United States Senate
Senate Foreign Relations Committee

Hearing on: "Sabotage in the Baltic Sea, Implications for European Security, and Lessons for the Indo-Pacific"

30 April 2026, 10:00-12:00 Hrs.
Dirksen Senate Office Building, Room 419
Washington, D.C.

Written Statement Document Package of:

Dr. Benjamin L. Schmitt

Senior Fellow, Department of Physics and Astronomy, Kleinman Center for Energy Policy, and Perry World House; University of Pennsylvania
Associate, Harvard-Ukrainian Research Institute, Harvard University
Senior Fellow, Democratic Resilience Program, Center for European Policy Analysis
Space Diplomacy Lab Co-Founder and Rethinking Diplomacy Fellow, Duke University
Term Member, Council on Foreign Relations

Thank you Chairman Risch, Ranking Member Shaheen, and Distinguished Members of the U.S. Senate Foreign Relations Committee. My name is Dr. Benjamin L. Schmitt, and I have previously served as European Energy Security Advisor at the U.S. Department of State. I'm now a Senior Fellow at the University of Pennsylvania, and the Center for European Policy Analysis, and I'm honored to speak before you all today.

The world is at war. We meet 1,525 days since the Putin regime unleashed its full-scale invasion of Ukraine. And now, this year, the Iranian regime has learned from Russia's air war in Ukraine and launched kinetic drone and missile strikes against the energy infrastructure of many of the United States' partners and allies in the Middle East.

For the first time in decades, these ground and air wars have spread across the global maritime domain – all with dire costs. The IRGC has fomented a global energy crisis by recklessly blockading the Strait of Hormuz, while its proxies in Yemen threaten to multiply the damage by resuming attacks in the Bab al-Mandab Strait.

For its part, the Kremlin continues to work overtime on the high seas, standing up a tanker "shadow fleet" to evade Transatlantic oil sanctions. Besides dodging Western trade restrictions, some of these tankers may be dual-use platforms for espionage and drone launches.

Meanwhile, there is another war being waged: a shadow war in Europe against energy and critical infrastructure undermining the security of NATO member states not only on land, but offshore, roiling the depths of the Barents and Baltic Seas. European partners have confidently attributed to Russia, attacks on such onshore facilities as rail and telecoms installations. The Kremlin's strategy includes

recruitment of non-Russian nationals – including Ukrainians – to damage critical infrastructure to sow panic and undermine support for Ukrainian victory across the West.

While attribution for onshore attacks has been common, technical and political challenges have remained for offshore sabotage attribution, despite data-driven evidence suggesting the Kremlin's role.

Unfortunately, our partners across the Indo-Pacific now face similar seabed subterfuge. There have been several instances of Taiwan's subsea cables being severed, suggesting sabotage carried out at the behest of the People's Republic of China.

The Senate needs to use today's hearing to catalyze further action that makes it clear to both Moscow and Beijing that their subsea sabotage sprees end here.

And while the Senate must drive the policy conversation, I believe academia has a role to play too. For three years, I have led the University of Pennsylvania's UNDERWATER MAYHEM research project, focused on analyzing how Russia and the PRC now brazenly conduct physical sabotage attacks against seabed energy and critical infrastructure across the NATO Alliance and beyond.

Four key case studies from our research include:

[1] Svalbard: My travel to the Norwegian island of Svalbard – just 400 miles from the North Pole – supported our ***assessment that it is highly probable*** that in January 2022, a Russian fishing trawler was responsible for severing a vital subsea fiber optic cable transmitting commercial satellite data from the SvalSAT ground station to the European mainland. Such commercial data would prove vital in Ukraine's defense just weeks later, suggesting this was part of a "shaping operation" before Russia's full-scale invasion.

[2] Nord Stream: Official attribution of the September 2022 Nord Stream 1 and 2 sabotage remains absent, and despite continued public debate, ***our research team assesses as probable that the Russian Federation was involved in this high-profile sabotage incident, and assess as improbable the media narrative that a "pro-Ukraine sailboat" launched from a marina next to a Nord Stream logistics hub was to blame.*** We arrived at this assessment after exhaustive open-source AIS and satellite data analysis, interviews with first responders and experts across Europe, and a technical counter-analysis of competing theories of the case. I also chartered a vessel from Denmark's island of Bornholm to travel to the blast site and gathered seabed sonar data in 2024.

[3] The Baltic Sea: I sailed on vessels offshore in the Gulf of Finland and the Central Baltic near the sites of several extended anchor drag incidents by Russia- and PRC-connected vessels all which crippled seabed installations, including the 2023 Balticconnector gas pipeline break, the 2024 C-Lion1 and BCS telecoms cable cuts, and the 2024 Estlink2 electricity cable cut. ***The circumstances of these incidents suggest sabotage, not accidents.***

[4] Taiwan: This month, I traveled to Taiwan near the site of the 2025 cut of the Trans-Pacific Express telecoms cable, which links Taiwan with the United States. I also visited locations close to the sites of the 2023 and 2025 cuts of telecoms cables linking Taiwan's Matsu and Penghu Islands to the main island of Taiwan. All of these incidents involved PRC linked vessels, and thanks to Taiwan's actions, a PRC captain is now sitting in a jail cell for sabotage. I also conducted research near the center of the Taiwan Strait itself, donning a wetsuit to view subsea cables running through a coral reef between the southern Penghu islands.

Senators, it's time to turn the tables on the Putin and Xi regimes and restore deterrence against maritime sabotage.

To this end, I leave you with three brief recommendations:

- The Senate should support the invocation of NATO's Article 4 consultative mechanisms by concerned Member States whenever there are sabotage incidents attributed to Russia or its agents, which is essential to solidify political and operational support to counter these threats.

- This Committee should revive the statutory sanctions against Nord Stream 1 and Nord Stream 2 that sunset in 2024 – key steps to ensure that no investor – American or otherwise – can work to resurrect these symbols of Russia's energy weaponization and strategic corruption.

- Congress should pass S. 3249, the comprehensive "Strategic Subsea Cables Act of 2026," and S. 2222 "The Critical Undersea Infrastructure Resilience Act of 2026," both that have been prudently passed by this Committee.

Through these actions, we can deter further Russian and Chinese sabotage, support our partners and allies worldwide, and make it clear to those that would propose otherwise: **there can NEVER again be a return to "business as usual" with regimes that continue to attack the physical foundations of our economy, prosperity, and freedom.**

Thank you for your time and I look forward to your questions.

Dr. Benjamin L. Schmitt, *Senior Fellow at the Department of Physics and Astronomy, Kleinman Center for Energy Policy, and Perry World House at the University of Pennsylvania*

NOTE: The below is a pre-print version of a forthcoming analytical publication that I have submitted to the ICDS-Tallinn Diplomaatia Magazine which will run in mid-May 2026 as a part of the Lennart Meri Conference in Tallinn, Estonia.

Europe's Energy Security Playbook

Nearly all Baltic Sea states have recognised and prepared to weather the Kremlin's energy security storms over the past two decades—but with a global energy crisis underway, the region will need to continue its steadfast efforts to maintain calm among the maelstroms.

Since the onset of Russia's full-scale invasion of Ukraine in February 2022, Moscow's energy weaponisation strategy has reached its logical apex. After all, what could be more damaging to the energy security of Ukraine than a relentless campaign of overt kinetic strikes by the Russian military against its civil energy infrastructure?

In the nearly two decades prior to this open energy warfare against Ukraine's power grid and energy production capacity, the Kremlin incrementally ramped up its multifaceted weaponisation of energy resources and infrastructure against the European continent. For casual watchers of European geopolitics, perhaps the highest-profile incidents involved the repeated Kremlin threats to cut off natural gas to the continent, including along the Ukrainian gas transit route. Putin's notorious gas valve shutoffs to Ukraine took place in 2009, 2014, and 2018, to name just a few.

Outrunning the Weapon

During these years, the Baltic Sea region largely recognised that it was not immune to these threats from the east, which went well beyond easily definable, politically motivated gas supply cutoffs. Indeed, for many years, the Kremlin has used every tool at its disposal to undermine European security, including by deepening EU member states' dependence on Russian energy and issuing legal challenges to Brussels' antimonopoly measures against Russian state-owned enterprises extracting political tolls. Perhaps most insidiously, the Putin regime has also pursued strategic corruption and elite capture, recruiting former senior European officials to become lavishly paid members of boards for Rosneft, Gazprom, and others.

For the most part, Baltic Sea states not only recognised these threats but also witnessed the Kremlin's actions against Ukraine's energy sector over the decade before 2022 and took proactive steps to outrun Russian efforts to wield its energy weapon in the region. To forestall Putin's ability to operationalise its dominant status in the European energy market, in 2014, Lithuania led the Baltic Sea region by opening the first large-scale LNG import facility—the aptly named *Independence* terminal in Klaipėda—followed up closely by Poland's own LNG terminal at Świnoujście in 2016. Not only did these import facilities provide optionality to plug into the global natural gas market—a commodity that has become more fungible with the expansion of global LNG trade and market entry by emerging

powerhouses like the United States over this period—but they also proved economically successful. The full import capacity of Lithuania's terminal was already booked as of 2023, a full decade in advance through 2033.

Critical interconnectors were also constructed across the region, ensuring increased liquidity in the natural gas and electricity markets—key drivers of Europe's energy security strategies, which have always prioritised diversification of sources, delivery routes, and fuel types. These vital energy conduits included the Estlink 1 (2006) and 2 (2014) subsea high-voltage electricity interconnectors spanning the Gulf of Finland, the Balticconnector subsea gas pipeline (2020) between Finland and Estonia, the NordBalt electricity cable (2015) linking Sweden and Lithuania, and the Gas Interconnector Poland-Lithuania (GIPL) and Baltic Pipe (Norway-Denmark-Poland) pipelines that came into operation in 2022, just months after Russia's full-scale invasion of Ukraine.

The Pivot

Of course, for all these prudent security investments that were made to pivot away from dependency, the largest economy in the Baltic Sea region—Germany—worked in the opposite direction, deepening its reliance on Russian energy infrastructure and resources through its dogged development of the Nord Stream pipelines and support of legal measures that would attempt to cement the Kremlin's market position. And of course, Germany was home to the most prominent example of Russia's elite-capture strategy: former German Chancellor Gerhard Schröder accepted positions on the board of Nord Stream AG and, eventually, Rosneft, after approving the Nord Stream 1 pipeline while in office.

Mercifully, the German government, following Russia's full-scale invasion of Ukraine, pivoted in line with its fellow Baltic Sea neighbours, just as the Kremlin began to cut off deliveries to Europe in an attempt to break the continent's solidarity with Ukraine. Energy leaders like former German Vice Chancellor Robert Habeck took rapid action to support the buildout of LNG import facilities, while the country finally abandoned projects like the Nord Stream pipelines. (Even Schröder ultimately—and belatedly—was pressured to give up his sinecures.)

Taken together, the long-term infrastructure diversification, interconnection, and regulatory actions taken by the majority of Baltic Sea states and EU institutions, especially from 2014 through 2022—coupled with Germany's rapid reorientation away from Russia and integration with the global LNG market—meant that the Kremlin's post-February 2022 energy cuts packed less of a punch than they might have otherwise. The adoption of the REPowerEU policy framework, which supported short-term market action paired with long-term investment in renewables, further weakened the Kremlin's grip.

The fact that the continent has narrowly avoided what could have been an extreme crisis post-2022 is a testament to the sound security-of-supply-oriented energy policies and the success of cross-border infrastructure cohesion. They trace their origin back to Europe's original energy security construct: the European Coal and Steel Community championed by visionary Jean Monnet more than half a century ago.

As positive an outcome as this was, for Europe—and the Baltic Sea region in particular—any celebration would have to be put on ice.

For just as EU member states took action to mitigate Russian security-of-supply threats and market manipulation, the Kremlin sought to counter those gains with a pivot of its own: one that would see not only overt kinetic strikes against Ukraine's power sector, but also a parallel, shadow war. Moscow launched this shadow war to undermine European democratic resilience and support for Kyiv via covert sabotage actions against energy, transportation, telecommunications, and other critical infrastructure.

Underwater Mayhem

To argue that the region was largely unprepared for such an eventuality would not give due credit to the serious military, intelligence, and law enforcement planners who advanced civil defence regimes, especially in the Nordic and Baltic states. After all, they were often treated as the Cassandras of national security by western European capitals despite their decades (if not centuries) of frontline understanding of the threats they faced as Moscow's nearest neighbours.

Nevertheless, in European policy circles, in-depth discussions of physical security threats against civil energy infrastructure were few and far between, compared to debates over market security, regulatory action, and investments in infrastructure diversification. To the extent that infrastructure damage was a focus, it was to discuss cyber threats, which had replaced outmoded clandestine physical sabotage as the threat vector of the day.

That's why, when the Russian fishing vessel *Melkart 5* dragged its seabed trawling equipment many dozens of times over a segment of the southern seabed fibre-optic line connecting the Norwegian archipelago of Svalbard with the European continent until the cable snapped, few might have guessed the incident marked one of the first suspected infrastructure sabotage attacks in this new phase of Russian shadow warfare. Indeed, the cutting of the Svalbard seabed cable—the first case study in the University of Pennsylvania's Underwater Mayhem research project—indicated a strategic move by the Kremlin, severing one of the two lines connecting the largest commercial satellite ground station on Earth, SvalSAT, with Europe. Six weeks later, Ukraine would use the type of open-source commercial geospatial imagery and satellite internet uplink data that transits through the station in its defence. According to military experts interviewed in Underwater Mayhem, the Svalbard cable cut was likely a shaping operation to undermine Ukraine's defence ahead of Russia's full-scale invasion.

In the years that followed, sabotage attacks, large and small, would occur around the Baltic Sea region. Some of the largest offshore attacks, such as the September 2022 Nord Stream 1 and 2 bombings, remain officially unattributed (despite findings from Underwater Mayhem providing data to suggest potential Russian involvement; conversely, some media narratives have pointed to a 'pro-Ukraine' sailboat diving team as the culprit). Onshore sabotage of energy connections, rail lines, telecommunications links, storage facilities, and other civil infrastructure began to be attributed to an increasingly regular pattern of Kremlin-backed activity. Often, when attribution has been possible, European law enforcement has pointed to Russia's military intelligence, the GRU, using Telegram and other social media platforms to hire non-Russian nationals, including Ukrainian, Belarusian, and Polish citizens, to conduct low-level infrastructure sabotage.

The offshore sabotage continued in October 2023 with high-profile incidents involving damage to the Balticconnector gas pipeline and other telecommunications cables between Sweden and Estonia, and between Estonia and Finland. The Hong Kong-flagged container ship *NewNew Polar Bear* dragged its

anchor across these cables and pipelines—all while being closely escorted by the Russian-flagged nuclear-powered icebreaker *Sevmorput* (according to open-source AIS data). While Baltic Sea authorities didn't act fast enough to interdict the *NewNew Polar Bear* before it exited European waters, the response time after subsequent incidents began to shorten. In 2024, when the China-flagged bulk carrier *Yi Peng 3* was found to have dragged its anchor through both the Finland-to-Germany C-Lion 1 and the Lithuania-to-Sweden BCS seabed telecommunications cables, authorities stopped the vessel in Danish waters before ultimately releasing the ship. Then, on Christmas Day, the Russian shadow fleet vessel *Eagle S* (hiding behind its Cook Islands flag of convenience) dragged its anchor through the Gulf of Finland, severing seabed telecommunications cables and the Estlink 2 electricity interconnector. The cut to Estlink 2 occurred just weeks before the Baltic states were to desynchronise their electricity grid from the legacy Soviet system that tied them to Russia and Belarus, and synchronise with the European Union grid. Thankfully, while the incident did increase the level of technical risk associated with the synchronisation effort, it didn't block the switch, which successfully took place several weeks later.

Looking for Legal Remedy

Some European policymakers have begun to merge two distinct Kremlin threat vectors—subsea sabotage and shadow-fleet sanctions-evasion activity—into one dismissible phenomenon. According to some, the damage to seabed infrastructure is, in retrospect, likely the result of accidents caused by the poor condition and unprofessional crews characteristic of the shadow fleet vessels. In truth, the majority of the suspected subsea sabotage incidents have been committed by non-shadow-fleet commercial carriers in relatively good repair, rather than by dilapidated Russian oil tankers like the *Eagle S*.

The *Eagle S* was seized after Finnish law enforcement rappelled from helicopters onto the deck in a daring operation in the Gulf of Finland. It led to the indictment of the captain, though the Finnish court case was dismissed in late 2025 in part due to insufficient jurisdiction, as the incident occurred in the narrow lane of the Finnish Exclusive Economic Zone (EEZ), rather than in its territorial waters. Given that outcome, experts wondered if other such incidents might follow. Sure enough, just weeks later—on New Year's Eve—another Russia-linked vessel, the *Fitburg*, was seized by Finnish authorities after dragging its anchor across seabed cables along nearly the same EEZ lane as the *Eagle S*; an investigation for gross sabotage was launched.

Does this mean that no legal deterrent is possible? For another possible legal course, one needs to look to the far side of the world, at a landmark legal case in Taiwan. In February 2025, a China-flagged vessel, the *Hong Tai 58,* was seized by Taiwan's Coast Guard after it had been caught severing one of the subsea telecommunications cables operated by Chunghwa Telecom, which links the main island of Taiwan with the Penghu islands in the centre of the Taiwan Strait.

