determined first in the electromagnetic realm, and only then in the kinetic realm. In fact, Russia's war against Ukraine has transformed electronic warfare as a component of anti-drone defence from a narrow specialization into a comprehensive tactical reality. Moreover, it prioritized (and made more complicated) the deconfliction between air and ground forces and electronic warfare assets for preventing "friendly fire". On the technical level, EW shifted from the employment of a limited number of now vulnerable, big "dome" systems toward the mass deployment of dispersed tactical-level assets to provide flexible protection for command posts, UAV and UGV crews, small infantry groups, individual technical systems, and individual combatants. At the same time, EW saturation of the battlefield skyrocketed development of electronic immunity know-hows.



Along with Ukraine, Russia, already being traditionally highly capable in EW, has fully learned and adapted to the new reality. Along with its legacy large vehicle- or ship-mounted platforms such as Krasukha, Murmansk-BN, Zhitel and others, built to blind NATO's aircraft, radars and C2 networks in a conventional war – a capability Russia continues to modernize and enhance, it developed a powerful tactical echelon composed with compact, modular jammers mounted on individual vehicles, dispersed positions and even soldiers, designed for the drone-dominated killzone. In Russia's war against Ukraine, these two distinct tiers are operating together – and so would they do in a potential war against NATO.

The latter tier is the one Norway almost completely lacks, while in Ukraine it has already passed several distinct evolutionary phases, including linear frequency denial, frequency agility and adaptive frequency hopping based on software-defined radios, physical immunity based on using fiber-optic drones at scale, introducing infrared and acoustic detection along with RF detection as a counter-response, and finally embedding AI-powered autonomy for functional independence from any comms link at the terminal stage.

Thus the current EW challenge differs dramatically from the Cold War model of contesting the spectrum.

Finnmark has lived inside an active Russian jamming footprint since 2017, and the record of it is well documented by Norwegian and Finnish regulators. The source is Northern Fleet EW units based near Severomorsk and in the Pechenga district, a few tens of kilometres from the Norwegian and Finnish borders. The trend is clear: from five recorded incidents in the seventeen months after autumn 2017, to 294 days in 2023 and since 2024 described by Norwegian aviation authorities as practically a daily basis. In April 2026, Norwegian police measured jamming and spoofing reaching down to 1,800–2,000 feet (compared to the 4,000 feet recorded before).

This can be in part explained as Russia's own electromagnetic self-protection around Kola military and critical infrastructure against

[54] Therefore Oslo's decision not to exercise the option for a further 18 in favour of drones and long-range fires reflects exactly the right instinct

[55] High North News, "Serious GPS disruptions in East Finnmark," April 28, 2026 en.highnorthnews.com/business/gps-disruptions-at-lower-altitudes-close-to-norways-border-to-russia/1110164

Ukrainian deep strike attacks. But the distinction of intent should not distract from the capability scope that can be potentially aimed directly against Norway and allies in the case of a direct war. With simultaneous, full-power, broad-spectrum jamming and spoofing across GLONASS/ GPS/Galileo/BeiDou constellations, likely combined with barrage jamming of aerial communication, civil aviation will be effectively unflyable, maritime navigation would lose GPS positioning entirely in affected windows, GPS-guided munitions, ISR systems and communication layer would be degraded. Emergency and search-and-rescue services could lose positioning capability at the exact moment they are most needed (see Phase 1 in the Chapter 2.5).

What makes this threat particularly acute is that in any hostilities scenario, this is not a capability Russia would need to deploy: it is already switched on, fully operational, and being permanently consolidated.

What can Norway currently put against it? Its own EW inventory is small even at the high-end tier. There is no Norwegian equivalent of a dedicated airborne jamming platform. Its only dedicated airborne EW unit, 717 Skvadron, was retired in September 2022, and no dedicated replacement has entered service since. The F-35's internal EW suite is built for self-protection and localized suppression only, in contrast to Russian Khibiny (L-175V).

Europe's broader gap in this capability is not expected to close before 2030, when Germany's still-unbuilt Eurofighter EK is due to enter service.



On the ground, the Army only recently began fielding a modern EW capability, but currently it actually provides only electronic surveillance (SIGINT) functionality, and the Fåvne R&D project is on the way to develop and add an electronic attack (offensive jamming) capability Norway doesn't have at all. Prototypes are currently actively tested in sandboxes, operational delivery is expected 2027-2028.

Detecting and attributing Russian Kola EW emitters is well within reach of Norwegian and allied sensors, but physically suppressing them is a different matter, given the dense S-400 / Pantsir air defence belt around Severomorsk and Pechenga, the partially mobile and rapidly regenerating nature of systems like Murmansk-BN.

The challenge for Norway intensifies at the low end, tactical EW having emerged as a new complex reality throughout Russia's war against Ukraine. Neither electronic offence nor electronic protection capabilities for the modern battlefield are being deployed, based on adaptive software-defined radio, let alone physical immunity through fiber optics and functional independence through onboard AI.

[56] Key Aero, "Norway bids farewell to Falcon 20ECM fleet after 50 years of operations," Oct. 6, 2022 key.aero/article/norway-bids-farewell-falcon-20ecm-fleet-after-50-years-ops

[57] Heimdall, a Rohde & Schwarz system now replacing six P6-300M tracked platforms dating to the 1990s

But the first right step in this direction was made by 2024 contract with Radionor (as a part of Mime program) for EW-resilient tactical broadband radios, straightforwardly focused on GNSS-independent navigation – today's key need of the battlefield – along with communication resilience (yesterday's key need, whilst still relevant).

Moreover, the respective agile innovation ecosystem transcending a single vendor is non-existent but essentially required, as EW on the modern battlefield is a constant frequency competition necessitating not just tactical, but technical adaptation 24/7 in a wartime. That logic is exactly what Ukraine has spent 4+ years developing and what Norway would require in a potential conflict with Russia, extending well beyond the ground domain.

What probably would soon make Oslo more attentive for tactical-levl EW is realization that this capability is critical not just for combined-arms operation on the ground (a low-priority scenario for Oslo). Yet the case for tactical EW becomes far more urgent when we find out it similarly – and even stronger – applies to Norway's most critical operational priorities: continental air defence, littoral air and maritime defence, and offshore sea denial. Modern unmanned systems, including both fixed-wing and rotary-wing UAVs, surface and subsurface uncrewed vessels, ground and amphibious robots, have become the primary distributed sensor and effector in all physical domains and far beyond the frontline on the ground.

This means, all Norway's total 100+ thousand km - long coastline area, with all of its islands, jagged fjords, and rugged inlets, is endangered with a type of a threat addressing which needs exactly the same EW-approach as on the battlefield. Despite the trend towards AI-powered autonomy, most are still vulnerable to precision jamming, and spoofing as any tactical radio network in a trench. Ukraine's massive integration of EW into its air defence architecture since 2022 confirms this operational reality. This reality demands not just centralized strategic EW, but distributed, object- and platform-based electronic detection and attack systems tuned against small aerial and maritime threats with adaptive frequency hopping. Moreover, the current EW development logic made UAVs, uncrewed surface and underwater platforms carriers of SIGINT and electronic warfare packages.

Norway's EW challenge is therefore focused on this distributed "tactical" layer which is tactical only by name, while actually becoming the key and extending into air and littoral multi-domain defence.

2.7. The Quantum Leap from C5ISR to C7ISR Challenge

Norway's program to build the connective C2 layer that would be relevant to the modern warfare requirements is real, substantially funded, and deserves an accurate description before any critique.

Mime is a program running from 2018 to 2030, managed by the Norwegian Defence Materiel Agency with Kongsberg as prime contractor responsible for overall architecture and systems integration. What is known from open sources, its scope includes crypto solutions, antenna solutions, communications infrastructure, C2 and decision support systems, as well as modernizing tactical command systems across the land, sea and air domains. Requested capabilities are expected to enter service in 2028 - 2030. The stated goal is a tactical information infrastructure giving Norwegian forces greater operational freedom of action compared to pre-2018 stance, as well as fitness to joint operations with NATO while preserving the total defence framework.