According to the lead prosecutor, the *Hong Tai 58* was in extremely poor physical condition at the time of the incident. When it was boarded and inspected, its bulk cargo holds were entirely empty, and its cargo doors were rusted shut so that it couldn't have been used for cargo transit. It was reasonable to conclude that the vessel was a 'pawn sacrifice': using a very old and decrepit vessel wouldn't result in high cost if it were seized. Moreover, the captain, a Chinese national, was arrested and tried, and is currently serving three years in jail; he had a satellite phone and was in regular contact with the ship's owner in China. The final call was recorded less than an hour before the incident, suggesting it could

have been an order to drag the anchor, according to the prosecutor (though the contents of the call are unknown).

The key outcome of this case lies not just in the forensic evidence, though it could suggest a growing tactical convergence between Russia and China. Indeed, Taiwan's legal interpretation and related studies may be useful to Finnish and other prosecutors. First, the Penghu Islands cable cut occurred in Taiwan's territorial waters, giving the case considerable jurisdictional leverage. However, the prosecutor described a related study examining what legal recourse Taiwan might have if a future subsea cable incident occurred further afield, within Taiwan's EEZ or beyond.

This all comes down to the so-called 'results principle'. According to Article 4 of Taiwan's criminal code, "where either the conduct or the result of an offence takes place within the territory of the Republic of China, the offence shall be considered as committed within the territory of the Republic of China." Therefore, the prosecutor explains that, "if the submarine cable is damaged in our EEZ or further out […], our country has jurisdiction over the case." However, he notes, "the law does not grant investigative agencies law enforcement powers outside of the EEZ." The results principle, applied to subsea cables, could be compared to how a democratic state indicts international corrupt actors preying on its citizens from a third-party national jurisdiction. This is a legal study in Taiwan, rather than a legal precedent, since it has yet to be tested in a court case involving Taiwanese seabed cable damage beyond its territorial waters, but it could be instructive for the Baltic Sea region.

Transatlantic Troubles

Beyond legal deterrence strategy, a striking absence of action is felt. Even for onshore acts of sabotage against energy and critical infrastructure—conducted by Russian or Russia-recruited actors—with clear and public attribution, no member state has invoked the consultation mechanism under NATO's Article 4. While stopping short of the collective defence clause, Article 4 has the benefit of increasing political recognition, and could expand the resources NATO has already allocated through initiatives like Operation Baltic Sentry. Article 4 has been invoked over the past year due to Russian incursions into NATO airspace: Russian drones in Poland and military aircraft in Estonia. So, it is vital to use the same political action when it comes to sabotage.

Such incidents have illustrated new and emerging threat vectors against EU energy and critical infrastructure, beyond sabotage. In September 2025, Russian fighter jets performed a low-altitude manoeuvre in Polish waters over the PetroBaltic offshore oil platform; the Russian shadow fleet vessel *Boracay* was interdicted by French authorities after it was suspected of launching drones near the Danish Kattegat, which forced the shutdown of the Copenhagen airport. The *Boracay* had been previously stopped by Estonian authorities in the Muuga Bay months earlier, when the vessel was called *Kiwala*. It shows the extent to which Moscow uses its shadow fleet vessels not just for evading western sanctions on Russia's Urals crude oil exports, but also as platforms for dual-use threats. This includes recent reports of Russian security personnel posted onboard 'merchant' vessels, unaccountable to the captains or crews.

As these threats have evolved, European authorities have worked to catch up, especially by focusing on vessel seizures, which enhance the efficacy of energy sanctions. These seizures have become increasingly frequent just as Washington has begun to weaken sanctions unity. After a month-long waiver of Russian oil sanctions by the Trump administration—and despite claims by US Treasury

Secretary Scott Bessent that this waiver would not be extended beyond mid-April 2026—on 17 April, the US Department of the Treasury did just that, with the extension set to expire in mid-May.

This move may well be solely about the White House mitigating the uptick in global oil prices—and thereby stabilising costs for US consumers—due to the Iran war, and specifically due to the closure of the Strait of Hormuz by the Iranian Revolutionary Guard Corps. But regardless of core motivation, the short-term impact is the same: this destructive move allows the Putin regime to make windfall profits for another four weeks, while providing the Kremlin a fresh injection of capital at a time when it would otherwise face macroeconomic impediments to fund its illegal aggression against Ukraine. And although any economic lifeline to the Putin regime is clearly unacceptable even for another four weeks, the bigger concern is the long-term impact of this waiver on the efficacy of the transatlantic sanctions infrastructure that has been built up since Russia's full-scale invasion. Any loopholes in these increasingly restrictive sanctions regimes can undermine Alliance cohesion to hold Russia to account for the humanitarian misery it is inflicting on the Ukrainian people. And what the Trump administration has done is create a loophole through which Putin could sail a shadow-fleet tanker.

The global energy security crisis stemming from oil cargoes stuck in the Persian Gulf and continued threats that Iran's Houthi allies in Yemen could also choke off the Bab al-Mandeb Strait should make it abundantly clear: even though Europe did not start the conflict, the energy security impacts of the war have reached Europe at a moment when its response to Russian energy and infrastructure weaponisation is taking shape. Although the Iran war may be considered 'not Europe's war', to avoid a jet fuel crisis or broader oil and gas shortages as the heating season begins in the Fall, as well as to secure alternative supplies, Europe will again have to evolve its energy security strategy to include robust global diplomatic outreach. And yes, European states will likely have to go further to include some degree of military action against Iran to help open and maintain these vital conduits of the global energy economy.

History will tell if Europe can evolve on a sufficiently fast timescale to maintain its leadership and hold Russia to account for its crimes in Ukraine and against EU member states, while also helping to ensure global energy security in the Middle East and beyond. As we have seen over the past two decades, although it might take time for Europe to develop its energy security response, it can rise to the challenge.

.

UNDERWATER MAYHEM:

COUNTERING THREATS TO ENERGY AND CRITICAL INFRASTRUCUTRE ACROSS THE NATO ALLIANCE AND BEYOND (VOL. 01)

DR. BENJAMIN L. SCHMITT
PROF. MICHAŁ KURTYKA
PROF. ALAN RILEY

Penn
University of Pennsylvania

REPORT - MAY 2025

FULL REPORT DOWNLOAD PAGE:
https://upenn.app.box.com/s/wvrobfk9j1h34agng36chj73ibtkcx0h

In May 2025, a team led by Dr. Benjamin L. Schmitt (Senior Fellow, University of Pennsylvania), Michał Kurtyka (Professor, College of Europe, Natolin), and Alan Riley (Visiting Professor, College of Europe, Natolin) published a new report entitled: ***Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond (Volume 01)***. The report is based on a research project launched at the University of Pennsylvania in 2023. This sheet provides a quick-glance overview of the project scope and case study findings, that led to the policy recommendations appearing in the report.

UNDERWATER MAYHEM: Project Scope

This report is the first in a series of volumes that present findings resulting from research that has driven a multi-year investigative project launched at the University of Pennsylvania in 2023. The project is focused on exploring global energy and critical infrastructure security trends, with a particular focus on analysis of suspected subsea sabotage incidents potentially involving the Russian Federation and People's Republic of China since 2022.

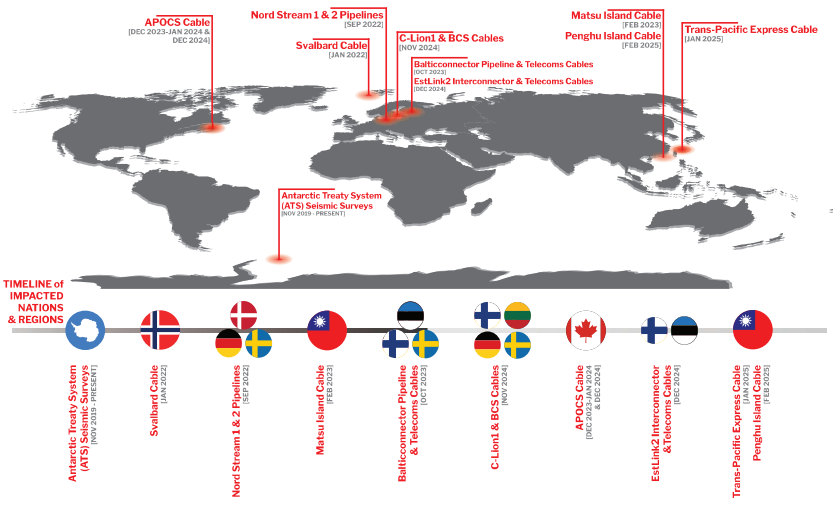
This project furthermore provides policy recommendations to enhance offshore protection and deterrence of future physical attacks on subsea infrastructure, driven by the investigation of case studies of recent suspected sabotage incidents that have occurred globally, including:

- **January 2022:** The cut of a subsea fiber optic telecommunications cable connecting the Norwegian archipelago of Svalbard with the Norwegian mainland.
- **September 2022:** The destruction of three of the four trunklines comprising the Kremlin-backed Nord Stream 1 and Nord Stream 2 natural gas pipelines.
- **February 2023:** The cutting of subsea telecommunications cables connecting the main island of Taiwan to the Taiwanese Matsu Islands.
- **October 2023:** The destruction of the Balticconnector natural gas pipeline, as well as several subsea telecommunications cables connecting Finland and Estonia, and Estonia and Sweden.
- **November 2024:** The cutting of subsea telecommunications cables spanning the Baltic Sea between Lithuania and Sweden, and Finland and Germany.
- **December 2024:** The damage of the Estlink2 subsea electricity interconnector cable, as well as several subsea telecommunications cables connecting Finland and Estonia.
- **Dec 2023-Jan 2024 and December 2024:** The cutting of a subsea telecommunications cable linking Cape Breton Island to Newfoundland in the Cabot strait in northeastern Canada.
- **January/February 2025:** The cutting of subsea telecommunications cables connecting Taiwan with the United States, the Republic of Korea, and Japan, and a cable between the main island of Taiwan with the Taiwanese Penghu Islands.

In addition to these case studies, a companion volume will be included that highlights a five-year study of the Russian Federation's actions to undermine provisions against commercially oriented hydrocarbon exploration and exploitation through seismic surveys conducted within the waters of the Antarctic Treaty System (ATS). Furthermore, this study will provide open-source AIS and commercial geospatial imagery of some of these same vessels that Russia has operated in the ATS maritime region suggesting their involvement in surveys of Western owned-and-operated critical subsea cables and related infrastructure around the globe.

PROJECT: UNDERWATER MAYHEM

Case Study Areas



CASE STUDY 01:
Svalbard Cable Cut (January 2022)

The summary of key assessments from the Svalbard Cable cut Case Study in the report go as:

- Based on open-source AIS analysis, expert interviews, site visits, and the review of investigative media reporting and related public literature, we assess as ***highly probable*** that the Svalbard subsea cable was cut by a commercial fishing trawler, the Russian Federation flagged <MELKART-5> (IMO: 9130183).

- We have a ***moderate level of confidence*** in this judgement. We also note that as of the writing of this report volume, public attribution for the culpability of the Svalbard cable cut has yet to be officially made by Norwegian authorities.

  Moreover, experts suggested that this event may have been a so-called military "shaping operation" by the Russian Federation ahead of Moscow launching its full-scale invasion of Ukraine that would follow just six weeks later.

CASE STUDY 02:
Nord Stream Sabotage (September 2022)

The summary of key assessments from the Nord Stream sabotage Case Study in the report go as:

- Based on open-source AIS and commercial satellite imagery analysis, expert interviews, site visits, and the review of investigative media reporting and related public literature, we assess as ***highly improbable*** the theory that the United States military (with help from the Norwegian military) was to blame for the Nord Stream 1 and Nord Stream 2 sabotage.

- Furthermore, we assess as ***improbable*** that a group of Ukrainian commandos operating from a rental sailboat was behind the destruction of the Nord Stream 1 and Nord Stream 2 pipelines.

- Moreover, we assess as ***probable*** that the Russian Federation was involved in the Nord Stream sabotage incidents.

- We have a ***moderate level of confidence*** in these three judgements.

  These key assessments are based on findings in the report, including:

- The Russian Federation has been demonstrated to regularly recruit and use non-Russian nationals, including those from Eastern European nations, to carry out vandalism and sabotage attacks against critical infrastructure across Europe in recent years.

- The Russian Federation has been shown via open-source AIS data and commercial satellite imagery to have deployed military vessels, some with subsea warfare capabilities at the eventual site of the Nord Stream 1 sabotage northeast of Bornholm just days before the incident, as well as at the same site months earlier in June 2022. Furthermore, the Russian Federation had construction vessels stationed over the exact spot southeast of Bornholm already for lengths of time in the first half of 2021, in which the Nord Stream 2 incident would take place. In this context, we also present the findings of an October 2021 think tank report suggesting that Russian "military personnel" had been observed aboard Russian vessels "in the work zone" in 2021.

- Combined open-source AIS and commercial satellite analysis completed for this report found that there were vessels observable as "dark vessels" (without their AIS enabled) within the immediate vicinity of the Russian construction fleet for Nord Stream 2 in 2021.

- The marina in which the eventual alleged "pro-Ukraine" rental sailboat would be rented from in Germany, is physically located in close proximity within the same port as a logistical deployment facility utilized by the Russian Nord Stream 2 construction fleet in 2021.

- Open-source AIS monitoring demonstrated that after the Nord Stream sabotage incident, at least three Russian-flagged vessels attempted to approach the blast site investigation areas, which appear to have been intercepted and escorted away from the sites by Swedish, Danish, and United States naval and coast guard assets. All three of these Russian-flagged vessels were later observed at the October 2023 Balticconnector natural gas pipeline damage site in the Gulf of Finland, either during the incident (in the case of the Russian-flagged nuclear class icebreaker <SEVMORPUT>), or in the days following that incident.

- Multiple commercial and military technical divers and subsea demolitions experts who were interviewed for this study raised significant questions regarding the assertion that it would be technically feasible (though not impossible) for the rental sailboat <ANDROMEDA> to have been used as the platform for an operation of this scale, as alleged by multiple media reports in the recent past.

- While media reports have suggested that the alleged <ANDROMEDA> sabotage operation was directed by the former Chief of the Ukrainian General Staff Valeriy Zaluzhnyi, a current U.S. government official raised concerns with this claim, citing that such an operation would not have been under the operational capacity of Zaluzhnyi, a point echoed by several experts.

- Senior Polish national security officials interviewed for this study claimed that "Poland's intelligence shared data on the Nord Stream sabotage case with German officials, and the findings suggested Russian actors may have been behind the attacks."

- Investigative journalists have publicly reported on the details surrounding some of the individuals that have been reported in, e.g., public German media accounts, to have been behind the <ANDROMEDA> operation, showing that at least one of the alleged team appeared to be freely living within the Russian Federation in 2023 after the attacks took place, as well as others reportedly "under investigation for trying to overthrow the Ukrainian government."

- Experts interviewed as a part of this study have commented on past instances of suspected Russian damaging of its own energy infrastructure as a potential means of creating a *force majeure* scenario for Gazprom and other Russian entities.

- Despite the recent prevalence of the rhetorical question "why would Russia destroy its own pipeline?" expert interviews and analysis conducted for this study suggest that the Russian Federation arguably did have possible motivation to sabotage the Nord Stream pipelines, including on economic, security, and legal grounds.

- Concerns about the Russian Federation potentially using energy infrastructure deployments to mask the installation of intelligence or military equipment in the Baltic Sea has been a concern for decades.

NOTE: Full citations for the details discussed in this overview sheet are provided in the full report document.

REPORT | ENERGY SECURITY · DEFENSE POLICY · OPEN-SOURCE INTELLIGENCE

Penn
University of Pennsylvania

BENJAMIN L. SCHMITT
MICHAŁ KURTYKA
ALAN RILEY

MAY 2025

COVER PHOTO: Baltic Sea Southeast of Bornholm, Denmark (September 2024) / CREDIT: B. L. Schmitt

THANKS TO THE KLEINMAN CENTER FOR ENERGY POLICY

The University of Pennsylvania's Kleinman Center for Energy Policy fosters impactful energy research, develops the next generation of energy leaders, and provides a home for stakeholders to explore complex issues that impact energy decision making reaching from the Philadelphia community to nations around the world. We thank the Kleinman Center for supporting this project.

Located in the historic Fisher Fine Arts Building on Penn's Philadelphia campus, the Kleinman Center for Energy Policy was established in July 2014 with a generous $10-million gift to the University of Pennsylvania Stuart Weitzman School of Design from Scott (C'94 and W'94) and Wendy Kleinman. In 2019, their second gift of $30 million established the Center's endowment fund. This fund has benefited from the generosity of many Penn alumni donors.

As we move toward a more sustainable energy future, the Kleinman Center for Energy Policy drives policy innovations that support this transition. The center convenes students, faculty, and practitioners from all disciplines to explore global energy challenges through research, courses, events, and hands-on learning.

PHOTO: Christiansø ferry building in Gudhjem Havn, on the island of Bornholm, Denmark (January 2024) / CREDIT: B. L. Schmitt

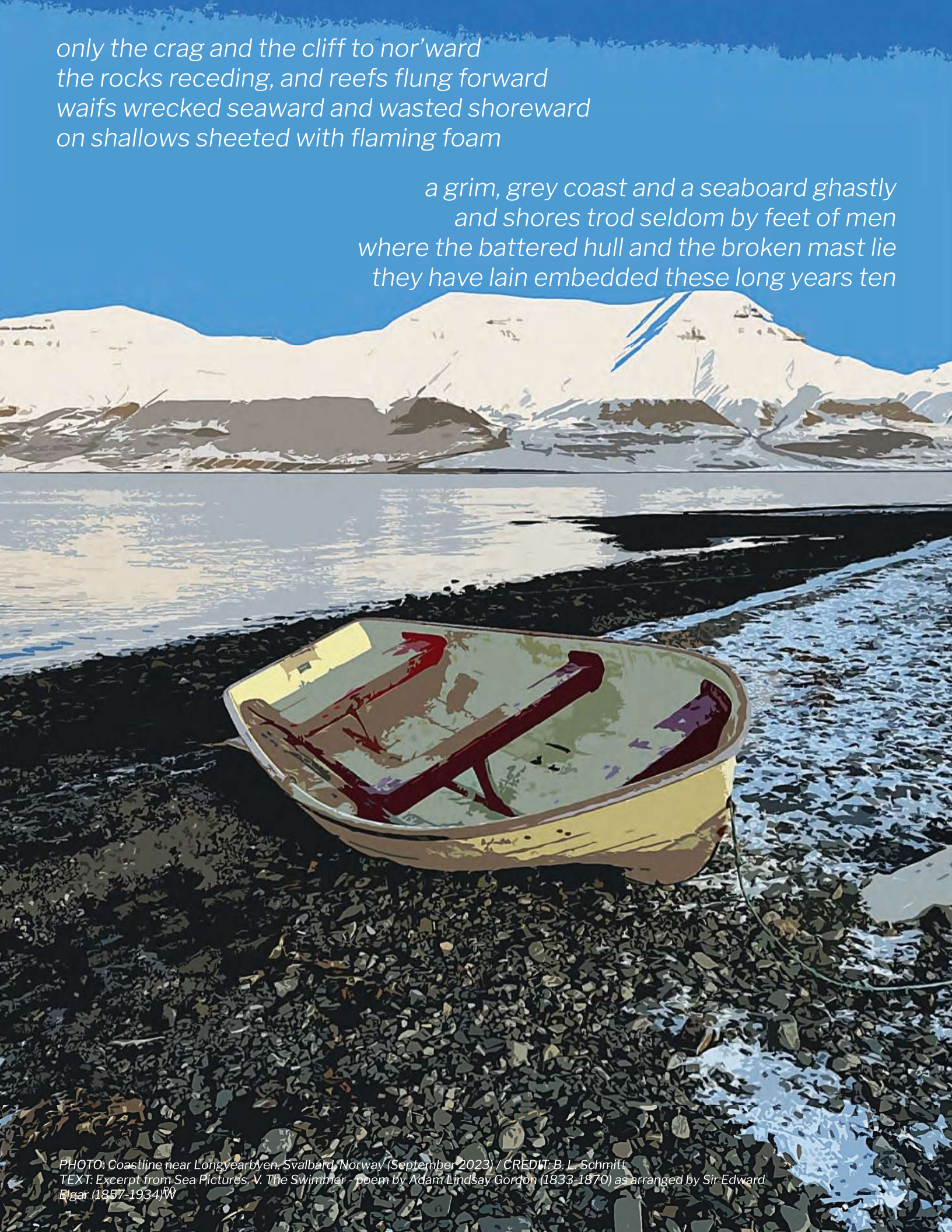


PHOTO: Coastline near Longyearbyen, Svalbard, Norway (September 2023) / CREDIT: B. L. Schmitt
TEXT: Excerpt from Sea Pictures, V. The Swimmer - poem by Adam Lindsay Gordon (1833-1870) as arranged by Sir Edward Elgar (1857-1934)

REPORT | ENERGY SECURITY · DEFENSE POLICY · OPEN-SOURCE INTELLIGENCE

UNDERWATER MAYHEM:

COUNTERING THREATS TO ENERGY AND CRITICAL INFRASTRUCTURE ACROSS THE NATO ALLIANCE AND BEYOND

VOLUME 01

BENJAMIN L. SCHMITT
MICHAŁ KURTYKA
ALAN RILEY

MAY 2025

Penn
University of Pennsylvania

CONTENTS

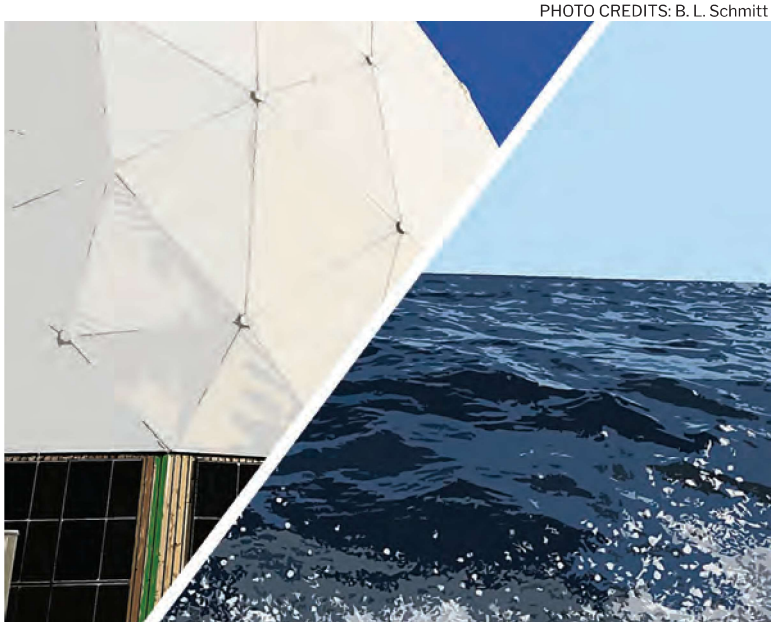
RUSSIAN ENERGY WEAPONIZATION

PHOTO CREDIT: B. L. Schmitt

PROLOGUE	v
EXECUTIVE SUMMARY	2
INTRODUCTION	10
European Energy Security: Before Russia's Full-Scale Invasion of Ukraine	13
European Energy Security: After Russia's Full-Scale Invasion of Ukraine	15
ASSESSING RUSSIA'S "SHADOW WAR"	18
Project Overview	19
Pre-2022 Incidents of Russian Malign Activities Involving European Energy and Critical Infrastructure	23
Trends Exhibited in Recent European Onshore Sabotage Attacks	25

SABOTAGE CASE STUDIES

PHOTO CREDITS: B. L. Schmitt



CASE STUDY 01: SVALBARD CABLE CUT 30
SUMMARY OF KEY ASSESSMENTS 30
INCIDENT BRIEF 31
PRIMARY ACCOUNTS OF INCIDENT 31
OSINT AND FIELD ANALYSIS 31
POLICY CONTEXT AND EXPERT ANALYSIS 33
CASE STUDY 02: NORD STREAM 1 AND NORD STREAM 2 SABOTAGE 40
KEY ASSESSMENTS/ INCIDENT BRIEF 41/44
PRIMARY ACCOUNTS OF INCIDENT 47
POLICY CONTEXT AND EXPERT ANALYSIS 51
ECONOMIC AND LEGAL CONTEXT 52
INFORMATION ENVIRONMENT 59
SECURITY CONTEXT 60
OSINT AND FIELD ANALYSIS 62
CLIMATE CONSIDERATION / COMMENTARY 69/71

POLICY RESPONSES

PHOTO CREDIT: B. L. Schmitt

RECOMMENDED POLICY ACTIONS 86
ACKNOWLEDGEMENTS 91
UNDERWATER MAYHEM WILL RETURN 92
ABOUT THE AUTHORS 94
APPENDIX A: Suspected Russian Hybrid/Sabotage Activities in EU Since 2022 95
APPENDIX B: Public Primary Source Documents 97
APPENDIX C: Nord Stream Maritime AIS Tracking Situation Report Maps 103
ENDNOTES 111

PHOTO: Karlskrona Nedre Lighthouse, Karlskrona, Sweden (January 2024) / CREDIT: B. L. Schmitt

View from Allinge Havn, on the island of Bornholm, Denmark. Island of Christiansø visible on horizon (August 2023) / CREDIT: B. L. Schmitt

PROLOGUE

Even in the earliest moments of the crisis, the magnitude of the events unfolding in the normally quiet waters just miles from his office were evident to the police commissioner of Bornholm, a windswept Danish island in the Western Baltic Sea. “As soon as we learned of the explosions having taken place near Bornholm, it was clear from the very beginning that something very extraordinary had taken place.”

That commissioner, Martin Preisz Gravesen of Bornholms Politi, acted quickly to report “on the incident from the Bornholm Police Headquarters to authorities in Copenhagen immediately” before calling “in all relevant personnel to coordinate a rapid response.” Gravesen explained that in those immediate hours, “the first step was to assess what the danger to lives and property might be, which needed to take place even before the beginning of the investigation for cause.”

While the investigation for cause would go on to grip Europe’s energy and national security circles for years to come, establishing what had taken place in the early hours of September 26, 2022, in the inky waters of the Baltic Sea was front of mind for European authorities.

Based out of Sweden’s historic maritime port of Karlskrona, Mattias Lindholm, spokesperson for the Swedish Coast Guard illustrated the dramatically increasing stakes. “We had gotten information already in

the morning from a merchant vessel that a large outgassing site had formed in the Danish exclusive economic zone (EEZ), but Swedish authorities didn't respond as there was not an immediate request from Danish authorities."

"However, hours later," Lindholm continued, "there was a report of a similar incident taking place in the Swedish exclusive economic zone, so the Swedish Coast Guard immediately deployed a vessel."

According to Lindholm, "Swedish Coast Guard responders thought immediately the incident might have involved Nord Stream since they could see a huge bubbling cloud that had formed. The sea was boiling!"

Beyond immediate safety and environmental concerns, the realization that Russia's dual Nord Stream subsea natural gas pipeline systems might be involved - with blast sites in both Danish and Swedish waters - underscored the growing geopolitical seriousness of the situation since, in Lindholm's view, "given that Russia was a country of interest related to Nord Stream, the response rapidly went from an environmental issue to a geopolitical and security issue, since it would now have to do with defense as well."

Just 24 hours later, the whole world would see images of the churning maw of methane that had confronted Danish and Swedish first responders. Some of the first photos of the Nord Stream 2 pipeline outgassing site in the Danish EEZ southeast of Bornholm were taken by a Danish F-16 interceptor fighter jet that was scrambled from that very Danish island. Those images, released by the Danish military on September 27, 2022, also revealed multiple leak sites over the Nord Stream 1 pipeline route northeast of Bornholm in Swedish waters.[1] Within days, commercial satellite images would join these aerial photos, illustrating the wide extent of the damage as viewed from low earth orbit.[2]

Not only would the Nord Stream sabotage result in the largest single human-created methane release event in history - but the security concerns associated with the incident rocketed around the transatlantic

"...they could see a huge bubbling cloud that had formed. The sea was boiling!"

community, when, just days later preliminary forensic investigations uniformly pointed to "detonations" and "gross sabotage."[3,4]

While the Nord Stream bombings were not the first examples of physical sabotage against energy and critical infrastructure in the European offshore in the past decade, they certainly captured the public imagination more than any other single incident to date. This public focus would lead to multiple narratives regarding responsible actors, and fueling debate on how countries in Europe and beyond can best ensure that offshore energy and critical infrastructure can be protected in a rapidly degrading global security environment.

The Nord Stream sabotage reinforced the need for transatlantic policymakers to take the threat of physical attacks against energy infrastructure just as seriously as they had begun to address Russian threats to energy supply security, monopolistic practices, and strategic corruption that had been tools largely used by Moscow to undermine Europe's energy and national security interests for decades.

Those policymakers would need to move fast: since 2022 the number of incidents involving energy and critical infrastructure sabotage across the continent would begin to multiply, and incidents of similar pathology

would begin to occur globally, including in the already tense waters of the Taiwan Strait.

And while traditional investigative methods could lead in some cases to attribution of actors responsible for onshore sabotage incidents, methods to overcome the challenge of probing and deterring offshore sabotage remained elusive.

The era of underwater mayhem had begun. ■

Dansk Forsvaret (Danish Defence) press release photo of the Nord Stream 2 outgassing site southeast of Bornholm. Image was acquired by a Danish F-16 interceptor fighter jet response unit dispatched from Bornholm on 27 September 2022. / CREDIT: Danish Defence [P1] ▼

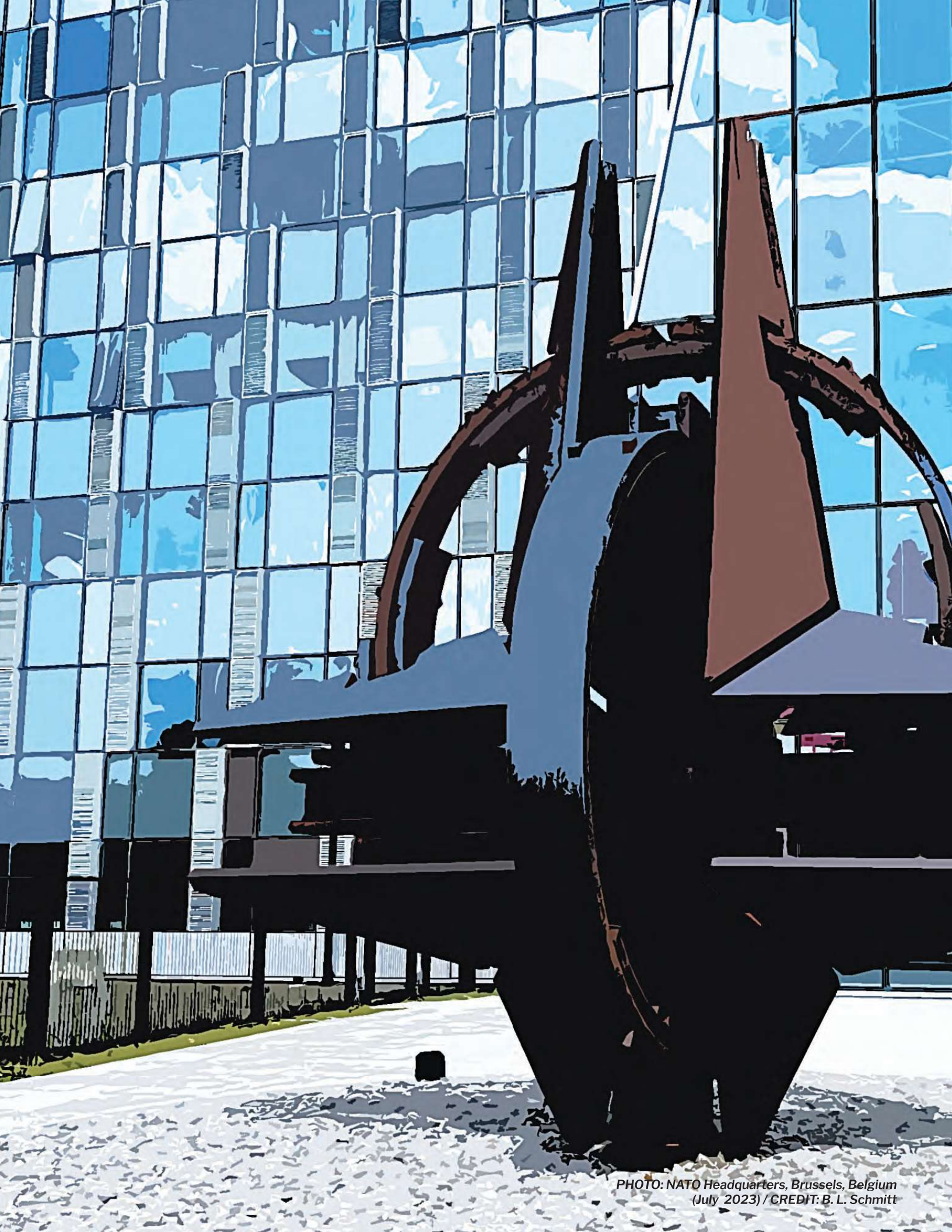


PHOTO: NATO Headquarters, Brussels, Belgium (July 2023) / CREDIT: B. L. Schmitt

"No More Gas From Putin." European Parliament building complex entrance at Place du Luxembourg, Brussels, Belgium. (July 2023) / CREDIT: B. L. Schmitt

EXECUTIVE SUMMARY

European dependence on Russian energy resources has been a key national security concern for policymakers on both sides of the Atlantic dating back to the Soviet era. Since Russian President Vladimir Putin's rise to power more than a quarter century ago, the Russian Federation has regularly used energy as a geopolitical weapon to undermine the democratic resilience of European democracies, with national security impacts across the transatlantic community and beyond.

Especially over the past 15 years, Putin's Kremlin has used its traditionally dominant position in the European natural gas market to extract geopolitical concessions from European states through a variety of strategies, including:

- threatening and enacting politically motivated gas cutoffs.[5]
- utilizing monopolistic practices and lawfare to undermine European Union market liberalization efforts.[6]
- conducting cyberattacks impacting energy installations across the transatlantic community.[7,8]
- eroding democratic resilience through the promotion of strategic corruption and elite capture within European democracies.[9,10]

During this same period, policymakers in the European Union and the

United States have focused on blunting Russia's weaponization of energy by supporting policies that have promoted the deployment of energy diversification infrastructure and antimonopoly regulations, with the aim of undermining Russia's ability to effectively utilize a dominant market position to threaten sudden or sustained energy poverty across the continent.

To be certain, European energy security policies developed in recent years have proven capable at advancing measures to counter Russian energy security of supply threats and monopolistic domination of the European energy market. While this is notable progress, Putin's Kremlin has over the same period expanded its hybrid warfare toolkit to move well beyond energy delivery threats, legalistic assaults, strategic corruption of Western political and business elites, and crippling cyberattacks. Russia's hybrid warfare toolkit now prominently includes physical sabotage against energy and critical infrastructure. Since the beginning of 2022 – just weeks before Russia's full-scale invasion of Ukraine – through to the present, there have been dozens of reports of damage to energy, telecommunications, transportation, and other critical infrastructure across the territory of NATO member states. While many of these incidents remain under investigation, there have already been a significant number of cases in which European security officials have publicly attributed acts of sabotage to either Russian actors, or non-Russian nationals who have been recruited via social media apps like Telegram to conduct a wide spectrum of infrastructure damage on NATO soil.[11,12]

Sabotage attacks in which attribution has been possible have mostly taken place against onshore critical infrastructure, where, even in remote locations, infrastructure monitoring and the collection of forensic evidence can be challenging, however comparatively straightforward in relation to sabotage incidents in offshore and subsea environments.