THOR is the Kongsberg-built multiband tactical radio backbone that Mime complements. Around it sits a set of supporting acquisitions such as a Tactical Core Network System (awarded to Clavister in January 2026), Rohde & Schwarz high-power HF transmitters at some twenty locations providing beyond-line-of-sight naval command and control and

[58] Kongsberg, "MIME Program," kongsberg.com/what-we-do/defence-and-security/advanced-solutions/mime-program/ Accessed Aug. 15, 2026

[59] Armada International, "Sprucing up Norwegian Army Comms," Feb. 12, 2026 armadainternational.com/2026/02/sprucing-up-norwegian-army-comms-milcom/

operated by the Cyber Defence Force, as well as noted Radionor's EW-resilient tactical broadband radios. The available data on the Mime program does not provide the picture comprehensive enough to make any radical assumptions on the relevance and efficiency of its accomplished output relative to the challenges of AI-powered robotized warfare. What is actually the impression, however, is that Mime's key center of gravity is a communications infrastructure with a decision support layer attached.

This decision support layer is represented but what may be called a workable digital connective tissue for the kill web in a narrow form – the Teleplan Globe's Network-Enabled Weapons software, integrated into the NORBMS and FACNAV battle management systems and delivered under Mime's own funding. It gives Norway an all-weather engagement capability for moving targets, and includes a dedicated module, FACNAV UxS C2, built specifically for manned-unmanned teaming across air, ground, surface and subsurface domains, giving unmanned system operators two-way information sharing with the wider battlespace picture. However, as a tactical weapon guidance based on external sensor data, it currently realizes just a tiny portion of the Ukrainian Delta features.

What Russia's war against Ukraine has produced is something structurally different: a data and application layer that functions as an integration core, into which communications are one input among many.

Below we present a short summary of some key features of Ukraine's Delta system. The intention is neither to contrast it with the system emerging from the Mime program (data for such a comparison remain inadequate) nor to position Delta as a better alternative. The objective is to enable the Norwegian expert reader to form a working appreciation of similarities, differences, and potential complementarity.

Ukraine's Delta system is not hermetic communication environment but a cloud-hosted, zero-trust platform (deliberately hosted outside Ukraine for the duration of the war since February 2023) built around a national data lake spanning air, land, maritime, cyber, space, medical and logistics domains, accessible through a single login on a laptop, tablet or phone. Its modules map directly onto the functions this report has described as the "missing piece" for Norway's total defence: Monitor for the shared digital picture of friendly and enemy forces; Vezha module for secure continuous video streaming from over a hundred UAVs simultaneously, with voice, joint video interpretation and monitoring of drone unit effectiveness; Target Hub for managing targeting and battle damage; mission control for planning and synchronising reconnaissance and target-acquisition assets; and a specific Delta Mobile tool for offline use when connectivity fails. In addition to this, the Avengers AI component processes drone and camera footage to identify pieces of Russian equipment per week, with Vezha classifying some 4,000 objects daily out of huge volumes of raw sensor input – both pooling structured data lake for AI training – unique "new gold" of the future AI-governed warfare. At NATO exercises, Delta has coordinated more than fifty drones simultaneously.



Three architectural differences follow from this, and each maps onto a specific Norwegian gap.

1. Delta is built as a data-first integration core, not a comms-first network.

It embeds standard NATO formats directly into its core architecture (Cursor-on-Target for position reports, MIP-derived structures for the ground picture, NFFI for friendly-force tracks, ADatP-34 for tactical data links, STANAG 4586 for UAV control) so that any sensor or effector implementing those standards can be exchanging tracks within days. That is an integration cadence, and it exists because Delta sits inside the Brave1 ecosystem where Ukrainian sensors and effectors publish into it directly. Mime's architecture apparently seems to be designed by a prime contractor to a defined specification, and it remains unclear how a newly fielded drone, UGV, C-UAS autonomous turret or a sensor grid is expected to appear in the common operational picture without passing long-way specification and access procedures.

2. Delta assumes connectivity can be denied.

Mime assumes connectivity must be secured, and its design language puts special stress on resilience, redundancy, crypto, and beyond-line-of-sight coverage. Delta's design language, as well as specific battle management systems it integrates, that in the heavy EW contest connection would be regularly cut, and builds for effects to continue anyway: offline mobile modules, mesh relay, and the onboard autonomy of systems progressively deployed, shape the space for the 'Terminator' segment of the new C2 architecture. This currently has no counterpart in Mime and other NATO C2 digital environments.

3. Delta is a live combat data engine for AI-governed warfare.

The aspect deserves distinct consideration, as the AI layer is emerging as the backbone of the next-generation warfare, enabling a leap of currently digitally half-automated detection, classification, prioritisation of targets, and eventually coordination within the kill web to a completely different scale of autonomous performance. The result is a dramatic reduction in both the cognitive load on human operators and the overall number of operators required. But to mature this layer necessitates structured combat data for training – data that only exists where combat is happening.



The Ukrainian MilTech producer Swarmer, for instance, builds hardware-agnostic swarm-control software trained on over 82,000 of its own combat missions, with the declared aim that a nation's drone deployment should be limited by production capacity rather than by the number of trained pilots. For a country with Norway's geography-to-population ratio, it is the core of the argument.

Overall, there appears to be scope for synergy to ensure that the Mime program would not aspire to modernizing C2 for human- and platform-centered C5ISR paradigm, and would be scoped as a fleet-management layer tuned for unmanned and robotized systems as the combat core, where AI-supported human operators supervise fleets of semi-autonomous machines – C6ISR, progressing into C7ISR. This paradigm has a completely different scope of data, real-time latency and authority decentralization requirements.

C5ISR – a military and defence acronym standing for Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance. It is an integrated framework of systems, software, and hardware that gives leaders real-time data and awareness to manage operations across land, air, sea, and space.

C6ISR – the next stage of a command architecture development, adding combat systems for the 6th "C". It implies that unmanned and robotic systems become an integral component of planning and executing combat missions.

C7ISR – the upcoming most advanced C2 architecture powered by artificial intelligence (Cognition stands for the 7th "C"), and implying that narrow agentic AI facilitates and streamlines data procession and combat functions, while human decision-making is backed by military generic AI.



One critical asset deserves a special credit in this section – the one Norway already holds as a foundation for next-generation AI-native C2 – and what Ukraine currently lacks as sovereign capability. The 'Matrix' segment is no less important than the 'Terminator', and its core is secured resilient digital communication with global coverage – i.e. a space-based one. That is exactly why access to Starlink remains one of the key competitive edges of Ukraine in the war, and why Russian "Rassvet" project development is so perilous for both Kyiv and NATO allies. In this respect, Norwegian ISR and space layer is a real national advantage few NATO members can match, including the Globus radar complex at Vardø, the Andøya Spaceport, and the NorSat microsatellite family supporting Arctic surveillance.

3. The Golden Card of Ukraine

The Totalforsvaret ‘Missing Piece’ Provider

Ukraine does not pretend to have and offer superior defence solutions for everything. 4-5 years of the most intense adaptation, innovation and combat practice cannot substitute for the accumulated depth of the Western (and Norwegian in particular) defence R&D, institutions and command culture across the entire capability spectrum: it cannot, and does not claim to. It is a claim about where the specific capability areas mastered in Ukraine and new to Norway as its partner matter most for the latter’s defence. It is precisely these areas of Ukrainian expertise that can address the capability gaps Norway currently lacks.

3.1. Ukrainian Security-as-a-Service: the New Horizon of Defence

Ukraine and Russia are, at present, the only two forces operating at scale in the new warfare paradigm based on the mass of unmanned systems in the air, on the ground and in the water, AI-powered kill-web, pervasive electronic warfare and differentiated algorithmic air defence. Pre-2022 solutions carry limited weight in this environment; many systems, including modern drone-based reconnaissance, strike and EW platforms, passed NATO evaluation in a laboratory but repeatedly failed on first contact with the new battlefield reality, being useless until adapted and integrated into the holistic capability contour.