Since early 2022, there has also been a growing list of high-profile incidents resulting in damage against energy and critical infrastructure located in offshore environments, ranging from the Barents to the Baltic seas to the Taiwan Strait to Canada's Atlantic coastline. Given the relative lack of persistent monitoring required for total maritime domain awareness, the remoteness of these incidents, and the technical difficulty associated with offshore forensic investigations, most of these acts of suspected maritime sabotage have not yet resulted in official attribution, and as a result, have set off heated debates in the policy, military, expert, and commercial maritime communities.

Russia's hybrid warfare toolkit now prominently includes physical sabotage against energy and critical infrastructure.

Underwater Mayhem: Project Scope

This report – ***Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond (Volume 01)*** – is the first in the series of volumes that present findings resulting from a multi-year research project launched at the University of Pennsylvania, and focused on exploring global energy security trends as they pertain to energy and critical infrastructure protection from suspected sabotage operations, including those potentially involving the Russian Federation and the People's Republic of China.

▲
Salvage/Rescue vessel <LEOPOLD ROSENFELDT> (IMO: 8902670) in the port of Nexø, on the island of Bornholm, Denmark.[31] (September 2024) / CREDIT: B. L. Schmitt

While many of the incidents studied within this research project have a distinct energy security nexus, the report series will also consider threats to other critical infrastructure deployments, including telecommunications and transportation installations. Such a wider spectrum approach is required to properly analyze these trends since, among other factors, energy infrastructure is often collocated with other forms of critical infrastructure, and the pathologies associated with attacking and defending subsea infrastructure, in particular, carry many distinct similarities, which are detailed in this report series.

In addition to the broader dynamics at play, the ***Underwater Mayhem*** report series aims to provide a detailed assessment of several of the highest profile acts of offshore energy and critical infrastructure damage that have taken place since early 2022, including:

- **January 2022:** The cut of a subsea fiber optic telecommunications cable connecting the Norwegian archipelago of Svalbard with the Norwegian mainland.[13]
- **September 2022:** The destruction of three of the four trunklines comprising the Kremlin-backed Nord Stream 1 and Nord Stream 2 natural gas pipelines.[14]
- **February 2023:** The cutting of subsea telecommunications cables connecting the main island of Taiwan to the Taiwanese Matsu Islands.[15]
- **October 2023:** The destruction of the Balticconnector natural gas pipeline, as well as several subsea telecommunications cables connecting Finland and Estonia, and Estonia and Sweden.[16]
- **November 2024:** The cutting of subsea telecommunications cables spanning the Baltic Sea between Lithuania and Sweden, and Finland and Germany.[17]
- **December 2024:** The damage of the Estlink2 subsea electricity interconnector cable, as well as several subsea telecommunications

cables connecting Finland and Estonia.[18]

- **Dec 2023-Jan 2024 and December 2024:** The cutting of a subsea telecommunications cable linking Cape Breton Island to Newfoundland in the Cabot strait in northeastern Canada.[19,54]

- **January/February 2025:** The cutting of subsea telecommunications cables connecting Taiwan with the United States, the Republic of Korea, and Japan, and a cable between the main island of Taiwan with the Taiwanese Penghu Islands.[20,21]

In addition to these case studies, a companion volume will be included that highlights a five-year study of the Russian Federation's actions to undermine provisions against commercially oriented hydrocarbon exploration and exploitation through seismic surveys conducted within the waters of the Antarctic Treaty System (ATS). Furthermore, this study will provide open-source AIS and commercial geospatial imagery of some of these same vessels that Russia has operated in the ATS maritime region suggesting their involvement in surveys of Western owned-and-operated critical subsea cables and related infrastructure around the globe.

In this first report volume, ***Underwater Mayhem (Volume 01)***, we provide case studies focusing on the first two of these incidents: the January 2022 Svalbard subsea telecommunications cable cut, and the September 2022 destruction of the Nord Stream 1 and Nord Stream 2 natural gas pipelines. This report also provides broader project-framing analysis, background on the evolution of Russia's weaponization of energy, along with technical and policy recommendations to increase the analytical understanding of the growing list of physical sabotage against energy and critical infrastructure globally, especially in offshore and subsea environments, and proposed actions for deterrence. The security analysis and case studies included in this series aim to serve as a resource for investigators and policymakers considering how best to characterize acts of suspected energy and critical infrastructure sabotage, especially in offshore and subsea domains. To satisfy this broad scope, the research for this report series has been conducted within a multidisciplinary framework to mirror the interdisciplinary nature under which these incidents took place.

Analytic Methods

The studies, analysis, and assessments

Isfjorden fjord in the archipelago of Svalbard near Longyearbyen, Svalbard. The Svalbard Undersea Cable System runs on the seabed of Isfjorden near where this photo was captured aboard a vessel under weigh on the fjord.[32] (September 2024) / CREDIT: B. L. Schmitt

represented in ***Underwater Mayhem (Volume 01)*** relied on the following methodologies:

- Field research conducted at or near the energy or other critical infrastructure sites in which these offshore incidents took place across Northern Europe.

- Interviews with dozens of experts on both sides of the Atlantic, including:

    - Commercial leaders with expertise in offshore energy and critical infrastructure construction and operations.
    - Commercial ship operators and related maritime industry professionals.
    - Commercial and military divers and subsea demolitions experts.
    - Current and former naval, military, coast guard, and law enforcement professionals.
    - Current and former senior energy and national security officials.
    - Leading experts and academics focusing on European energy and national security issues.

- Open-source intelligence (OSINT) analysis, including maritime automatic identification system (AIS) data (sourced from the MarineTraffic AIS platform) and commercial geospatial intelligence platforms (particularly from the Planet optical-wavelength satellite platform).[22,23]

- Review of literature, academic analysis, and press reporting related to these incidents, and related publicly-available primary source documents.

Underwater Mayhem (Volume 01): Key Assessments and Recommendations

The case studies included in this volume were based on expert interviews, OSINT data analysis, field research, media reporting, and a review of public literature and documents, which have allowed us to reach certain judgements regarding our analysis of the two case studies reviewed, as well as policy recommendations aimed at providing officials with guidance to respond to the ongoing trend of suspected sabotage incidents against energy and critical infrastructure across Northern Europe included herein.

The analysis presented in this report series is solely based on open-source and academic research, all unclassified in nature. Nevertheless, as an academic exercise, we have attempted to review and present our key assessments in terms of best practice metrics publicly set forth by, i.e., guidance made public by the U.S. Intelligence Community, as well as related published academic studies and expert commentaries we have reviewed and cited in this report, guiding our use of estimative language, words of estimative probability, judgements of likelihood, and confidence in assessment. We detail the rationale behind the likelihood and confidence in assessment language decisions made for this report in the main text of this volume.[24,25,26,27,28,29]

Key Assessments

With this context in mind, we present the following key assessments from the two case studies presented in this report volume:

Svalbard Cable Cut Incident (January 2022):

- Based on open-source AIS analysis, expert interviews, site visits, and the review of investigative media reporting and related public literature, we assess that it is ***highly probable***

that the Svalbard subsea cable was cut by a commercial fishing trawler, the Russian Federation flagged <MELKART-5> (IMO: 9130183).[30]

- We have a moderate level of confidence in this judgement. We note that as of the writing of this report volume, public attribution for the culpability of the Svalbard cable cut has yet to be officially made by Norwegian authorities.

- Moreover, experts suggested that this event may have been a so-called military "shaping operation" by the Russian Federation ahead of Moscow launching its full-scale invasion of Ukraine that would follow just six weeks later.

Nord Stream 1 and Nord Stream 2 Incidents (September 2022):

- Based on open-source AIS and commercial satellite imagery analysis, expert interviews, site visits, and the review of investigative media reporting and related public literature, we assess as ***highly improbable*** the theory that the United States military (with help from the Norwegian military) was to blame for the Nord Stream 1 and Nord Stream 2 sabotage.

- Furthermore, we assess as ***improbable*** that a group of Ukrainian commandos operating from a rental sailboat was behind the destruction of the Nord Stream 1 and Nord Stream 2 pipelines.

- Moreover, we assess as ***probable*** that the Russian Federation was involved in the Nord Stream sabotage incidents.

- We have a moderate level of confidence in these three judgements. A wide range of open questions regarding the Nord Stream incidents that we identify in this report preclude us from increasing beyond 'probable' the judgement of the Russian Federation's potential role in the incident and likewise cannot decrease beyond 'improbable' for the 'pro-Ukraine rental sailboat' or beyond 'highly improbable' for the 'United States and Norway' theories.

- The basis for these judgements and our confidence in them, is driven by significant questions regarding the technical feasibility, circumstances, and geopolitical motivation of the 'pro-Ukraine sailboat' explanation of the bombing, as well as the largely-publicly-debunked nature of the United States and Norwegian military explanation of the bombing. These questions were combined with the significant open-source data showing the extensive seabed warfare capabilities that the Russian Federation had at what would become the blast sites both months and then days ahead of the attack, the presence of Russian construction vessels directly over one of the eventual blast sites for significant periods of time in 2021, as well as the geopolitical and economic motivations that may have driven Moscow, among other data which is presented in the second case study of this report volume.

- We note that as of the writing of this report volume, public attribution for the culpability of the Nord Stream 1 and Nord Stream 2 sabotage incidents has still not been made by investigators in any jurisdiction of the Transatlantic community.

Key Policy Recommendations

Furthermore, we provide key policy recommendations aimed at providing officials with guidance to respond to the ongoing trend of suspected sabotage incidents against energy and critical infrastructure across Northern Europe in this report volume, including:

- NATO Member States should invoke the Article 4 consultative mechanism clause of the North Atlantic Treaty in response to incidents of sabotage against energy and critical infrastructure taking place across NATO territories for which official attribution has been made to Russian actors, or actors that have been publicly shown to have been recruited to conduct such operations by the Russian government.
- The European Union should permanently phase out energy imports from Russian Federation under Vladimir Putin given the long track-record the Kremlin has had to weaponize Europe's dependence on Russian energy resources.
- European authorities must proactively utilize strategic communications to counter Russian disinformation campaigns associated with suspected attacks against energy and critical infrastructure across the European continent.
- Transatlantic countries must coordinate protection efforts as well as foster public-private partnerships to increase commercial monitoring technology hardware and data analysis tools to deter energy and critical infrastructure threats.
- Leaders must fully integrate national security, energy security, and critical infrastructure protection strategies into any future climate and energy transition policy frameworks.

NATO Member States should invoke the Article 4 consultative mechanism clause of the North Atlantic Treaty in response to incidents of sabotage...

Throughout this report and the ***Underwater Mayhem*** volumes to follow, we argue that if policymakers do not elevate the policy, technological, and defense steps needed to deter physical sabotage threats from the Russian Federation, People's Republic of China, or any other malign actor, then there can be significant public degradation in the confidence in authorities to ensure energy and critical infrastructure security across democratic societies worldwide. In Europe's case, such a potential will have profoundly negative impacts on a much wider array of policy areas, including support for European defense and Ukrainian sovereignty, countering Russian malign influence across the European energy sector, and a reduction in public support for the deployment of renewable energy infrastructure required to enable the energy transition.

Moreover, an insufficient response will likely embolden other authoritarian nations around the world – and perhaps already has in the case of the People's Republic of China – to use similar infrastructure sabotage methods to undermine the national security of democratic states. Subsea critical infrastructure sabotage threats are particularly acute across East Asia, especially connected to any possible future military action taken by Beijing against Taiwan, and this series conveys why strategies to counter energy and critical infrastructure sabotage needs to remain a high priority of democratic leaders worldwide. ■

General view of the Meeting of the North Atlantic Council at the level of Heads of State and Government at the 75th NATO Leaders Summit in Washington, D.C. (July 2024) / DESIGN: B. L. Schmitt / PHOTO CREDIT: NATO Flickr[P2]

General view of the Meeting of the North Atlantic Council at the level of Heads of State and Government at the 75th NATO Leaders Summit in Washington, D.C. (July 2024) / CREDIT: NATO Flickr[P3]

INTRODUCTION

The terminology used by national security professionals can often play an outsized role in the outcome of any policy decision making process. The practice of energy security policy development is not immune to this reality. Whether or not the current era of Russian energy weaponization toward the Transatlantic community – which has been characterized by physical sabotage against energy and critical infrastructure sites across the NATO alliance – should be characterized as "hybrid threats," "terrorism," or simply "acts of war" may be subject to debate. However, selecting between these terms is not merely an academic exercise—it has direct implications regarding the sort of deterrence measures that are merited, and the policies and actions ultimately operationalized by national security officials to respond.

The statement in **[BOX 01]**, delivered by Danish Prime Minister Mette Frederiksen at an on-the-record Council on Foreign Relations event held on the margins of the NATO Leaders Summit in Washington, D.C. on July 9, 2024, well encapsulates this definitional dilemma as well as the broader moment in European energy and national security policy.[33] Over the past decade, and especially since Russia's full-scale invasion of Ukraine began in February 2022, the Russian Federation under autocratic President Vladimir Putin has utilized nearly every area of modern society as a multi-spectral weapon to pressure the democratic nations worldwide.

The recent level of Kremlin pressure is aimed at eroding western

BOX 01

Danish Prime Minister Mette Frederiksen in response to a question posed by author Schmitt at a Council on Foreign Relations event on the margins of the NATO Leaders Summit in Washington, D.C. on July 9, 2024:

"Well, first of all, thank you for looking into Danish critical infrastructure. I did not know you were doing that. Thank you. And when you were listing some of the events we have seen just in a few months, it sounds like a bad movie, right? And I think that's our main problem, and it was a bit the same feeling I had before the attack on Ukraine. It was like we could not understand that Russia were going in a full-scale war in Europe, but they were. And they are attacking, as I said before. I think they are attacking us every day now, not only on critical infrastructure, hybrid attacks, cyberattacks, disinformation, but also on migration. We have seen it in Belarus, into Lithuania. We have seen it on the Finnish border, that they are using migrants to destabilize inter-European countries. And all of it is a part of modern warfare. I mean, that's what we are looking into. So I think we have to take it much more seriously, and it has to be prioritized in NATO because I think we have to look at it as an attack on us instead of just, well, now, something again happened, and again, and again, and again. So I think we are being too friendly in our reaction to this...I don't think its on this stage we will take that NATO decision, of course it's something that we really have to look into together with our allies, but I guess you can hear—when I'm listening that I think we are—I think we are being—we are simply being too polite."

support for Ukraine's defense, pushing for a suspension of energy and other sectoral sanctions and technology export controls that have been levied by global democracies against the Russian Federation since February 2022, and, more broadly, to undermine the resilience of and confidence in democratic norms worldwide. Frederiksen's apparent frustration about the lack of a cohesive response to these threats on the part of NATO member states reflects a yearslong divide between those Transatlantic leaders who favor "escalation management" with respect to Putin's Kremlin and those that favor a more comprehensive security response.

The Danish Prime Minister lists several of the pressure points that Putin's Kremlin – in command of Russia's authoritarian, kleptocratic societal model – has utilized against the west, the panoply of which have been for years categorized under the guise so-called "hybrid threats."

This spectrum of Russian challenges launched against Europe certainly includes Moscow's long-term proclivity to weaponize energy supplies against nations across the European continent. Particularly over the past two years, the use of energy as a weapon has evolved from undermining confidence in the security of energy supply by, i.e., threatening to or overtly enacting a cutoff of natural gas in an attempt to extract political concessions from European states, to perhaps what could be considered the logical apex state of Russian energy weaponization: overt kinetic strikes against Ukraine's civil energy infrastructure by the Russian military, coupled with a growing list of sabotage incidents in which Russian actors or their proxies have been attributed to have been behind or are suspected of physical attacks against both onshore and offshore energy and critical infrastructure across the European continent.

So how are policymakers to distinguish between "hybrid threats," "terrorism," or

simply “acts of war”? According to Gunhild Hoogensen Gjørv, Professor of Security and Geopolitics at the Arctic University of Norway (UiT), viewing Russia’s multispectral threats as linked – as described by Frederiksen – is appropriate since, “…we cannot see Russian activities as isolated events, but rather all part of a broader strategic objective to weaken western democracies and/or make some regions unstable enough to not be able to withstand larger, more militarized incursions.” Gjørv, who leads a research group at UiT called *The Grey Zone* which focuses on Arctic security, hybrid threats and warfare, and total defense added, “…that is how hybrid threat activities work – multiple activities that together, over a period of time and within a given context – will weaken the target society ideally without going over the ‘threshold’ of military intervention or [NATO] Article 5.”

Still, after many years of hybrid threat activities emanating from Moscow against the West, security experts may be approaching a semantic turning point on how these activities are categorized. For example, U.S. Army Lt. Gen. (Ret) Ben Hodges, who served as Commander of U.S. Army, Europe from 2014 to 2017 emphasizes that he “no longer think[s] of these Russian activities as ‘hybrid,’ but as a part of the spectrum of Russian warfare. They are constantly at war with us, even if we don’t acknowledge it, and are using different parts of that spectrum based on objectives and conditions.”

As for energy and critical infrastructure sabotage in this context? Hodges explained his view that, “the use of sabotage is as much a part of the Russian way of war as are rocket and missile attacks and ground assaults by tanks and BMPs.”

Further to this point, speaking at the 2025 Delphi Economic Forum in April 2025, General Hodges doubled down on this concept, arguing that “the most important thing first of all is for every country to realize that Russia is at war with us. Until we finally start acting and realizing that they are at war with us – even if there are not missiles shooting directly at NATO countries – in their mind they are at war with us… I have to say I don’t like the word ‘hybrid’ because ‘hybrid’ sounds kind of fuzzy…so there is no urgency in our governments to do anything about it.”[34]

Speaking at the 2024 Riga Conference, then Lithuanian Foreign Minister Gabrielius Landsbergis took the semantic importance of what democratic leaders call such acts

Danish Prime Minister Mette Frederiksen (center) along with Czech President Petr Pavel (left) and Estonian Prime Minister Kaja Kallas (right) at the meeting of the North Atlantic Council at the level of Heads of State and Government at the 75th NATO Leaders Summit in Washington, D.C. (July 2024) / CREDIT: NATO Flickr[P4]

by Russia a step further, and emphasized his point on social media by asking "why do we call it 'hybrid warfare'? Because if we called it terrorism then we would have to do something about it."[35]

European Energy Security: Before Russia's 2022 Full-Scale Invasion of Ukraine

The manner in which policymakers classify the wide range of threatening actions by the Russian Federation is indeed central to the response expected by populations in democratic societies. However, it is also important to remember that, especially with respect to supporting European energy security, policies advanced by Transatlantic leaders have often been reactionary to types of threat manifested by Russia toward the Europe's energy market, rather than proactive. **[FIGURE 01]** illustrates what could be considered the five primary pillars of European energy security policy pursued by European leaders and supported by U.S. diplomats and officials over the past decade. As illustrated in **[FIGURE 01]**, those policy areas include:

1. **Diversification of Energy Infrastructure ("Hardware"):** For decades, the EU has focused on infrastructure development proposals that would increase energy security through the diversification of sources, routes, and fuel types. This focus on energy "hardware," has been a hallmark of Transatlantic energy security cooperation for decades, and the European Commission's Energy Union policy framework enshrined the trajectory of the EU to specifically decrease dependence on Russian energy as a focus of its infrastructure investments starting in 2015;[36]

2. **European Energy Market Liberalization and Regulatory Structures ("Software"):** Like the development of European energy diversification "hardware," the EU has focused on becoming more resilient to Russia's traditional monopolistic economic practices within Europe's energy market through regulatory steps like the EU Third Energy Package legislation, which came into force in 2009, and enforce market liberalization measures including ownership unbundling, third-party access, regulatory authorities, and market transparency onto the EU energy system. These measures could be considered the legal "software" needed for a well-functioning European energy market;[37]

"...the use of sabotage is as much a part of the Russian way of war as are rocket and missile attacks, and ground assaults by tanks and BMPs..."

3. **Cyber and Physical Security of Energy Infrastructure:** Even with an energy market that is physically diversified and well regulated, cyber and physical attacks against European energy infrastructure can increase security of supply risks and undermine public confidence in the reliability and governance of energy utilities. While actions to deter and mitigate cyberattacks against energy and critical infrastructure have consistently been the focus of policymakers for the past few decades, the recent increase in physical sabotage incidents has brought physical security back into

▲
[FIGURE 01] Illustration of the Five Primary Pillars of Contemporary European Energy Security.

FIGURE DESIGN: B. L. Schmitt / TEMPLATE AND ILLUSTRATION CREDIT: Petr Vaclavek, Tuna salmon, Icons-studio, SkyLine, Genestro, Dewi, AxelBlogoodf – stock.adobe.com[P5]

the policy spotlight;

4. **Operational Energy Security Action Supporting NATO Defense Objectives:** Beyond civil energy security measures, the NATO alliance continues to focus on operational energy security priorities to ensure that NATO defense operations are not vulnerable to supply shortages of both specialized military grade fuels and civil-military interfaces (e.g. electricity supplies to NATO bases from Member State grids). An area of continued discussion is the potential extension of the NATO Central Europe Pipeline System (CEPS) from its current extent (which does not extend beyond the so-called "Fulda Gap" in Germany) that was developed during the Cold War era to interconnect Western European NATO states, to connect with NATOs Eastern Flank nations;[38]

5. **Countering Russian Malign Influence, Strategic Corruption, Elite Capture, and Disinformation Trends in the European Energy Sector:** Over the past two decades, the Kremlin has often utilized its dominate energy market position and energy infrastructure project investments to co-opt former senior European officials to leave the public trust to join the ranks of Russian state-owned energy enterprises through a process known as "elite

capture" – once "captured" into one of these well-paid positions, these leaders often espouse pro-Kremlin policy positions that counter policies needed to support European security against Russia's multispectral threats. This practice endangers democratic resilience and public confidence in the motivations behind Western leaders decisionmaking vis-a-vis Putin's Russia. While the nature of "strategic corruption" and "elite capture" in the Russian energy context has begun to result in public understanding of the threat, legal countermeasures to these practices continue to lag.[39]

While all of these policy areas have been a part of European energy security frameworks for years, the overarching policy focus of leaders supporting Europe's energy security on both sides of the Atlantic has been on energy infrastructure diversification and market liberalization measures, both of which were vital to address Russia's overt security of supply threats to the continent in the past two decades. After all, Russia had cut off gas flows to Europe dozens of times between 1991 and 2006, and continued to ramp up these politically-motivated gas cutoffs through high-profile incidents in 2009, 2014, and 2018, and even cut off oil to its ally Belarus in 2020.[40,41,42,43,44]

European Energy Security: After Russia's 2022 Full-Scale Invasion of Ukraine

Since the weeks leading up to Russia's full-scale invasion of Ukraine in February 2022, the characteristics of Russian energy weaponization have become both broader and more dramatic in their impact. **[FIGURE 02]** shows the conceptual escalation of Russia's use of energy as a weapon over time, moving from security of supply threats, monopolistic practices, and strategic corruption in the lead up to 2022, to the dramatic tactics that are now ongoing, including military strikes to destroy Ukraine's civil energy network – likely aimed at exacerbating an already widespread humanitarian crisis across the country – and physical sabotage actions against energy and critical infrastructure installations across NATO Member States – likely aimed at undermining European resolve to provide support for Ukrainian victory. This is not to say that Transatlantic leaders did not long suspect the real potential that Putin's Russia might one day resort to the destruction of energy and critical infrastructure as a means of escalating pressure against European democracies. A former senior U.S. government policymaker with expertise in European energy and security issues emphasized that, "across multiple administrations, we worked to support European energy security, especially focusing on helping Europe diversify its supplies. But we also assumed Putin had a long list of physical infrastructure in the West — including energy infrastructure — that he would be prepared to take out someday. Why would he limit himself to cutting off (or threatening to cut off) oil, gas, or electricity supplies when he could physically damage or disrupt pipelines, cables, hydroelectric dams, or other key infrastructure?"

The reality foretold within this sage policy foresight has come to pass since 2022. As expected, Russia continued to follow its long-term security of supply threat strategy since its large-scale invasion of Ukraine. After all what good would years of building up European dependence on Russian energy supplies be if it were not dramatically utilized by Moscow for geopolitical purposes in a time of crisis of the Kremlin's making? These actions included dramatic cutoffs of both natural gas – such as the April 2022 cutoff of the Yamal-Europe natural gas pipeline to Poland and Germany, and the partial and then full cutoff of the Nord Stream 1 natural gas pipelines between June and September 2022 – and electricity – such as Russia's cutoff of electricity supplies to Finland in May

◀ ***[FIGURE 02] Illustration of the increasing scope and impact of Russian energy weaponization, which has over the years included threats of energy cutoffs, energy lawfare, strategic corruption and elite capture, but has increased most recently to physical sabotage of energy and critical infrastructure across NATO member state territories as well as overt kinetic military strikes against civilian energy and critical infrastructure installations across Ukraine.***

Figure Design: B. L. Schmitt / Template and Illustration: Petr Vaclavek, Terriana, Icons-studio, SkyLine, Genestro, Dewi, Cetacons – stock.adobe.com / Media Headlines: New York Times, Reuters, The Guardian, The Washington Post (full source list in Endnotes)[P15]

2022.[45,46,47,48]

Added to these supply cutoffs, however, was the launch of what could possibly be best described as Nordic media characterized in 2023: a "skyggekrigen" or "shadow war" – consisting of an ever-growing list of onshore and offshore incidents that have resulted in the physical damage of energy and critical infrastructure across the continent. Since the beginning of 2022 – just weeks before Russia's full-scale invasion of Ukraine – through to the present, there have been dozens of reports of damage to energy, telecommunications, and transportation infrastructure across the territory of NATO Member States. While many of these incidents remain under investigation, there have already been a significant number of cases in which European security officials have publicly attributed acts of sabotage to either Russian actors, or non-Russian nationals who have been recruited via the social media apps like Telegram to conduct a wide spectrum of infrastructure damage on NATO soil.[49,50] Sabotage attacks in which attribution has been possible have mostly taken place against onshore critical infrastructure, where, even in remote locations, infrastructure monitoring and the collection of forensic evidence can be straightforward compared to offshore environments. Since early 2022, there has also been a growing list of high-profile incidents of damage against energy and critical infrastructure located in offshore environments, ranging from the Barents to the Baltic seas. Given the relative lack of persistent monitoring required for total maritime domain awareness, the remoteness of these incidents, and the technical difficulty associated with subsea forensic investigations, most of these acts of suspected offshore sabotage have not yet resulted in official attribution, and as a result, have set off heated debates in the policy, military, expert, and commercial maritime communities.

And these debates, once centered across Northern Europe, are rapidly spreading to other far flung regions around the globe. ■

Naval sonar equipment demonstration during NATO exercise Dynamic Monarch 24, held off the Norwegian Coast. (September 2024) / DESIGN: B. L. Schmitt / PHOTO CREDIT: NATO Flickr[P6]

A Finnish Navy crew member looks through binoculars during Exercise Freezing Winds 24 in the Baltic Sea, focused on the protection of subsea energy and critical infrastructure. (December 2024) / CREDIT: NATO Flickr[57]

ASSESSING RUSSIA'S "SHADOW WAR"

This report – ***Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond (Volume 01)*** – is the first in the series of volumes that present findings resulting from research that has been the focus of a multi-year investigative project launched at the University of Pennsylvania, and is focused on exploring global energy security trends as they pertain to energy and critical infrastructure protection from suspected sabotage operations, including those potentially involving the Russian Federation and the People's Republic of China.[51,52,53]

As introduced in the previous sections, extending traditional energy security policy analysis to include the characterization and formulation of deterrence methods against a growing pattern of physical sabotage incidents against energy and critical infrastructure globally is essential. Not only do physical sabotage events specifically undermine the security of supply that threatens both acute and widespread energy poverty, the erosion of confidence in democratic institutions tasked with ensuring the resilience of such infrastructure is vital to sustain public support for future energy systems development, including those projects required to achieve a rapid, safe, and sustainable energy transition.

While many of the incidents studied in the context of the ***Underwater Mayhem*** research program have a distinct energy security nexus, the

report series will also consider threats to other critical infrastructure deployments, including telecommunications and transportation installations. This approach was taken as the authors felt it important to provide a sufficiently broad picture of the this current trend within which suspected energy infrastructure sabotage has taken place. Such a wider spectrum approach is required to properly analyze these trends since, among other factors, energy projects are often collocated with other types of critical infrastructure, and these systems are generally operationally interdependent. For example, distributed infrastructure networks like passenger and rail lines require both distributed electricity and telecommunications cables for reliable functionality of these transportation systems.

Moreover, the pathologies associated with attacking and defending subsea infrastructure carry many distinct similarities, whether one considers, e.g., subsea hydrocarbon pipelines, electricity interconnectors, or telecommunications cables. It is especially vital that the offshore energy and telecommunications industries understand the convergence of infrastructure security risks and related deterrence methods for their respective systems. Assessing the analogous vulnerabilities manifest across these subsea installations, and supporting cross-industrial synergies for response and deterrence represents a major theme found throughout this research program.

UNDERWATER MAYHEM: Project Overview

In addition to the assessment of the broader energy and national security dynamics at play, the ***Underwater Mayhem*** report series aims to provide a detailed characterization of several of the highest profile acts of offshore energy and critical infrastructure damage that have taken place since early 2022, in terms of their economic and geopolitical context, technical circumstances, official response, and potential climate impacts, including:

- **January 2022:** The cut of a subsea fiber optic telecommunications cable connecting the Norwegian archipelago of Svalbard with the Norwegian mainland.[13]

- **September 2022:** The destruction of three of the four trunklines comprising the Kremlin-backed Nord Stream 1 and Nord Stream 2 natural gas pipelines.[14]

- **February 2023:** The cutting of subsea telecommunications cables connecting the main island of Taiwan to the Taiwanese Matsu Islands.[15]

- **October 2023:** The destruction of the Balticconnector natural gas pipeline, as well as several subsea telecommunications cables connecting Finland and Estonia, and Estonia and Sweden.[16]

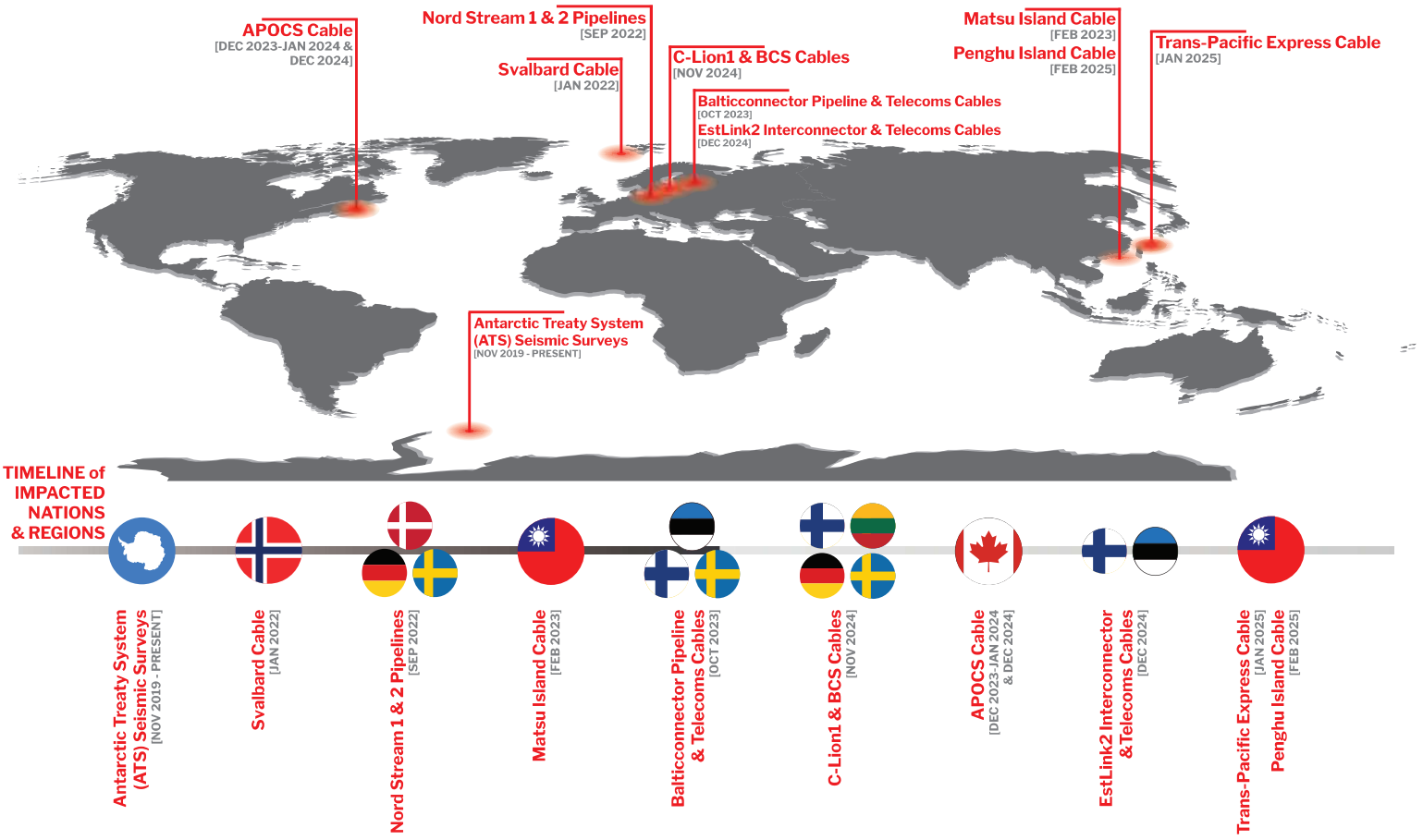
- **November 2024:** The cutting of subsea telecommunications cables spanning the Baltic Sea between Lithuania and Sweden, and Finland and Germany.[17]

- **December 2024:** The damage of the Estlink2 subsea electricity interconnector cable, as well as several subsea telecommunications cables connecting Finland and Estonia.[18]

- **Dec 2023-Jan 2024 and December 2024:** The cutting of a subsea telecommunications cable linking Cape Breton Island to Newfoundland in the Cabot strait in northeastern Canada.[19,54]

- **January/February 2025:** The cutting

Case Study Areas



▲ ***[FIGURE 03]*** *Map and timeline of impacted nations and regions for incidents and trends that serve as the primary research case studies of the Underwater Mayhem project.*

Figure Design: B. L. Schmitt / Template and Illustrations: korkun, stockdevil, S_E – stock.adobe.com[P8]

of subsea telecommunications cables connecting Taiwan with the United States, the Republic of Korea, and Japan, and a cable between the main island of Taiwan with the Taiwanese Penghu Islands.[20,21]

In addition to these case studies, a companion volume will be included that highlights a five-year study of the Russian Federation's actions to undermine provisions against commercially oriented hydrocarbon exploration and exploitation through seismic surveys conducted within the waters of the Antarctic Treaty System (ATS). Furthermore, this study will provide open-source AIS and commercial geospatial imagery of some of these same vessels that Russia has operated in the ATS maritime region suggesting their involvement in surveys of Western owned-and-operated critical subsea cables and related infrastructure around the globe.[55,56]

The security analysis and case studies included in this series aim to serve as a resource for investigators and policymakers striving to consider how best to characterize acts of suspected energy and critical infrastructure sabotage, especially in offshore and subsea domains. To satisfy this broad scope, the research for this report series has been conducted within a multidisciplinary framework to mirror the interdisciplinary nature under which these incidents took place. The global scope of the

Underwater Mayhem project is illustrated in **[FIGURE 03]**.