Modern Warfare Doctrine

A new generation of warfare requires a new doctrine, which Ukraine has developed, battle-tested, and continues to improve. Rather than a simple list of lessons or technical know-hows, Ukraine offers this integrated system to partners in a modular, practical way. Partners select the areas they need (e.g., drone operations, ISR, electronic warfare, counter-drone, battle management, fortification), and receive a full package: proven procedures, adapted technology solutions, joint planning tools, wargaming exercises, and on-the-ground veteran advisory support until fully operational.



Modern Warfare Training

The greatest bottleneck in modern warfare is personnel. Standard drill-and-repeat training is no more enough. Today's battlefield demands a higher level of technical and analytical skill, and every specialist takes more time to develop, while can be lost instantly. This is why Russia invests heavily in training hundreds of thousands of teenagers in drone engineering and operation. Ukraine can address this for partners through two approaches. The first is focused short-term courses — intensive, practitioner-led training for rapid mastery of specific systems and capabilities. The second is embedded training missions, with mobile teams operating at battalion and brigade level, running realistic combat scenarios. This also covers officer-level instruction in unmanned operations, counter-drone defence, camouflage, and force protection. Ukrainian veteran instructors bring a deep, practical understanding of modern warfare and are well-positioned not just to transfer skills, but to help partners build a capability.

Battle Management Transition

Many partner nations believe their digitized command-and-control systems are state-of-the-art. They are not. Norway is a notable exception openly acknowledging the scale of the challenge (including in the national Drone Strategy). There is a fundamental gap between C4/C5ISR — built around secure radio, networks, and basic cybersecurity — and the C6/7ISR architecture centered around combat systems and agentic AI that modern warfare actually demands. The latter is built for managing fleets of unmanned platforms, real-time targeting, and automated big data processing (the mentioned 'Matrix' - 'Terminator' loop). It can only be truly refined through real combat experience. No amount of simulation or field testing replicates that. Ukraine offers the most direct path forward. Its Delta battle management system is fully operational, constantly evolving, and aligned with proven procedures covering mission planning, command and control, reconnaissance, strike, damage assessment, air defence, counter-drone, and counter-battery operations. Equally important, Ukraine holds large, structured combat datasets critical for training AI systems and for making the genuine leap to the next-gen C2, where AI and autonomy become the core.

Unmanned/Robotic Combat Ops

Robotic warfare is no longer a concept. It is already happening. Ukraine's forces have successfully conducted a series of fully robotic offensive operations to seize enemy positions and to capture enemy combatants, as well as fully autonomous defensive operations where AI-managed firing points destroy attacking enemy forces. Ukraine offers partners a complete capability package in this area that include networked deploying of unmanned aerial and ground systems for combat and support tasks – mining, demining, obstacle clearing, carrying kamikaze drones, communications, reconnaissance, strike, EW, and interception, all managed within a unified fleet management infrastructure. This covers everything from establishing procedures within partner units to personnel training, technical transfer, field maintenance, and support for planning and executing complex robotic operations.

Electronic Warfare

The old EW paradigm, focused primarily on suppressing control of big platforms and jamming radio-frequency communications in the operational area, is obsolete. Today's battlespace is more complex, where sheer quantity, tactical adaptability and, notably, physical survivability, matter more than the quality of a few high-tech systems. Ukraine's EW capability is being industrialized across nearly 200 firms and best practices mastered across 140 brigades, creating a layered jamming and spoofing defence from the strategic countrywide level to the individual soldier level. This also includes mobile EW units, dedicated EW drones, and a rapid adaptation cycle that responds to the enemy's frequency changes every two to six weeks. Real combat testing matters here more than anywhere else. There are documented cases of European systems passing NATO evaluation standards, then failing completely when deployed against Russian and Ukrainian EW assets. Laboratory results are not enough. Ukraine is also moving beyond preplanned frequency hopping into cognitive EW – AI-integrated systems that read the electromagnetic environment in real time, select the best response, and reconfigure themselves on the fly. In a battlespace dense with drones on both sides, preventing friendly interference is equally critical. Ukraine offers proven frequency coordination methods and technical solutions including frequency-hopping systems and navigation tools that reduce dependence on jammable GPS signals.

Tactical Air Dominance

The traditional model of air dominance built around manned aircraft no longer holds at the tactical level. Drone saturation and layered air defences have effectively removed conventional airpower from the low-altitude battlefield. A force with sufficient drone capacity can establish air dominance at that level regardless of the enemy's advantage in manned aircraft. Ukraine is the only European force operating at industrial scale in unmanned warfare with multi-million multirotor and fixed-wing drone production capacity, tens of thousands of trained operators, growing fleets of ground and maritime robots, and a proven command-and-control backbone. Deep strike capabilities via drones and cruise missiles are also being scaled, and a foundation for ballistic missile production exists. This matters directly for partner nations facing critical shortages in fires. Even if the NB8 countries (including NATO forward-deployed forces) meet all augmentation targets by 2027, their combined fires capacity will remain far below that of Russia, the one continuously refined through combat use. A pooled munitions reserve built with Ukrainian industrial and operational support would not close the gap entirely, but would narrow it significantly at a fraction of the cost.

Counter-Drone Warfare

The legacy air defence model is broken against large, combined drone-and-missile raids Russia has mastered. Waves of cheap drones and decoys drain expensive missile stockpiles while providing cover for cruise and ballistic missiles, overwhelming even the most advanced systems through sheer volume and complexity. Ukraine offers a battle-proven, perpetually refined architecture to build a resilient, affordable territorial air defence shield. This includes distributed sensor networks fused into a single command platform for semi-automated threat assessment, procedures managing hundreds of mobile fire groups, and technical solutions for targeting and kinetic intercept. Critically, it includes co-production and deployment of an effective, low-cost drone-on-drone intercept capability. This working system was explicitly built against the world's most intense aerial threat.

Unmanned ASW / AUW at Sea

The maritime domain is undergoing the same transformation. The era of a small number of large, expensive surface combatants controlling littoral zones is giving way to swarms of low-cost unmanned systems. Ukraine, “a country without navy”, has nonetheless severely degraded a major naval force and now is the global leader in this form of warfare. It can offer Norway combat-proven USV and UAV platforms to generate mass in strike and mine countermeasures, the fleet management software and command architecture to operate them, and the doctrine for sea denial, coastal defence, and maritime air defence. This provides a cost-effective way to hold large sea areas at risk, at a fraction of the cost of conventional naval platforms.

Military Medical Services

Warfare 5.0 has created medical challenges that did not exist before, and Ukraine has built practical expertise to address them. Conventional medical evacuation is almost impossible under persistent drone surveillance and attack. Ukraine’s solution centers on UGV-based evacuation procedures and a refined pre-hospital care system that has demonstrated strong results in reducing casualties. The offer covers the full chain: from point of injury through stabilization to field hospital, including equipment use, transport, medical procedures adapted to drone-caused injury patterns, and training programs for medics and evacuation crews. Ukraine can also grant access to its experience in bionic prosthetics as an area that has advanced rapidly out of necessity, with companies such as Esper Bionics and Allbionics at the global forefront, and rehabilitation centers like Superhumans setting high professional standards.

Logistics

On the modern battlefield, the advantage goes to whoever has the stronger engineering capability and more resilient logistics. The ability to adapt and replenish hardware in real time is now a core operational requirement. Ukraine has built this capacity through brigade-level R&D hubs, DefTech accelerators, and mobile repair stations. It can help partners embed the same: setting up facilities, technical intelligence processes, assembly lines, and training personnel in mechanical, technical, and software skills. Mobile repair teams can also be deployed forward to maintain reconnaissance, EW, and strike systems directly in the operational zone. Last-mile logistics is equally critical. Delivering supplies by manned vehicle into active combat zones is already untenable under constant drone surveillance. Ukraine can help deploy thousands of logistics drones and UGVs across selected partner brigades to sustain dispersed operations under drone threat. The most important transfer here is not just the platforms, but the tactics, techniques, and training to make the capability effective when it is actually needed.