In this first volume, we provide case studies focusing on the first of the two aforementioned incidents in the order they occurred chronologically: the January 2022 Svalbard cable cut, and the September 2022 destruction of the Nord Stream 1 and Nord Stream 2 natural gas pipelines. This study aims to serve as a resource for investigators and policymakers considering how best to characterize these events and develop policy and technical responses to deter similar future incidents. The research included in this volume relies on field research, expert interviews, public reporting and primary source document review, and open-source intelligence (OSINT) data analysis and techniques, as detailed in **[BOX 02]**.

Additionally, some of the analysis and results presented in this report draw from ideas and text that were provided in oral and written testimony by author Schmitt on September 24, 2024, as a part of a U.S. Senate and House joint Congressional hearing entitled "*Russia's Shadow War on NATO*" hosted by the United States Commission on Security and Cooperation in Europe (CSCE) in the Cannon House Office Building in Washington, D.C.[57,58] In addition to the three coauthors of this volume, the detailed cataloging of suspected instances of suspected hybrid activities and energy and critical infrastructure sabotage was completed with support from several University of Pennsylvania student research assistants acknowledged later in this report.

The analysis presented in this report series is solely based on open-source and academic research, all unclassified in nature. Nevertheless, as an academic exercise, we have attempted to review and present our key assessments in terms of best practice metrics publicly set forth by, i.e., U.S. Intelligence Community public guidance, as well as related published academic studies and expert commentaries that we have reviewed and cited in this report, guiding our use of estimative language, words of estimative probability, judgements of likelihood, and confidence in assessment.[24,25,26,27,28,29]

Given that the ***Underwater Mayhem*** study is broad in scope and considers a variety of types of energy and critical infrastructure damage events across disparate global locations, it is essential to employ a standardized vocabulary for estimative probability and confidence in assessment to allow for comparative analysis between these incidents, and across multiple volumes. Additionally, it should be noted at the outset, that there is a fundamental difference in terms of evidentiary requirements when comparing between intelligence analysis of any type (including OSINT) and those thresholds for legal and/or criminal investigations.

Writing for RAND in an article entitled "The Big Difference Between Intelligence and Evidence" in 2003, military and intelligence author Bruce D. Berkowitz described the danger of the common yet false public expectation that intelligence estimates can usually reach a reasonable legal level of proof on par with that generally understood for criminal investigations.

As Berkowitz writes:

> *"Usually intelligence does not offer crystal-clear answers, and we should not hang decisions to go to war or do anything else on its ability to do so. In my own experience, intelligence is usually full of uncertainty. In the intelligence business, foolproof, airtight evidence — the kind that changes minds and convinces the public — is, as one of my first branch chiefs at the CIA used to tell me, as 'rare as hens' teeth." That's why expecting intelligence to provide 'proof" in the legal sense of the word is so dangerous.*

BOX 02

HOW WAS THE RESEARCH FOR "UNDERWATER MAYHEM (VOL. 01)" CONDUCTED?

The research in this volume relied on:

- *Field research conducted at or near the sites of where these offshore attacks took place across Northern Europe, including visits to: Longyearbyen, Svalbard in September 2023; onshore locations near both of the Nord Stream blast sites on the Danish island of Bornholm in July 2023 and January 2024; and an offshore research expedition to gather subsea sonar data of the Nord Stream 2 blast site southeast of Bornholm in September 2024;*

- *Interviews with dozens of experts on both sides of the Atlantic, which were conducted as off-the-record discussions in which notes were taken, and then on-the-record or on-background quotes were provided by the experts for use in this volume and approved in late-December 2024 (unless otherwise noted). The experts consulted for this report include:*

  - *Commercial leaders with expertise in offshore energy and critical infrastructure construction and operations*
  - *Commercial ship operators and related maritime industry professionals*
  - *Commercial and military divers and subsea demolitions experts*
  - *Current and former naval, military, coast guard, and law enforcement professionals*
  - *Current and former senior energy and national security officials*
  - *Leading experts and academics focusing on European energy and national security issues*

- *Open-source intelligence (OSINT) analysis, including maritime automatic identification system (AIS) data (particularly the MarineTraffic AIS platform) and commercial geospatial intelligence platforms (particularly the Planet optical-wavelength satellite platform)*[22,23]

- *Review of literature, academic analysis, and press reporting related to these incidents, and related primary source documents*

Detective work and intelligence collection may resemble each other, but they are really completely different.

Detectives aim at meeting a specific legal standard — 'probable cause," for example, or 'beyond a reasonable doubt" or 'preponderance of evidence." It depends on whether you want to start an investigation, put a suspect in jail or win a civil suit. Intelligence, on the other hand, rarely tries to prove anything; its main purpose is to inform officials and military commanders.

The clock runs differently for detectives and intelligence analysts, too. Intelligence analysts — one hopes — go to work before a crisis; detectives usually go to work after a crime. Law enforcement agencies take their time and doggedly pursue as many leads as they can. Intelligence analysts usually operate against the clock. There is a critical point in time where officials have to 'go with what they've got,"

ambiguous or not."[29]

While the Berkowitz analysis was written in the context of the question of the question of Saddam Hussein possessing weapons of mass destruction in the run up to the 2003 Iraq War, the same distinction is key to the way in which we can characterize levels of assessment versus "proof" related to the potential sabotage incidents appearing in the ***Underwater Mayhem*** project. In nearly all these subsea infrastructure damage cases, public discourse has been consistently unclear when considering the linguistic and estimative differences between national intelligence assessments related to these incidents, compared to the language and dynamics of the criminal investigations that national prosecutors have pursued in many of these cases.

For example, for incidents in which law enforcement and prosecutors have not been able to reach the burden of proof required to bring specific charges against a person or entity in a specific jurisdiction, it does not necessarily suggest that intelligence estimates do not provide a reasonable understanding of the nature of that same incident. Likewise, prosecutors closing a given investigation without reaching a legal burden of proof to bring charges, does not necessarily suggest that those same prosecutors would not be able to make a reasonable analysis of what has occurred under the broader rubric of intelligence assessments.

With this in mind, **[FIGURE 04]** illustrates the estimative language that is used throughout the ***Underwater Mayhem*** project to reach judgements of likelihood and to express confidence in those judgements. **[FIGURE 04]** is a reproduction of the metric set forth in a U.S. National Intelligence Council Intelligence Community Assessment from March 10, 2021, and provides the specific estimative language for the judgements that appear in this series roughly mapped onto the percentage of likelihood that is meant to be conveyed. Furthermore, we attempt to use the metric the U.S. Intelligence Community sets forth in the same document for self-assessment of said judgements in terms of low, moderate, and high levels of confidence. The entire estimative language page from the March 10, 2021 U.S. National Intelligence Council Intelligence Community Assessment document is provided as an appendix for reference.[24]

Pre-2022 Disruptive Russian Activities Involving European Energy and Critical Infrastructure

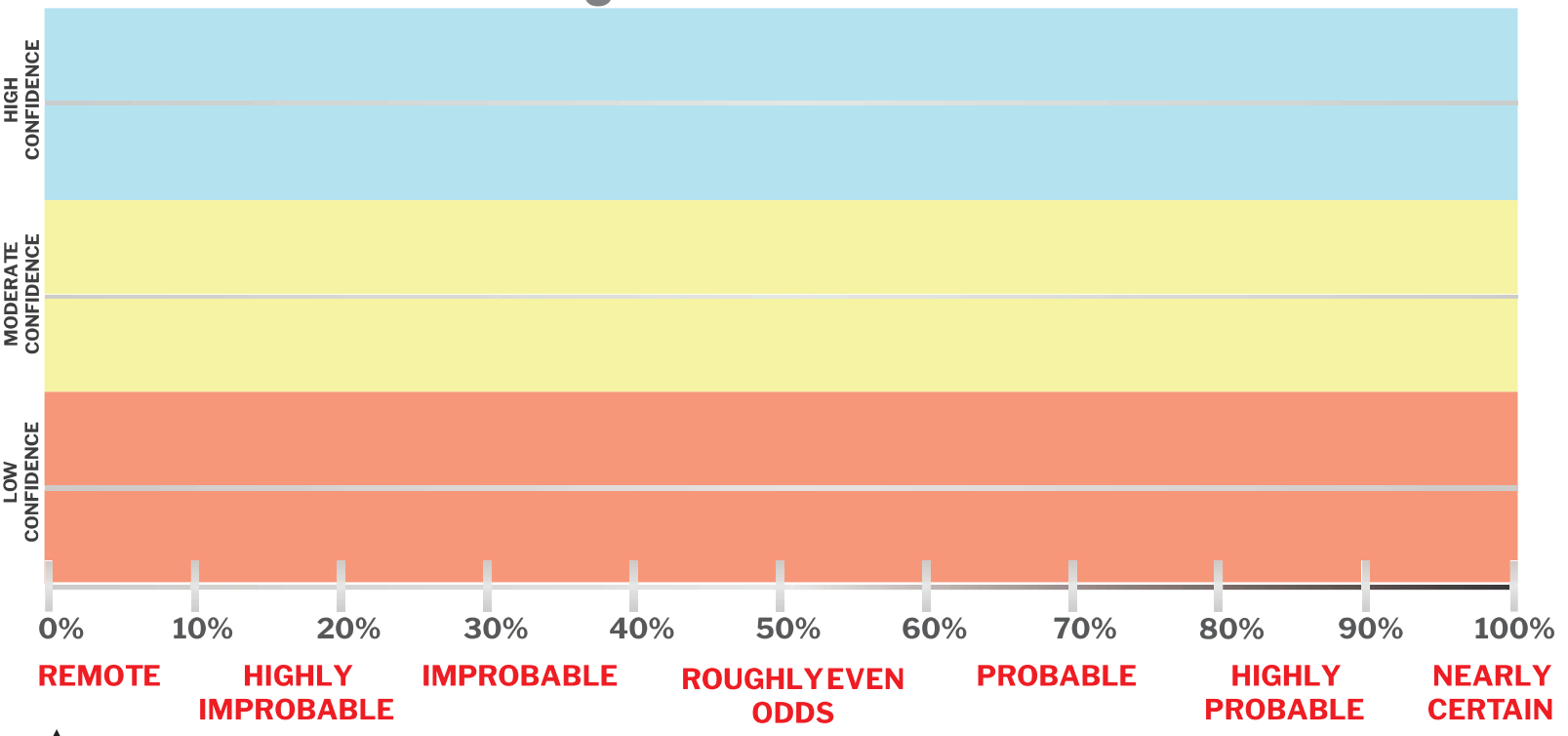
Although Russia's attributed and suspected sabotage actions against energy and critical infrastructure on NATO soil and across its waters have made headlines with increasing regularity since 2022, the Kremlin has taken steps to practice for the current contingency for years. From a policy standpoint, these incidents presaging the current crisis ought to have resulted in significant policy actions to address these warning lights that were flashing red well before Russia's February 2022 full-scale invasion of Ukraine.

Some pre-2022 examples of Russian actions taken to menace, attack, or otherwise disrupt energy and critical infrastructure systems in Ukraine and across NATO territory or waters include:

- **Russia's GUGI Fleet:** Repeated reports of Russia's development of systems, dual-use vessels, and military platforms that could enhance the Kremlin's ability to conduct subsea and seabed warfare, including reports that Russian submarines and a specially-designed surface vessel – the <YANTAR> – were publicly revealed by U.S. Naval Intelligence in 2015 to have been patrolling off the U.S. East Coast and loitering near vital Transatlantic telecommunications cables. A follow-up report in *Naval News* by the

INCIDENT ASSESSMENT:

Estimative Judgement and Confidence Level



▲ ***[FIGURE 04] A reproduction of the metric set forth in a U.S. National Intelligence Council Intelligence Community Assessment from March, 10 2021, and provides the specific estimative language for the judgements that appear in this series roughly mapped onto the percentage of likelihood that is meant to be conveyed.***

Figure Design: B. L. Schmitt as adapted from an Unclassified U.S. National Intelligence Council Intelligence Community Assessment document from March 10, 2021.[24,P9]

subsea warfare expert H. I. Sutton in 2021 showed that using OSINT data sources like AIS signals displayed on the commercial maritime-tracking platform MarineTraffic the <YANTAR> was again spotted operating near key transatlantic subsea cable infrastructure off the coast of Ireland, and pointed out the fact that while the <YANTAR> was often referred to by the Russian Federation as an "oceanographic vessel" for research, the vessel is operated by none other than "Russia's secretive Main Directorate of Underwater Research (GUGI) who also operate Russia's 'special mission' (read 'spy') submarines."[22,59,60]

- **Cyberattacks against Energy and Critical Infrastructure:** Repeated cyberattacks by Russia or Russia-aligned groups in 2015 and 2016 against Ukrainian power grid operators that resulted in widespread power outages for civilians across large areas of Ukraine. The December 2016 attacks specifically targeted Ukraine's capital city, Kyiv, and resulted in an outage of roughly "...200 megawatts of capacity, equivalent to about a fifth of the capital's energy consumption at night." Ultimately, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provided an update on July 20, 2021, stating that "The U.S. Government attributes this activity to Russian nation-state cyber actors and assess that Russian nation-state cyber actors conducted a cyber campaign against Ukrainian critical infrastructure."[61,62,63,64,65]

- **Impedance of European Offshore Energy Infrastructure**

Construction: Repeated disruption of the construction of the Sweden-to-Lithuania subsea electricity interconnector cable NordBalt in 2015 within the exclusive economic zone (EEZ) of Lithuania by Russian naval vessels operating in the central Baltic Sea region.[66,67]

If the actions highlighted here – and many more – that took place against onshore and offshore energy and critical infrastructure by the Russian Federation in Ukraine and in the maritime jurisdiction of NATO Member States over the past decade served as a prelude to the operations that Putin's Kremlin would undertake in the immediate run up to and following its full-scale invasion of Ukraine, then it could be argued that a turning point in the scale and severity of these Russian operations was highlighted by a dramatic incident that took place not on NATO land or maritime environments, but instead far above the heads of Transatlantic leaders in low-Earth orbit. That incident, the November 2021 Direct Ascent Anti-Satellite (DA-ASAT) Weapons Test by the Russian Military, which created a massive debris field endangering satellite and space station operations in low-earth orbit, will be covered in greater detail in the analysis of the context first case study involving the January 2022 cut of the Svalbard subsea telecommunications cable system.[91]

Moreover, according to Eero Kytömaa, Ministerial Advisor at the National Security Unit of the Finnish Ministry of the Interior, "it's important to remember that the spike in events causing damage to European offshore energy and critical infrastructure installations began in the weeks around Russia's large-scale invasion of Ukraine, and have only increased since then." Eero, who serves as a senior adviser on national security and hybrid threats to the Finnish government in Helsinki, and represents Finland in both EU and NATO critical infrastructure protection networks, added that, "whether we like it or not, given the uptick in malign activities, Europe must take a step back to assess the broader picture and conduct a clear-eyed evaluation of whether we are the target of sub-threshold warfare from Russia."

Likewise, speaking on Russia's proclivity to conduct such attacks, including in the maritime environment, Johannes Riber, an active-duty Commander in the Royal Danish Navy and a Ph.D. Fellow at the University of Copenhagen focused on sea power explained that, "Russian naval thinking for the last decade has been focused on using technology as a force multiplier, when competition at force levels of an opponent is impossible. Sinking [an] opponent's merchant navy, or destroying subsea infrastructure raises the stakes and can be aimed at pressuring populations to make diplomatic concessions to Russia. There is a long history of this in European warfare - for example, the French navy used the tactic of sinking British merchant vessels during the Napoleonic wars, and Putin's tactics against subsea energy and critical infrastructure mirrors such a tactic."

Pekka Virkki, a Finnish investigative journalist and author with expertise in national security and geopolitical trends in the Baltic Sea region described the trend in even starker terms, warning that "all of these sabotage incidents feel like Russia sending a mafia warning sign to Europe to not support Ukraine."

Trends Exhibited in Recent European Onshore Sabotage Attacks

Given the growing number of suspected onshore and offshore energy and critical infrastructure sabotage occurrences across Europe, it is vital to identify as a baseline any general trends that may exist among these incidents. To do so, our team has conducted a survey of suspected hybrid activities and sabotage incidents against energy and critical infrastructure between 2022 and

2024, and an excerpt from a larger repository created in this study that includes nearly 100 such incidents is included as an appendix with this volume.

Sabotage attacks in which attribution has been possible since 2022 have mostly taken place against European onshore critical infrastructure, where, even in remote locations, infrastructure monitoring and the collection of forensic evidence can be relatively straightforward compared to offshore environments.