Military-Industrial Symbiosis

The separation between military requirements and industrial production is no longer viable. In modern warfare they must function as one. Direct, immediate feedback between the battlefield operator and the developer or production line is now a necessity. Ukraine has built working models for this: decentralized procurement structures, secure digital marketplace platforms, and public-private ecosystems where industry responds to battlefield demand in real time. This expertise can be available to partners.

3.2 Not Starting From Scratch

The specific value of this report is in giving strategic shape and priority to the nascent Norway – Ukraine defence partnership that already exists in embryonic form. Since October 2025, Ukraine and Norway have run Brave-Norway, a bilateral grant program pairing Ukraine's Brave1 defence innovation cluster with Norwegian startups on drone technology, AI-enabled defence tools, and tactical innovation. In April 2026, President Zelensky and Prime Minister Støre signed a Joint Declaration on Enhanced Defence and Security Cooperation, with air defence, unmanned systems, electronic warfare, maritime security, and logistics as the key priorities, and specifically flagging integrated, multi-layered air and missile defence as a joint focus (absolutely in line with the threat profile portrayed in Part 1). Joint production of Ukrainian-designed mid-strike drones was announced by both sides. Ukraine's Defence Procurement Agency and Norway's Defence Materiel Agency (NDMA) have moved from ad hoc contact to standing working groups, exchanging intelligence, coordinating joint R&D, and training Ukrainian procurement officials. On the industrial side, Radionor declared plans while Kongsberg already actually opened an office in Kyiv in 2025, with partnership agreements signed with two Ukrainian companies.

In other words, the right direction is already set. It is time to elevate this cooperation to the next stage. The paradigm shift in warfare necessitates a change in the cooperation model, moving from sporadic transactions to systemic defence-industry cooperation and joint capability development.

Ukraine's approach to this modern warfare including battle management, ISR, tactical kill-web, AI- and drone-powered middle - and deepstrike operations, electronic warfare, special maritime operations, air defence, frontline counter drone capacity, logistics, fortification, MEDEVAC, deception and forward R&D and repair capacity, is an integrated package of combat effectiveness that cannot be mechanically split into discrete pieces. This is the system – still pending optimization, urged for permanent adaptation under extreme stress of attrition warfare stress – but working for modern warfare.

This is the opportunity for Norway, and it is right now. NATO enemies are already drawing doctrinal, technological and capability generation blueprints from Russia. This applies not just to the military, but also to the industry that needs rethinking and shifting to match the "warfare smartphonization" trend, shifting from focus from limited numbers of high-end platforms toward scalable and cost-efficient attritable mass whose individual deficiencies are compensated by deeper embedding within digital (the 'Matrix') and algorithmic (the 'Terminator') contours.

The fastest, cheapest ways to close Norway's capability gaps and increase deterrence now are to import Ukrainian scale, speed, and doctrine in drones, counter-drone systems, electronic warfare, and distributed air defence; build coastal sea-denial capabilities with unmanned surface and aerial systems; protecting logistics with unmanned ground vehicles; and integrating Ukrainian technology and operational blueprints into partner capabilities.



[60] Norwegian University of Cooperation and Commerce, "Ukraine and Norway launch €20 million 'Brave-Norway' defence innovation program," Oct. 9, 2025 nucc.no/news/ukraine-and- norway-launch-eu20-million-brave-norway-defence-innovation-program .

[61] Office of the Prime Minister of Norway, "Norway and Ukraine to establish closer defence cooperation," Apr. 14, 2026 regjeringen.no/en/whats-new/norway-and-ukraine-to-establish-closer- defence-cooperation/id3156260/

[62] Kongsberg, "Kongsberg to develop missiles and drone boats in Ukraine," Jun. 22, 2025 kongsberg.com/news/news-archive/2025/kongsberg-to-develop-missiles-and-drone-boats-in-ukraine/

3.3. “Low-Hanging Fruit” in NO-UA Defence Partnership

C-UAS Capability for the Heimevernet

Norway’s Home Guard is planning a transformation into a nationwide distributed short-range air defence network. Ukraine can deliver a ready capability architecture encompassing tactical concepts and standard operating procedures (SOPs/TTPs), operator training programs, technical solutions, C2 instruments, and blueprints for integration with the NASAMS layer (see the Chapter 3.4 for detail).

The scale of the challenge for Norway was addressed in detail in Chapter 2.2., as the one even of a bigger scale than it is for Ukraine: Norwegian Home Guard (backed perhaps by Royal Air Force) would potentially need to counter Shahed-type drone mass in the sky above their land along with neutralizing a far larger, more difficult to track and intercept mass of small UAVs along their endless coastline.

This is where Norway, in our opinion, needs help most and where Ukraine is positioned to provide multi-vector strategic assistance.

An interesting fact is that while facing quite such a challenging situation in the domain, Norwegian industry right now builds C-UAS for a different country – Poland.

This may set a useful precedent for reciprocal cooperation: while Norway helps to build C-UAS for Poland, Ukraine may help to build it for Norway.

On 30 January 2026, Kongsberg and Poland’s state defence group PGZ signed a NOK 16 billion contract for Poland’s SAN counter-UAS program: eighteen modules, each built around multiple firing platoons of PROTECTOR-based turrets combining guns, guided rockets and missiles under a single sensor-fused command layer, forming what is expected as an integrated anti-drone wall of roughly 700 vehicles, sensors and effectors, with initial operational capability targeted before the end of 2026. It is explicitly designed around lessons from Ukraine on drone saturation and electronic warfare[63].

This means, in this particular part of the counter-drone architecture, Norway does not need to invent or import a solution; it just needs to buy, for its own territory, what its own defence industry is already delivering to Poland at scale.

Now, what Kongsberg’s hardware cannot supply on its own and where Ukraine may lend a helping hand, includes: battle-tested blueprints for distributed mobile fire groups, with a training pipeline built to bring an operator to useful engagement effectiveness in weeks; AI-powered sensor fusion and terminal guidance technical solutions, trained on combat data, for making a small number of people supervise a large distributed C-UAS grid; missing technical puzzles such as interceptor drone layer, pervasive short-range EW layer, pervasive ISR layer for drone motherships detection and denial from the sea; physical protection and interception layer from the EW-immune small drones; first medical assistance tuned against drone-caused injuries; a decoy, spoofing and deception layer which grows enormously critical given vastness of objects

Oslo needs to protect; an acoustic sensing layer, complementing radar and electro-optical coverage; decentralised civilian alert layer to supplement Norway’s current model.

Concluding guideline: counterdrone defence is Norway's most pressing, immediate need. Therefore, rather than wait for EDDI's 2027 target (whose timely realization and ultimate efficiency is a question), Norway has a direct interest in building a faster capability pooling pipeline with Ukraine. There is no need to wait until Norway finds itself in the position that countries in the Near East faced in 2026, when the same pipeline would still have to be installed, only under fire.

Protection of Critical Infrastructure in the Maritime Domain

Norway is acutely vulnerable to drone attacks on its naval bases and offshore oil and gas infrastructure. Ukraine possesses the doctrinal expertise and technological solutions to build layered sensing and active defences against surface, and subsurface drone threats, as the prime carrier of these threats to the Russian Black Sea Fleet.

Robotised Deterrence for Finnmark

Norway needs a capability to deny Russia's potential, while low-probability disturbing attempts on the ground in Finnmark. Ukraine engaged in a kind of warfare having its center of gravity in the land domain has a primary set of assets to offer here, to give the Norwegian army a fast track to build unmanned capabilities critical to make a modern Ukrainian mechanised or assault brigade combat-effective with a fraction of the manpower a Cold War-era formation would have needed, including a kill-chain built on 24/7 drone-powered ISR and tactical precision strike; digital battle management tying it together; long-range fires for massing effect at range; robotized last-mile logistics and casualty evacuation; unmanned remote mining and demining; modular fortification designed against drones strike rather than artillery alone; pre-positioned minefields and non-explosive barriers; autonomous robotic positions.

Closing the Ballistic Gap Together

Norway has no defence at all against an Iskander-M ballistic missile, which in contrast to Oniks or Zirkon super/hypersonics Russia is capable of producing at the industrial scale. Since recently, neither has Ukraine. While national procurement management is going to deliver a technical decision by spring 2027, the current global deficit of this hard-to-stockpile asset contrasted to the growing demand may turn into a situation where there will be nothing to choose (in the needed volume). Ukraine's Fire Point develops the FP-7.x Freya interceptor system as an explicitly lower-cost, higher-volume alternative to Patriot (estimated at roughly $700,000 to $1.2 million per round). Norway is already a member of the Anti-Ballistic Missile Coalition committed to accelerating Freya toward a first live interception targeted for mid-2027. One needs to be honest: the success is far from guaranteed, and there are certain insider rumours the resulting system may have PAC-2 performance rather than PAC-3 (which is not sufficient against the modern-generation Iskander). But the need is pressing, and with Norwegian enhanced funding and deep technical expertise in networked fire control architecture, data fusion, and NATO tactical data link integration (domains where Norway's two-decade NASAMS program has accumulated unmatched institutional knowledge).

[63] Kongsberg, "KONGSBERG wins NOK 16 billion contract to deliver counter-UAS solutions in Poland," Jan. 30, 2026 kongsberg.com/news/news-archive/2026/kongsberg-wins-nok-16-billion- contract-to-deliver-counter-uas-solutions-in-poland

[64] This least is not exhaustive.

Bringing Mime Program to the C7ISR

The profile of Mime program and its presumable architecture and functionality distinctions from Ukrainian Delta, making the room for fruitful cooperation, were addressed in Chapter 2.7. in sufficient detail. The room exists for sure, as by Norway's own assessment, C2 at the operational-tactical level is one of its most critical bottlenecks, while the Mime/THOR C2 suite will not be ready until 2030.

The cooperation with Ukraine can expedite the process and, most critically, ensure that the accomplished C2 concept will not lack architecture and features to be fully relevant to modern robotized battle management. Delta has mature fleet management and autonomous effects layers built on the assumption that connectivity will be cut rather than secured under heavy EW of the modern battlefield. Along with offering Delta as an integration reference, cooperation may also include testing FACNAV UxS manned-unmanned teaming against a real mass-scale unmanned fight Ukraine may emulate (more than fifty drones simultaneously).

Technically, two forms of cooperation are available. The first is structured technical access to Delta itself, including modules such as Monitor, Vezha and Target Hub, or the underlying architecture principles (CoT, MIP, NFFI, ADatP-34 and STANAG 4586), as an integration reference for Mime program. The second is direct consulting and advisory support for Norway's C2 digital architecture development, to ensure its further evolution toward a full-fledged battle management universe with full functionality set needed in C7ISR architecture (managing massive unmanned fleets with AI-assisted cognition support for human decision-making).

All-Weather ISR Capability

An important C2 element is space. Norway is a leader in SAR intelligence (ICEYE Norway, KSAT) and space infrastructure (Andøya Space Center). Ukraine seeks expanded access to SAR data, automated processing algorithms, KSAT ground infrastructure, and joint development of reconnaissance payloads — offering Norway in return the most cutting edge options to capitalize on those space capabilities for Norway's own defence needs.

For instance (one example among many) Ukraine possesses an EW-resistant, GNSS-independent reconnaissance UAV technology already validated for deep operational and tactical-level missions 50–100 km behind the line of contact, with a combat-proven anti-icing configuration capable of sustained flight inside cloud and icing conditions that ground most tactical drones outright; icing remains one of the most common causes of small UAV loss in cold, wet climates precisely because few airframes carry the power margin for electrothermal de-icing. Norway's SAR assets — ICEYE Norway's satellite constellation and KSAT's ground-station network — solve the other half of a problem: a platform flying inside cloud cover has no usable picture from its own electro-optical payload, but SAR imagery is generated independently of cloud cover, daylight, or camouflage discipline, since it images by radar return rather than reflected light and is materially harder to defeat with visual concealment.

Paired together, the two capabilities produce a force-multiplier: the reconnaissance profile of a platform that can persist inside any weather and under interrupted connectivity. Norway's own operating environment – persistent Arctic and North Sea cloud cover, long periods of low light, terrain is close to an ideal proving ground for this solution, making it a natural joint G2G project.

Joint Development of Autonomous Surface and Underwater Technologies

Ukraine can offer a live combat testing environment for Norwegian underwater drone programs such as SMAUG, HUGIN, and MUNIN, as well as synergy in adaptation of Norwegian cutting-edge civil underwater systems for military applications, by extending the successful Brave-Norway cooperation framework into the subsurface domain. Ukraine may also offer collaboration on building Norwegian capability for providing the Royal Navy with attritable unmanned naval mass for a prolonged war of attrition, that necessitates having access to cheap and simple, easily replenishable, but effective for their mission COTS-built one-way intelligence, minelaying and strike platforms, along with reusable solutions with premium sensory payload in which Norway already holds a leading position. In turn, Ukraine needs Norwegian hydroacoustic modules, sensor payloads, and navigation systems for its high-end underwater drone fleet for closing critical capability gaps in Ukraine's campaign to degrade the Russian Black Sea Fleet.

The same cooperation applies to the unmanned surface combatants, where Ukraine has a considerably greater extent of capability maturity. Oslo seems currently to underestimate the significance of this drone class, while it can become a perfect force multiplier reducing risks and releasing burden from Royal Navy's manned assets in anti-surface and mine warfare missions.

A "Drone Line" for Norway

Norway's basic geographic problem is a very long coastline and land border relative to a small population and a far smaller standing force. This problem is structural and cannot be conclusively solved by increasing personnel within affordable limits. Ukraine's specific offer here is to help Norway build a highly automated permanent robotic zone of remote monitoring and fire control with embedded agentic AI for autonomy under supervision of a reasonably limited high-level operators, along the coastline and border, combining networked ground sensors, reconnaissance and strike UAVs, and remote mining systems into defined kill zones. Properly built, this directly offsets the personnel constraint and gives Norway a hedge against the risks of surprise unprovoked escalation in the littoral areas and on the ground in Finnmark. Ukraine holds unique expertise and proven solutions for establishing such a system.

R&D Cooperation with the Norwegian Defence Research Establishment

FFI operates with an annual budget exceeding €270 million and a staff of over 800 scientists and engineers. It serves as the critical bridge between academia, industry, and the armed forces, and is the custodian of Norway's defence technology know-how. Ukraine requires deepened cooperation in autonomous air defence algorithms, multi-sensor fusion, underwater acoustics, strategic electronic warfare, and ballistics; on a three-to-five-year horizon, also in AGI, space technologies, hypersonics, and quantum systems. Its offer is in turn to provide an ecosystem for systemic immediate combat validation and adaptation of FFI solutions, which would expedite their development and maturation cycles radically. For that purpose, FFI should open its branch in Ukraine to launch rapid-cycle prototyping and field testing for Norwegian manufacturers in a real high-intensity operational environment.

Joint Development and Production of Medium and Long-Range Reconnaissance and Strike UAVs

Kongsberg, Radionor Communications, and Maritime Robotics collectively hold world-class competencies in this domain. Ukraine needs the supply of production-scale communications modules – not prototypes – for deep-strike operations, offering Norway in return live combat validation under the toughest electronic warfare conditions in the world as well as joint scaling to meet Norway's own defence requirements against the prospective need to counter and neutralize hundreds of Russian USV motherships across the vastness of the Barents and Norwegian Seas. Ukraine brings a powerful tactical innovation ecosystem for unmanned platforms; Norway can contribute Kongsberg's engineering pedigree and a cluster of high-technology start-ups with competencies in larger platforms optimised for extended endurance and low observability. Joint development and production of long-range, EW-resilient autonomous UAVs represents a natural convergence of these capabilities.

Joint Development of Seismo-Acoustic Battlefield Monitoring System

NORSAR and FFI possess unique competencies in seismic monitoring, developed originally for nuclear test verification, but directly applicable to the detection of artillery positions, armoured vehicle movement, underground tunnels, and enemy field engineering activity. Ukraine faces persistent challenges in locating concealed artillery positions and subsurface fortifications, and requires these systems for integration into its existing signals intelligence network.