A very small subset of examples of the wide range of onshore incidents, sabotage methods, and infrastructure targets that have been reported in recent years across NATO territory, include:

- **May 2025:** A cache of explosives and detonators was found *deliberately buried* in May 2024 next to a section of NATO's Central Europe Pipeline System (CEPS);[68,69,70]

- **July 2024:** A cell communications tower operated by Finnish telecommunication provider Elisa in Janakkala near Helsinki, Finland was knocked down following what authorities credit as "vandalism" when the tower support guy-wires were found cut;[71]

- **July 2024:** An arson attack on a cable shaft supporting DeutscheBahn rail lines near Bremen, Germany was responsible for a train outage in northern Germany;[72]

- **August 2024:** Reports in Germany emerged that long-range, military-grade surveillance drones had been tracked by German authorities operating over the ChemCoast Park in Brunsbüttel, Germany, adjacent to the Brunsbüttel floating LNG facility – the onshore pipeline for which was itself damaged in a separate sabotage action in late-2023 near Hetlingen, Germany;[73,74]

- **September 2024:** A cable in Norway connected to a "…jammer [that] had been set up at the far northern island [of Andøya] in connection with an international exercise…" had been found "…cut and destroyed…" according to reports from The Barents Observer.[75]

From the many onshore and offshore energy and critical infrastructure damage incidents that our team has tracked over the past two years, some trends emerge:

- **Attribution Can Be A Challenge:** A minority of incidents have thus far been positively attributed by authorities to be the result of any actor, and in some cases, speculation can cause debates regarding whether a given incident was deliberate sabotage or else the result of accidental means or technical fault. Indeed, it is useful to remember that not every incident of suspected sabotage considered by our team may ultimately be shown to be the result of a sabotage activity at investigation end. However, experts have highlighted that there also may be political motivations to (at least initially) characterize a deliberate incident as an "accident" given a reticence to "escalate" the state of the ongoing conflict with Russia beyond Ukraine's boundaries.

- **Nationality Can Be Disconnected:** While European security authorities have attributed suspected sabotage plans to Russian actors, the use of non-Russian nationals has also been a hallmark of many of these attacks. For example, a Russian national with "extensive ties to FSB and GRU officers" was arrested in France for plotting "destabilizing" acts to disrupt

***[FIGURE 05]** (Left) Detusche Bahn mobile app view announcing rail closure on the Siegburg/Bonn to Frankfurt airport high-speed ICE rail line due to sabotage on February 2, 2024. (Middle) Bonn main train station. (Right) Alternative rail line along the Rhine River taken by author Schmitt to make his flight home from the Frankfurt airport.*

CREDIT: B. L. Schmitt & DeutscheBahn iOS Mobile App (bahn.de)[68]

the Paris Olympics in July 2024. The trend of Russia's GRU recruiting non-Russian nationals (such as via social media apps like Telegram) to carry out sabotage actions has been reported across a number of European nations, including examples of:[76]

- Citizens from the Baltic states recruited by the GRU "to vandalize and set fire to targets in the West" according to Latvian and Estonian court documents;[77]
- The GRU targeting as recruits "young, marginalized people, often immigrants and mostly men" to carry out sabotage activities, including the case of a Ukrainian immigrant caught operating in Poland;[78]
- The case of the arson of a Ukrainian-linked business in the United Kingdom, for which multiple British citizens were charged in April 2024 with "assisting a foreign intelligence service" (in this case, Russian intelligence) "as well as aggravated arson" among other charges.[79]

- **Infrastructure Targets and Sabotage Methods Widely Vary:** Suspected sabotage incidents in Europe since 2022 have included a wide range of targets, from natural gas pipelines and electricity grids, to telecommunications cables and cell towers, to rail and logistical hubs. Some incidents that have been stopped by the apprehension of suspects by European authorities before attacks could be perpetrated have explicitly targeted sites with links to EU and U.S. logistical support of Ukraine's military. Moreover, the suspected sabotage methods have widely varied, with arson and cable cuts among the most frequently suspected methods.[80]

One of the authors of this report, Schmitt, wrote about his own experience with a still unattributed case of a German high-speed rail-line electricity cable being cut between Bonn and Frankfurt and directly impeding

travel (ironically) associated with the research of this report in late January 2024.[68] An excerpt from Schmitt's first-hand account as published in mid-2024 with the Center for European Policy Analysis (CEPA) is provided here, and an illustration of the incident appears in **[FIGURE 05].**

> *"I attended an academic workshop in Bonn, Germany, focused on European energy security, including the Nord Stream 2 saga and the emerging trend of attacks against European infrastructure. On the last day of the meeting, just after discussing the continent's vulnerability to hybrid (or gray zone) threats and potential European Union (EU) and NATO responses, I turned to finding a ticket to the airport for my return flight to the US.*
>
> *Logging onto the Deutsche Bahn mobile app to secure one of the regular high-speed trains to Frankfurt airport, I found a flurry of red text next to every departure. 'Trip is not possible" and 'Stop Cancelled" it said. The explanation was one I had not encountered before: 'Problems due to vandalism."*
>
> *Taking a slower train, I spotted news reports revealing the cause of the chaos: 'Deliberate damage to the power lines," which had been 'tampered with" on the Cologne-to-Frankfurt high-speed ICE route, and 'metal theft in the Siegburg/Bonn area."*
>
> *The irony was unmissable. Attacks on this key transit route meant I had to leave early from an event focused on policies to deter precisely such infrastructure attacks.*
>
> *As sabotage goes, the broader impact was mild. There were no reported rail accidents or casualties, and the rail corridor was quickly repaired and reopened. I made my flight with a few minutes to spare. For the German public, the attack may have just blended into the ongoing delays already inundating their strike-ridden public transit network.*
>
> *But viewed more broadly, this rail incident joins many others in Germany and across the EU since Russia's full-scale invasion of Ukraine in February 2022. A similar attack took place in October 2022, just days after the blasts that damaged three of the four subsea trunklines of the Nord Stream 1 and 2 pipelines. On that occasion, Deutsche Bahn was forced to halt rail traffic across much of Northern Germany after the near-simultaneous severing of primary and backup communications cables roughly 200km (124 miles) apart.*
>
> *Hours after the incident, multiple German officials characterized the event as intentional, and Transportation Minister Volker Wissing decried it as a 'targeted and malicious action." But Reuters reported shortly thereafter that German police had concluded there was no foreign state involvement. The next day Wissing issued a statement reversing the police conclusion, describing it as sabotage and saying that he couldn't rule out foreign responsibility.*
>
> *By May [2024], a German senior investigator on the case told the Wall Street Journal that 'it smells like Russia. It looks like Russia."*[81,82,83,84,85,86,87,88,89,90]

In the sections, which follow, we will take a deep dive into two case studies of subsea energy and telecommunications infrastructure damage taking place far below the surface of the Barents and Baltic Seas.

PHOTO: Svalbard Cable Landing Station, Svalbard, Norway (September 2023)
MAP PROFILE: GoogleEarth / CREDIT: B. L. Schmitt

View of the SvalSat commercial satellite data ground station near Longyearbyen on the archipelago of Svalbard, Norway. (September 2023) / CREDIT: B. L. Schmitt

CASE STUDY 01: SVALBARD CABLE

Based on the work of this case study **[FIGURE 06]** illustrates the estimative assessments and corresponding levels of confidence in our assessment regarding the probability of the suspected culprit for the January 2022 Svalbard subsea cable cut. This compact research study integrates open-source AIS, commercial satellite imagery analysis, expert interviews, site visits, and the review of existing investigative media reporting and public primary source documents to achieve our findings.

Summary of Key Assessments

The summary of the key assessments illustrated **[FIGURE 06]** goes as:

- Based on open-source AIS analysis, expert interviews, site visits, and the review of investigative media reporting and related public literature, we assess as ***highly probable*** that the Svalbard subsea cable was cut by a commercial fishing trawler, the Russian Federation flagged <MELKART-5> (IMO: 9130183).[30]

- We have a ***moderate level of confidence*** in this judgement. We also note that as of the writing of this report volume, public attribution for the culpability of the Svalbard cable cut has yet to be officially made by Norwegian authorities.

- Moreover, experts suggested that this event may have been a so-called military "shaping operation" by the Russian Federation ahead of Moscow launching its full-scale invasion of Ukraine that would follow just six weeks later.

Incident Brief

Infrastructure Name:

Svalbard Undersea Cable System

Infrastructure Type:

Subsea fiber optic telecommunications cable

Geographic Details:

Landing points at Breivika, Norway and Longyearyben, Svalbard, Norway

Length:

2,714 kilometers

Ownership:

Space Norway[173]

Operational Status at Time of Incident:

Operational

Incident Overview:

On January 7, 2022 at 04:10 hrs, one of the two subsea fiber optic cables comprising the Svalbard Undersea Cable System lost signal. In the weeks following the outage, one of the two cables was found broken by investigators, the damage of which was later reported by Norwegian public broadcaster NRK nearly two years later in May 2024, and suggested a damage scenario in which the "outermost layer" of the cable was "peeled off…[and]…reinforcement broken." Furthermore, according to NRK, "the tear enabled seawater to come into contact with a copper layer carrying electrical current in one of the two cables that together make up the Svalbard fiber. The current is used to amplify the fibre optic signals that flow through the 1300km long cables between the peninsula and the Norwegian mainland. Because of the breakage, the current went straight to ground, and the cable stopped working." Moreover, according to the manager of a Norwegian subsea telecommunications operator, speaking on background reacting to the images of the broken cable provided in the NRK report, "one might say that the pictures show damage after scraping or pinching by an object that has passed over or along the cable. This could typically be a trawl door or something that is towed along the sea floor."[174,175]

Primary Accounts of Incident

One of the areas of focus for this report series has been to better understand and, when possible, publish first hand accounts from law enforcement, coast guard, and military officials that often serve as the first responders to these European offshore energy and critical infrastructure sabotage incidents, as well as civilians that had first hand experience at or near the incident sites.

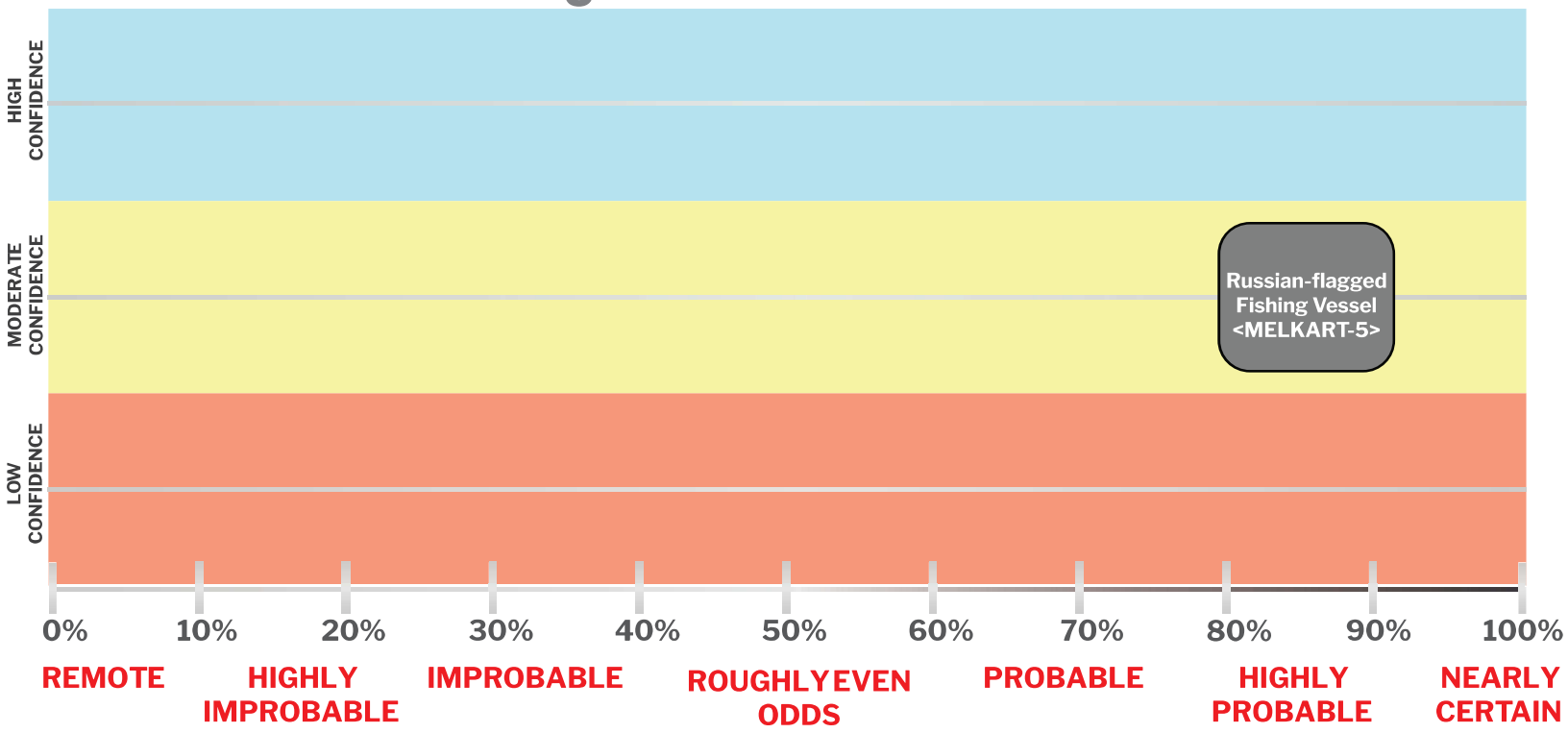
This section provides one such full on-the-record statement in the box on the opposite page, from an interview conducted during a visit to Svalbard in September 2023.

OSINT and Field Analysis

This case study involved both a field visit to Svalbard to conduct expert interviews, and included visits to both the Svalbard cable landing site near Longyearbyen, as well as the SvalSat satellite ground station, located on a plateau near Longyearbyen. Imagery of both sites can be found in **[FIGURE 07]**.

OSINT analysis in this case study relied

SVALBARD CABLE CASE STUDY ASSESSMENT:
Estimative Judgements and Confidence Levels



[FIGURE 06] Svalbard Cable Cut Case Study Assessment with Estimative Judgements and Confidence Levels based on metrics set forth and cited earlier in this volume.

FIGURE DESIGN: B. L. Schmitt as adapted from an Unclassified U.S. National Intelligence Council Intelligence Community Assessment document from March, 10 2021[24]

BOX 03

Terje Aunevik, Mayor of Longyearbyen, Svalbard, who previously served as founder and CEO of the Longyearbyen-based firm Pole Position Logistics from 2012 until April 2024.

At time of discussion in September 2023, Mr. Aunevik was running for Mayor, and ultimately was elected to the post just weeks later. He ran on a platform that would support a transition to sustainable energy production on Svalbard. Terje originally moved to Svalbard in 1998 to work as a dog musher. He later founded a technical logistics company focused on supporting scientific expeditions in the Arctic, and now the firm increasingly supports expedition ecotourism as well. As a result, overall port calls in Longyearbyen have grown quite a bit since he first moved to the community in 1998.

According to Aunevik, four Russian research vessels had formerly visited Svalbard over the years, including the <AKADEMIK IOFFE>, the <AKADEMIK SERGEY VAVILOV>, the <PROFESSOR

MOLCHANOV>, and the <PROFESSOR MULTANOVSKIY>. Since Russia's large-scale invasion of Ukraine these vessels have not visited Svalbard.

Pole Position logistics had a contract for logistics to support the construction of the subsea fiber optic cable connecting Svalbard with the Norwegian mainland around 2006. Before the cable was constructed, KSAT had to download satellite data onto physical drives and Pole Position Logistics would then need to ship them to the mainland via DHL to get the data to clients. NASA had co-financed the cable construction with Space Norway. Terje was actually aboard the Maersk ship during the physical laying of the cable project.

Russian fishing vessels, including those that operate around Svalbard, no longer have permission to make port calls in Norway aside from Kirkenes, Batsfjord, and Tromsø. As a result, Russia now operates offshore freezer vessels where the Russian fishing vessels transfer their catch during expeditions. The Russian freezer vessels generally sit off of Svalbard near Bellsund, an Arctic Sound southwest of Longyearbyen.

In the case of a scenario in which both fiber optic cables were cut, Svalbard does have the ability to make contact to the mainland via Iridium satellite communications and other platforms, but at lower bandwidth than the cables provide.

"In the past, we had generally treated these Russian vessels as normal fishing vessels, but we now look at them much differently. I have seen many Russian fishing vessels operating in these waters for years, including the <MELKART-5> that was the vessel that operated directly over the seabed fiber optic cable before it was cut. The sailing pattern for the <MELKART-5> was, frankly, weird - it would be an extraordinary activity for the vessel to focus its fishing maneuvers so directly over the cable like it did.