Joint Program on Insensitive Munitions

Norway is among the world leaders in the development of insensitive explosives – materials that will not detonate when struck by bullets, fragments, or fire. This technology has the potential to radically improve the survivability of Ukraine's armoured vehicles, ammunition depots, and logistics chain while providing Norway with critical lessons and blueprints for its Army operational security. A joint program with Chemring Nobel on licensed production in Ukraine is recommended.

3.4 From Programs to Partnership

Every proposal in this paper already has or may easily find a foothold in bilateral instruments established in 2025-2026. The key practical recommendation this report makes is hence not to create new architecture, but to deliberately widen and formalize what already exists into a standing Ukrainian-Norwegian strategic defence partnership with a clear vision of common threat picture and common total defence approach (formalized in Norway, implemented in Ukraine) and mutually reinforcing lines of effort transcending separate R&D, industrial or experience sharing initiative into what be called joint capability development framework. This framework would aim to address exactly the "missing pieces" of both Norway's Totalforsvaret and Ukraine's active defence amidst prolonged war for existence in attrition warfare – as both sides have strategic value to offer each other.

Conclusion

Norway's dilemma is not about skepticism over whether Moscow will attack; it is about whether it is fully ready given – even under a low-probability scenario – it does. The "Battle of Norway" scenario sketched in this paper does not require Russian troops on Norwegian soil, nor does it require Oslo to lose a symmetric fight in the air or at the sea, it is well equipped to win. It requires only that Russia exploits the "loopholes" having emerged with warfare paradigm shift. These gaps are invisible to peaceful nations of Europe just because their mindset did not yet adapt to the new reality, not being urged by wartime existential pressure. But they are fully visible to Russia which not just fully identified those new capability requirements, but pioneered and mastered them along with Ukraine. Moreover, even in most conventional capabilities, Norway's own clock, running on a 2029–2036 modernization timeline, may close after Moscow's clock, running on a shrinking economic and demographic runway.

Norway's advantage was never going to come from matching Russian mass "rifle for rifle" – and "drone for drone" in our case. A country of five million people spread across a hundred thousand kilometres of coastline cannot outcrew an adversary willing to burn manpower and waste hardware with little regard for cost or sustainability. Its advantage lies in the same direction as its economy, its industry and its society point – qualitative advantage over quantitative superiority, provided by superior technology and higher organizational culture.

This time, however, the stars of warfare seem aligned the way making reliance on attritable mass, rather than on a few big-and-beautiful platforms, inevitable in certain domains. Norway can certainly produce that cheap mass of hardware leveraging its brilliant defence industry if it needs to. But this is not the Achilles' heel – the true one is in timely understanding that drone warfare is not about drones but about a complex architecture making their effective deployment possible, and this architecture does need to be built in time. Moreover, it requires a giant pool of trained, technically competent combat and support operators. The time is pressing, and Ukraine offers doctrinal blueprints and technological frameworks that work, for Norway to be in time.



The Battle of Norway. Memories of the Future

Addendum

Intro

“Come in,” I heard.

An elderly man with grey hair stood with his back to me, facing the wide window, watching the panorama of the embankment as twilight was rapidly settling over it. Somewhere in the distance an autonomous air taxi flashed past.

I greeted him, and only then did he turn. When he saw it was me, he frowned, though he tried not to show it. I knew this would not be an easy conversation for him. Only after numerous attempts through friends, and friends of friends, had I managed to persuade this retired Norwegian general to grant me an interview. Until then he had categorically refused to revisit those memories – those few months that buried the old Europe and very nearly tested NATO to its limits, opening the page onto an entirely new reality: a sobering one, filled with the realization that the old sense of a safe world would not return for a long time.

“So, you say you’re writing a book about the Third World War?” he asked with restrained politeness. “And why would you want to do that?”

“Well, someone has to do it sooner or later,” I replied with a polite smile, carefully stripped of any intrusive warmth.

“Before I go on, I want to say this plainly. If you are looking for sensational material to impress your readers, you will not find much of it here. I have no drama to give you. What I have is an honest account of what happened, in the order it happened, told as plainly as I can manage. If your book needs excitement, go to Vilnius. Or Taipei. They had more of it than we did. You should understand we were not at the centre of it. We were on the periphery — a periphery that mattered a great deal to the whole theatre, but a periphery all the same. What happened here had effects but was not, however, the way people imagine a war sounds. Keep that in mind as I go on”.

“It’s ok. I need a full picture”

“Then take a seat. This conversation won’t be short.”

The account that follows was recorded from this general’s own words, almost verbatim. At the time of the events in question he was not yet a general, but only a senior officer at the Joint Headquarters of the Norwegian Armed Forces in Reitan, observing everything that unfolded from a bird’s-eye view. To some it may read like a dry military report – but that was simply the manner of his storytelling: militarily laconic, free of pathos or emotion, Nordic in its sobriety, with a distinct undertone of clarity.

June 12, 2048

The Denied War

We used to argue about when it started exactly, in the small hours after the official reports had already been written, filed, and were being quietly disputed by the people who had actually been there. Certainly, retrospectively we all recollected those signs that could be read as an open book – but here is what made the critical difference: NATO intelligence in 2026–2027 was not blind to them, and we were not passive observers.

Russian fishing boats, using 5-day stay exceptions for Kirkenes, Båtsfjord, and Tromsø ports, idling a little too long over cable routes north of the Lofoten wall, had been flagged by satellite imagery and signals intelligence within days of each occurrence. We knew exactly which trawlers were doing reconnaissance, and we shared that information with Washington and London in real time. The small unknown drones passing over Melkøya, Equinor platforms, and the rest of the energy coast that had become so routine our own duty officers logged as incidents – these were no longer accepted as background noise, but rather as part of a coherent pattern that was being actively tracked and analyzed. The cyber intrusions we found, patched, and then wondered whether we had found all of the dormant cyber agents – yes, we found most of them, because we had been running red-team exercises with the Americans and British for years specifically against this threat, and our defences were correspondingly hardened. Olenya Bay, that flat grey inlet barely a hundred kilometres from our own border, where GUGI kept its purpose-built motherships, waiting with a quiet, deliberate patience – we watched them, we catalogued them, and we made sure our NATO liaisons understood exactly what they were seeing. That one spring, two of those submarines came north together – an Akula running loud and known, a decoy playing itself in the open, while a pair of deep-research boats behind it went quiet and worked a stretch of seabed for over a month. But this time we detected them early. Our Triton-class Poseidon P-8 maritime patrol aircraft, operating out of Evenes airport at Harstad, picked up their acoustic signatures. The British and Norwegian navies coordinated to force their retreat before they could complete their deep-sea cable mapping work. It was not a close call – it was a successful interdiction that prevented the enemy from obtaining final targeting data. We had called it correctly, and we had acted on it correctly, stopping the reconnaissance in its tracks rather than congratulating ourselves after the fact.

In hindsight, it turned out to be exactly what we thought: a fitting, the last piece of reconnaissance filed away with everything gathered in the years before it – the seabed charts of every cable and pipeline corridor between our platforms and the continent; the detailed mapping of the entire offshore energy infrastructure; the target lists and catalogues of every major base, depot, and storage facility; the industrial sites, power stations, substations, and critical energy nodes along the coast and inland, all of it long observed, measured, and recorded with the same patient, methodical thoroughness. But we had already filed it ourselves and handed it to SACEUR at NATO's Supreme Headquarters. The intelligence was flowing upward. The warnings were being heard.

None of it looked like war. That was the design. A war that begins with a declaration is a war you are to answer immediately, whether you want it or you don't. A war that begins as noise you've already agreed to ignore is a war that always finds you still in bed – vulnerable, half-asleep, and already behind. Except we were not asleep, and we were not behind.