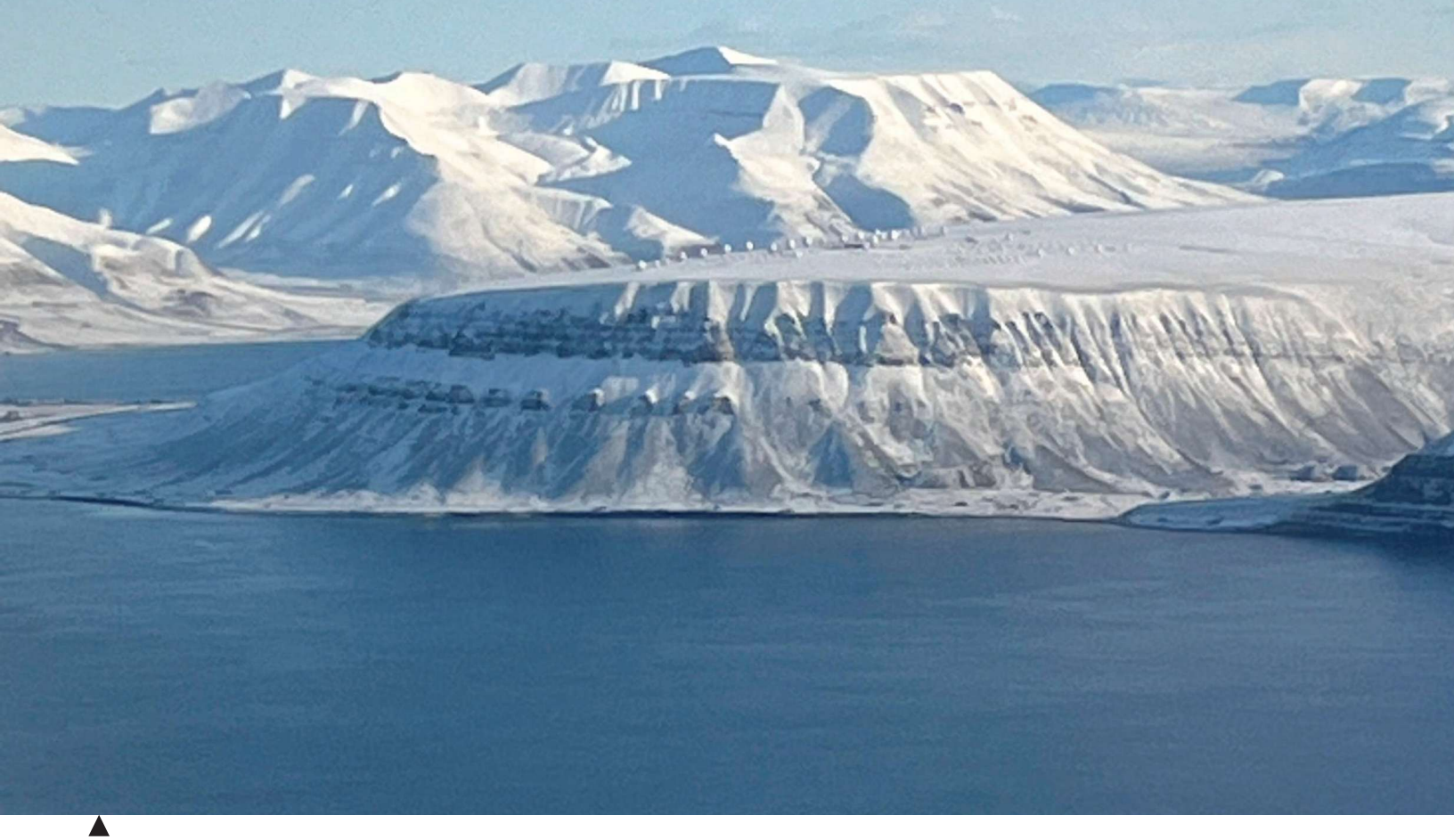
Thankfully, the cable cut didn't have a disastrous impact, as the redundant fiber optic cable had not been cut, but this incident raised the stakes significantly in terms of threat perception and the need to strengthen offshore infrastructure protection.

It seems now clearer than ever that Russia uses some of its commercial fleet for intelligence and military use, as was informally suspected in Norwegian circles for a long time."

solely on AIS data analysis, and found the same pattern uncovered by NRK researchers during their investigation of the incident, with the Russian-flagged fishing vessel, the <MELKART 5> shown to have sailed vigorously over where the cable would be cut in the days leading up to the cut incident – over 140 times according to NRK researchers, as described in the following section. **[FIGURE 08]** illustrates the limited OSINT AIS analysis conducted during this research study. Note that no Planet optical satellite imagery was available during the weeks surrounding the cut, likely owing to both the remote maritime environment involved, and since the Arctic location was in a period of 24-hour darkness at the time.

Policy Context and Expert Analysis

On November 15, 2021, the Russian military conducted a destructive "...direct-ascent anti-satellite test [(DA-ASAT)] that blew Kosmos-1408, a derelict Russian spy satellite, into more than 1,500 pieces of space debris." The event, which took place as the Russian military was building up troop and materiel presence along the Ukrainian periphery, was likely aimed at further warning Transatlantic leaders that support for Kyiv against Russia's large-scale invasion of



Aerial view of the SvalSat commercial satellite data ground station near Longyearbyen on the archipelago of Svalbard, Norway. (September 2023) / CREDIT: B. L. Schmitt

Ukraine would be met with threats to critical infrastructure – even against advanced orbital military and intelligence platforms, as well as potentially against communications and geospatial imagery satellites that have been deployed over the past five years in what is commonly considered our current commercial space renaissance.[176]

Extending this concept, just weeks after the DA-ASAT forced NASA and European Space Agency astronauts – as well as Roscosmos cosmonauts – to shelter in place aboard the International Space Station (ISS) and mission control to maneuver the ISS to dodge the space debris from that Russian space weapons test, another strike against infrastructure vital to the global space economy took place. However, this incident happened not hundreds of miles above Earth's surface, but rather in the frigid depths of the Barents Sea.

On January 7, 2022, one of two subsea fiber telecommunications cables connecting the Norwegian archipelago of Svalbard with mainland Norway were cut, reducing the bandwidth for data traffic to and from the islands. The damage site, which was located just off of the western coastline of Svalbard, was identified using AIS data analysis by investigative journalists Håvard Gulldahl and Inghild Eriksen from Norwegian public broadcaster NRK as having corresponded to a location that a Russian-flagged fishing trawler, the <MELKART-5> had "crossed the Svalbard cable more than 140 times, and more than a dozen times before the damage occurred in January 2022."[175,177]

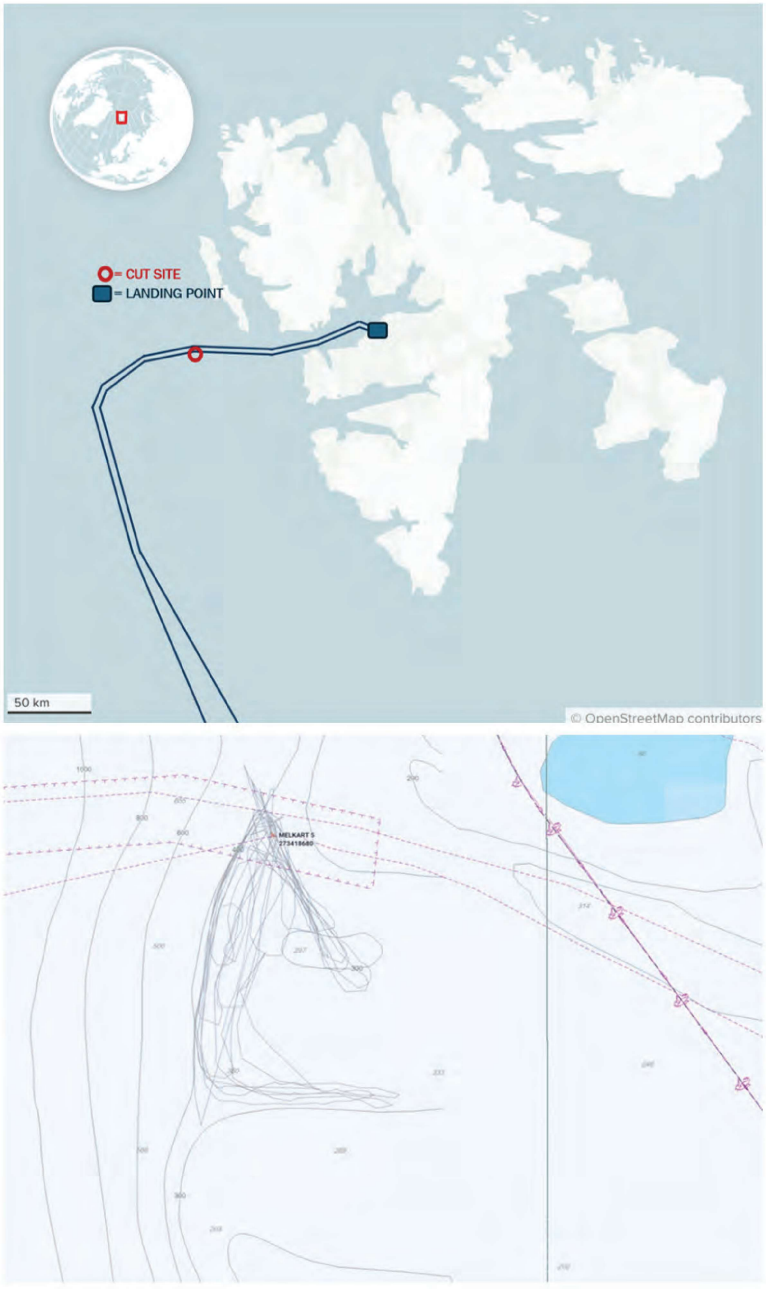
While Gulldahl and Eriksen reported that "the shipowners have denied having anything to do with the damage" the potential that this was in fact Russia-backed sabotage remains non-trivial. First, a pan-Nordic public broadcasting investigation reported in 2023 that the Russian Federation is increasingly using purported "commercial," "fishing," and "research" vessels to conduct espionage around energy and telecommunications

▲ *[FIGURE 07] Field research visit to SvalSat station and environs. (Top, Left) SvalSat ground station radome installation. (Top, Right) SvalSat station antenna, (Bottom, Left) Svalbard subsea cable landing site near Longyearbyen, Svalbard. (Bottom, Right) SvalSat station plateau view.*

PHOTO CREDIT: B. L. Schmitt

installations and infrastructure across Northern Europe – a trend that appears to be a growing central tenet of Russian maritime warfare and intelligence doctrine. For example, in early-October 2022 reports emerged from NRK that a Russian "research" vessel, the <AKADEMIK B PETROV> had been spotted transiting near strategic Norwegian offshore oil and gas infrastructure, with Norwegian academic researchers commenting that the vessel had "...more antennas than normal ships, it seems to have a large sensor capacity..." and that the ship "...has winches that can put things into the water...therefore [having] equipment that makes it well-suited to carry out missions other than pure research."[178,179,180]

Furthermore, the Svalbard fiber cable cut impeded vital commercial satellite data that



▲
[FIGURE 08] (Top) Geographic overview of the Svalbard Undersea Cable System (general path shown for illustrative purposes only. (Bottom) MarineTraffic AIS path excerpt of the Russian-flagged fishing trawler <MELKART-5> focusing turning radius over the southern Svalbard cable trunkline, which was ultimately cut. AIS excerpt MarineTraffic time stamp is January, 7, 2022 at 01:58:18 UTC.

FIGURE DESIGN: B. L. Schmitt as based on Telegeography online submarine cable map data, map created in Datawrapper and AIS data from MarineTraffic.[22,186,187]

would need to traffic the Svalbard Satellite Station, or SvalSat, which is a large-scale commercial satellite ground station that according to the U.S. Geological Survey (USGS) is the "...only commercial ground station that can support polar orbiting satellites every time they orbit the Earth, about 14 passes per day..." which make the installation "...an advantageous place for satellite control and downloading data." Given the role that commercial geospatial imagery and communications data would play in the support of Ukraine just weeks later, the strategic motivation for the Kremlin to potentially target such a subsea cable is evident.[181]

Russia's attacks against ground and space communications infrastructure with impacts on energy infrastructure continued during the opening hours of its large-scale invasion of Ukraine in late-February 2022. This included an attack reported by MIT Technology Review in which "...just an hour before Russian troops invaded Ukraine,

Russian government hackers targeted the American satellite company Viasat." That attack, which was nominally meant to impede Ukraine's communications systems needed for its defense, in turn, according to a June 2024 report from the United Kingdom's Alan Turing Institute "affected space-based assets engaged for command and control of Enercon's wind turbines in Germany, leading to the loss of remote monitoring access to more than 5,800 wind turbines."[182,183]

According to Tom Røseth, Associate Professor of Intelligence Studies at the Norwegian Defence University College, Command and Staff College, "Russia regularly operates maritime vessels across Northern Europe who sail under the guise of being "fishing" or "research vessels" when in fact their primary mission is to support activities of the Russian intelligence services." He ironically added, "there must be very good stocks of fish directly around the Svalbard cable to justify just how intensively the Russian fishing vessel was operating exactly over the site where the seabed cable cut would later be found."

Arild Moe, Research Professor focused on the Russian energy sector and geopolitical issues in the High North including Svalbard, at the Fridtjof Nansen Institute in Lysaker, Norway echoed these statements, pointing out that, "it is now widely understood that some Russian fishing vessels operating in Norwegian waters, including those calling at Svalbard, may be in fact operating with military-intelligence intent. As a result, Norwegian authorities have begun to crack down on these vessels, increasingly inspecting Russian vessels calling at Norwegian ports. To this end, it appears likely that a Russian fishing vessel may have been behind the cutting of one of the Svalbard cables, with the vessel possibly operating as such a Russian "spy ship.""

Furthermore, according to Eriksen and Gulldahl, regarding Russia's use of non-military or intelligence vessels for those purposes, "that we have uncovered is the extensive opportunity for Russia to use civilian vessels for intelligence gathering and other covert activities. Our findings highlight that this capability is closely tied to outdated and insufficient international maritime laws. These legal shortcomings make it difficult to attribute responsibility or prosecute such actions, even of it should come to sabotage, which in turn hampers efforts to inform the public about incidents at sea. This is a concerning development, according to sources, as it demonstrates how these legal gaps can be exploited, making space for hybrid threats towards critical infrastructure and undermine democracies. In the case of the Svalbard fiber optic cables— our first documented instance of damage to critical underwater infrastructure— there are unlikely to be further answers unless there is a significant shift in relation to Russia or the cable loses its critical global importance. The investigation has been closed, and public access to information has been restricted due to national security concerns." To this end, Mattias Lindholm, spokesperson for the Swedish Coast Guard, based in the port of Karlskrona, Sweden, pointed out that Russian "research" vessels including those with the prefix "Professor" and "Akademik" are definitely a cause for concern since, "the "PROFESSOR" and "AKADEMIK" ships have always been there and their activities go up and down over time - and it is not always obvious if those on board are military or civilian."

Nevertheless, given that the incident took place just six weeks ahead of Russia's large scale invasion of Ukraine, and the fiber optic cable carried commercial satellite data, likely including Starlink internet and commercial geospatial imagery data from satellite providers like Maxar and Planet, and given that all of these would have significant value in Ukraine's defense, General Hodges assesses the incident to be a so called military "shaping operation." As Hodges points out, "this was clearly a shaping operation, intended to disrupt our

communications and surveillance capabilities ahead of their full-scale invasion of Ukraine. The Russians see our reluctance to acknowledge actions like this as aggression that must be punished and will continue to do so until we can change our own posture and develop appropriate responses and policies. The overriding mentality of avoiding escalation only invites more aggression. Our approach has failed consistently over the last 20 years and will continue until we stop it.” ■

View of Tromsø harbor in Tromsø, Norway. (September 2023) / CREDIT: B. L. Schmitt ▶

View of headquarters of SvalSat satellite ground station operator KSAT in Tromsø, Norway. (September 2023) / CREDIT: B. L. Schmitt ▼

PHOTO: Energy Infrastructure Protest Sign, Bornholm, Denmark (August 2023)
MAP PROFILE: GoogleEarth / CREDIT: B. L. Schmitt

Public display of Nord Stream 2 pipeline pipe segment in Hanko, Finland. (April 2025) / CREDIT: B. L. Schmitt

CASE STUDY 02: NORD STREAM

The September 2022 sabotage of the Kremlin-backed Nord Stream 1 and Nord Stream 2 natural gas pipelines by subsea explosives created a dramatic churning maw of methane in the western Baltic Sea - a manmade outgassing of methane entirely unprecedented in scale.

The event captivated global audiences, launched investigations and heated debates over responsibility, and – as a higher profile incident compared to the Svalbard cable cut – arguably ushered in an escalating series of high-profile acts involving suspected energy and critical infrastructure sabotage across northern Europe and beyond.

Nevertheless, as shocking a sight as the outgassing zones for each of the Nord Stream detonations sites may have been, given longstanding security concerns with the deployment of Russian subsea energy infrastructure in the middle of the Baltic Sea, they may have also come as little shock to many experts who have been following this issue for years. In fact, as we explore in this case study, there were many security policy warning signs that events like this were never out of the question once energy infrastructure deployments from Russia were deployed in a compact and strategic maritime environment in northern Europe.

During the research period in which this case study was completed, three

competing narratives had largely emerged within the Transatlantic community regarding likely actors behind the sabotage of the Nord Stream 1 and Nord Stream 2 natural gas pipelines, including (i) the United States military supported by Norway, (ii) a group of Ukrainian commandos operating from a rental sailboat, and (iii) specialized naval and seabed warfare assets of the Russian Federation.

Summary of Key Assessments

Based on this the work of this case study **[FIGURE 09]** illustrates the estimative assessments and corresponding levels of confidence in these assessments regarding the probability of each of the three leading narratives combining the open-source AIS, commercial satellite imagery analysis, expert interviews, site visits, and the review of existing investigative media reporting and public primary source documents.

The summary of these key assessments illustrated **[FIGURE 09]** goes as:

- Based on open-source AIS and commercial satellite imagery analysis, expert interviews, site visits, and the review of investigative media reporting and related public literature, we assess as ***highly improbable*** the theory that the United States military (with help from the Norwegian military) was to blame for the Nord Stream 1 and Nord Stream 2 sabotage.

- Furthermore, we assess as ***improbable*** that a group of Ukrainian commandos operating from a rental sailboat was behind the destruction of the Nord Stream 1 and Nord Stream 2 pipelines.

- Moreover, we assess as ***probable*** that the Russian Federation was involved in the Nord Stream sabotage incidents.