The Trap Snaps Shut

At some point everything from Russia's side we had used to live with simply thickened. Not enough to alarm. That was the discipline of it, and it was better discipline than most of our own contingency plans had given the other side credit for. The cable, drone and cyber incidents kept coming, but no faster than before, and no less deniable: an anchor here, a trawl net there, a tanker with an all-Russian crew and papers that were technically in order. Baltic Sentry, and from that February, Arctic Sentry, gave us a presence in the north we hadn't had in a generation — more force but primarily more eyes, more of the recognised air and surface picture flowing into Sørreisa than at any point since the Cold War. And it worked exactly as advertised: it raised the price of sabotage and thinned its frequency. What it could not do, because it was never built to, was to prevent a surprise mass strike of those same deniable assets. There was a movement near Storskog, with a few companies with engineering vehicles delivering modular concrete fortifications in plain sight. The ground there is almost impossible to dig (rock and permafrost leave little choice). We assessed it, rightly as it turned out, as low in itself and possibly a rehearsal for distraction rather than an axis of real intent. What we underweighted was how little it would matter whether we read it correctly. A demonstrative move you have already decided is not the main effort still costs you attention, and attention was the resource in shortest supply on our side of the board. To jump ahead a bit, this was not really a war against Norway. Norway was the flank, not the front. The place where things had really gone crazy was the Baltic, where Moscow expected the fastest and most humiliating win the Alliance's cohesion could suffer at the lowest cost. That is where the mass of Russian reconnaissance and strike went. People who ask me about it always ask the same question, more or less in these words: if Vilnius and Riga were the real prize, why bother with us at all? We were not, in ourselves, worth much to them. What ran under us and past us was. More than half of the gas keeping this continent's lights on through the winter came down our pipelines. Sever what you can reach of that, or simply make us spend every hour preventing reaching it, and you have done something to Berlin and to Warsaw and to London without ever pointing a gun in their direction. The Alliance's weak point was its cables and its pipes, sitting in shallow water, and offshore energy production facilities whose lights amuse evening promenade walkers from the distance

This was our luck: the missile brigades that could genuinely have reached us if redeployed forward – Luga's, Kursk's – held instead against that theatre where NATO's own force density was thickest. But that was our bad as well, as our neighbours were busy there and had very small room to lend a helping hand to our contest in the air and at sea. Sweden and Finland, still new enough to the Alliance to feel the weight of first commitments, gave the bulk of what they could spare to the enhanced Forward Presence battlegroups and to the Baltic Sea itself – and that was right, but this meant, in practice, that the reinforcement and the attention we might once have assumed from next door simply weren't there. We had allies but we did not, in the north, have them with us in the same way as the army of Gondor had Theoden, the king of Rohan, with them near Minas Tirith.

Russians wanted the Baltics, but they could not leave us alone, of course. They needed to disrupt us comprehensively, cheaply, and with effects that went well past our own coastline – our communications, energy, all that stuff. They did not need to occupy Norway or beat its Army, of course – just to make a deadly wound to German industry, British and Dutch energy security, Polish gas storage, and NATO's ability to move troops.

The Doomsday

It came in the last dark of the polar night, which in hindsight was its own kind of message: strike a country that already lives eighteen hours in shadow, when a blackout doesn't announce itself against a bright sky.

The caches went first, having been sitting for months in hire cabins along the Helgeland coast, in the false bottoms of container units at quay-side yards, aboard shadow fleet hulls already loitering with legitimate cargo, and aboard a scattering of small unmanned surface craft that had been drifting, dormant, thoroughly disguised both visually and dormant to be invisible in RF spectrum, logged in our own tracking as fishing debris or research buoys nobody thought worth a second query. On the signal, they opened. What came out were small drones, fixed-wings from tanker and copters from USVs, hundreds of them, some of them autonomous, others – cued off a private, encrypted positioning layer Moscow had spent three years building for exactly this hour, precisely because it did not need our GPS, our Galileo, or anyone's goodwill to find a target once satellite navigation itself went to war. But here is where the first complication emerged: the encrypted positioning layer Russia had built was real, and yes, it worked. However, the drones themselves – particularly those held in cold storage for months in Arctic conditions – suffered from battery degradation that reduced effective range and endurance across the full swarm. Many units that launched had reduced operational windows by thirty to forty percent compared to what Moscow's planners had modeled. The electronic warfare countermeasures we deployed at critical sites – Kårstø, Kollsnes, the military installations – were not perfect, but they were effective enough to degrade targeting accuracy across the board. And GLONASS coverage over Norway did experience disruption, but not in the way that mattered most. It covered civilian and commercial channels. Civil aviation over the North Sea and the High North was grounded or diverted within the hour – that part was correct. Maritime navigation lost its fix in the sectors that mattered most. And the search-and-rescue crews who would, on any other night, be the last resort to people in a coastal emergency found themselves flying by dead reckoning over black water, at the exact hour the country needed them flying with certainty.

But military GPS receivers in NATO aircraft and ships operate on encrypted military M-code channels. GLONASS denial did not touch those. Our F-35s never lost their navigation fix. The British and Norwegian naval systems continued operating under full precision. This enormous disruption in the civilian sphere profoundly shocked people wherever they observed that hell, and still – even a few thousands of prepositioned drones were not enough to destroy Norway's infrastructure and energy sector, redundant and distributed along one hundred thousand kilometers. They had to choose, and it seemed Russian made target prioritization lists far in advance. Kårstø, Kollsnes and Nyhamna, the three processing hubs that between them handle most of what leaves the Norwegian shelf as gas, Kårstø alone the largest single point for natural gas liquids on the continent, each absorbed strikes against their soft, above-ground elements: switchyards, flare systems, the outdoor manifolds no engineer had ever been asked to armour, because armouring them had never once looked like the better use of money. All of the three experienced significant damage to surface systems and production was disrupted for weeks. Kårstø alone saw output drop by two-thirds for a month and a half. A continent watched its gas price peak. Sture and Mongstad took the same treatment on the oil side. The onshore landfalls of Europipe and Langeled – the point where an 8,800-kilometre subsea network most people

had never had reason to think about finally comes ashore and becomes a building you could put a drone through the window of — turned out to be exactly as exposed as that description suggests. Andøya's spaceport pads, new enough that nobody had yet finished arguing over how to defend them, took the same casual treatment.

The undersea reach was slower to register and harder to repair. GUGI teams, that conducted preparations for this D-Day for many months, operated the most upgraded versions of underwater autonomous vessels designed specifically for the deepsea sabotage operations. This time they went a more complex pathway by employing unmanned underwater motherships which in turn deployed sabotage platforms, along with numerous underwater decoys, to make the task most complicated for our Poseidons. They deployed and worked two of the interconnectors carrying Norwegian power toward the continent, and a stretch of the fibre serving the Svalbard routes and the North Sea crossings — cables most of us could not have named a decade earlier, and that European telecoms firms could, by then, price to the hour of downtime. Offshore, Troll and Ormen Lange absorbed harassment against support vessels and surface systems rather than their subsea templates, which was itself a kind of answer: the pieces Moscow could reach cheaply, it hit; the ones it could only reach at real cost, it mostly left alone, saving that cost for somewhere it would matter more.

It mattered more, by our count, twice. Kårstø's core export train, the one quite invulnerable to small drone mosquito bites, took a strike of the small handful of Zircons Moscow was willing to spend on a target outside the Baltic at all – a single node, hit hard enough to guarantee the result, cost the European NGL market weeks it could not make up on short notice from anywhere else. The Tromsø Network Operations Centre took a related but cheaper blow at a dish field at Platåberget above Longyearbyen, which the drones – and, we later confirmed, a patient cyber effort – had already worried for weeks, and which was now finished with a bulk of deepstrike Shaheds. Russia had flagged the site as dual-use in its own statements years before, which told us clearly enough how it intended to treat it. The single control room in Tromsø that ran the whole commercial ground network, Svalbard included, received a cruise missile blow as well. But here we must be precise: a single Kalibr, yes, worth more hit precisely than hit in a hurry. It took one cruise missile, and it got through only because NASAMS's attention was, by then, fully spent elsewhere – we had limited air-defence batteries and they were distributed across the length of the country, not concentrated in any one place where a determined effort could overwhelm them. The military ground stations at Eggemoen and above Andøya – smaller, less networked outward, better dispersed – absorbed probing and held.

Melkøya was its own case. Every other major terminal sits far enough south that Iskander's 500-kilometre reach from Kola cannot touch it at all. Hammerfest cannot say the same. It is Norway's only large liquefaction plant, the closest one to Russia by a wide margin. Here is what actually happened: Two Iskander-M systems fired at Melkøya from positions near Olenya. At these ranges – approximately 370 kilometers – the missiles require either real-time terminal guidance through satellite data-link or AWACS support. Russia had neither: our F-35s had achieved air superiority in the Norwegian Sea, and their own aerial platforms had been driven back. The first Iskander was guided by inertial navigation alone in its terminal phase; it impacted forty kilometers from the target, destroying a secondary facility. The second Iskander succeeded in hitting a storage tank and auxiliary systems.

Production at Melkøya dropped significantly – perhaps sixty to seventy percent – but the core liquefaction train, buried underground and hardened, remained functional. The damage was real and expensive, but it was not the destruction of Europe's northernmost LNG plant.

The Finnmark and Troms coast suffered heavily as well, as mobile Iskander TEMs reached the radar sites and dispersed positions strung along the north, then withdrawing before they could be reached by our Air Force.

The logistics arm fared no better, and here the intent to reach past us was least disguised. Narvik, Trondheim, Bodø and Tromsø, and the approaches to Haakonsvern – the ports through which any serious reinforcement north and east has to pass – absorbed strikes against cranes, fuel bunkering and rail-yard switching. Evenes and Ørland took drone raids against radar and above-ground stores that never came close to grounding the F-35 fleet, but cost tempo, and tempo was the actual target. North of Narvik, the single rail line to Sweden – Ofotbanen, a hundred-odd kilometres of track with almost no alternative routing – became the target of meshed Shahed drones returning to the same stretch of tunnel and track every time a repair crew cleared it, the kind of persistent, cheap interdiction. A standing threat was a lockdown that lasted as long as anyone's attention stayed on it – which, that winter, turned out to be most of it. Road transport along E6 provided some relief, but slower and more expensive. The E6 further south, more redundant, took the same treatment more lightly and coped better.

Most of what keeps Norway's economy running – the export terminals, the processing footprints further south, the shipyards, the depots – sits beyond five hundred kilometres of the Kola launch lines, which Iskanders cannot reach. Moscow could not use its ordinary cruise missiles as well since our NASAMS did their job quite well. So the enemy used Shahed-type drones Geran and Gerbera, cheap enough to send in the hundreds, and they were the actual weapons that did the actual damage to Kårstø, Kollsnes, Nyhamna and the rest of it.

Not everything gave way to the enemy. The hardened prepositioning caves in Trøndelag, cut deep enough into rock that neither drone nor missile was ever a serious threat to what they held, came through the autumn essentially untouched – equipment sitting exactly where it had always sat, ready the moment anyone could reach it. That last clause did the damage instead: the roads and the single rail line that would have carried it forward were exactly what had just been cut. The vault held. The current running to it did not.

That was a long night, yeah. By the time the sun came up on a morning that, this far north, was really only a paler grey, nothing decisive had happened. That was also the design. It was to make Norway spend the following weeks discovering what the damage had happened, and why its shields were broken in so many places, and why it hurt so much in many places at once, and what is to be the response to the nuclear power, while NATO's decision-making mechanisms moved slowly through their own nine circles of hell – not because anyone was paralyzed, but because the main theater was the Baltic, where things were far more dire, and every senior commander was calculating how to avoid losing Estonia while responding to what had happened to us in the north. We were not forgotten. We were not abandoned. But we were not the center of gravity either.

Where the Shell Held

And yet, bless it, not everything Moscow tried in those first days worked. They were the return on three decades of a fairly specific bet on precision, reach, and the same kind of quiet undersea patience Russia itself had always relied on.

The bet paid, and it did not pay. Northern Fleet aviation and surface combatants failed to close the range needed to fire their missile weapons, visible and reachable Sørreisa outward, with F-35s eagles of Ørland and Evenes having reached a couple of Gorshkov's. The remaining frigates and corvettes of the enemy that came forward to screen the effort were held off at distances that made what they carried irrelevant.

Beneath the surface the story took longer to tell but ended the same way: having recovered from the initial shock, the Royal Air Force fighters razed GUGI base to the ground, while a P-8 crew worked a familiar stretch of the Barents picked up a contact that behaved like a Yasen-M, tracked it patiently for the better part of a day without forcing an engagement, and handed the problem to a British submarine that could finish it. A full Russian push into the Norwegian and Barents Seas never happened and, to tell the truth, it looks like it was never planned as Moscow recognized the realities.

There was a second, quieter kind of shell that held, and it was geography rather than steel: most of what actually keeps Norway's economy running — the export terminals, the processing footprints further south, the shipyards, the depots that feed the rest of the country — sit beyond five hundred kilometres of the Kola launch lines, which is Iskander-M's reach and no further. It is not an accident that the missiles that could have hurt us worst — Kinzhal, Zircon — arrived in numbers too small to matter against that target set, husbanded instead for the handful of aims judged worth the scarcity. Distance, in this one respect, did what interceptors could not.

The Long Grey Water

What Moscow could not do – take the Barents and the Norwegian Sea by force, the way its own doctrine on some level still aspired to — it did not, in the end, need to do. It had watched Ukraine solve the same problem against a fleet built the old way, and it borrowed the solution rather than reinvent it: if you cannot win the sea in a battle, you make the sea unpleasant to use, indefinitely, with assets cheap enough to lose by the dozen.

So while Alliance's consultation processes passed through their protracted and difficult deliberations – focused primarily on the Baltic, where the real decision was being made – the acute phase gave way, over the following months, to something with no clean end, a standing condition rather than a campaign. Small, mesh-networked surface craft carrying drone swarms and mines, a meaningful share of them running on remote or autonomy guidance immune to anything we could jam (and we actually had nothing to jam with), worked patrols out of the Kola bases and the Barents in slow rotations: laying mines at Vestfjorden's mouth, along the Andøya–Bodø–Tromsø approaches, out toward the Bear Island gap, and in the sea lanes feeding Narvik, Trondheim, Bodø and Tromsø, and the approaches to Haakonsvern — the harbours through which any serious allied reinforcement, or any answer to what threatened it, would have to pass — threatening or striking when a target of opportunity appeared. Norway's own counter-response — the helicopters and surface ships built to hunt exactly this kind of

thing – turned out, uncomfortably, to be well-shaped targets themselves for a slow, low, cheap adversary that a fast jet or a submarine was never tuned to fight.

What made the standing condition genuinely dangerous, rather than merely tiresome, was how massively Russians used Shahed-type drones and mothership USVs to carry and disperse countless aerial swarms over Norwegian territory and territorial waters, autonomously hunting for all that stands or moves as long as it fits in one of pre-programmed target category. Special USVs also used special short-range surface-to-air fire aimed specifically at the helicopters sent out to hunt them, while supersonic F-35s were totally unfit to engage such small targets.

We were at least in part that the command had, to its credit, made a timely preparation – to the extent it was possible to prepare in such a short space of time – and in close collaboration with Ukraine used a preceding couple of years to deploy counterdrone capabilities tuned against small strike drones, both electronic and kinetic, as well as made extensive counterdrone engineering of our infrastructural sites and roadways, and shotguns which each home guardian has mastered to use for shooting drones down. Otherwise, the damage would be incomparably far more dramatic.

***

“Well then,” the general said, lifting his eyes to meet mine. I understood without a word and gave a silent mental command to my AI agent to stop the transcription.

“I’m tired. Let’s continue tomorrow. We managed to pull through in the end, since we both sit here safe and sound – but it didn’t come easily. By the way, if there’s time, I’ll take you up to the Kola Republic — once a part of what used to be Russia. I’ll show you a few interesting places. Sites of combat glory, so to speak”.

Scan for more information: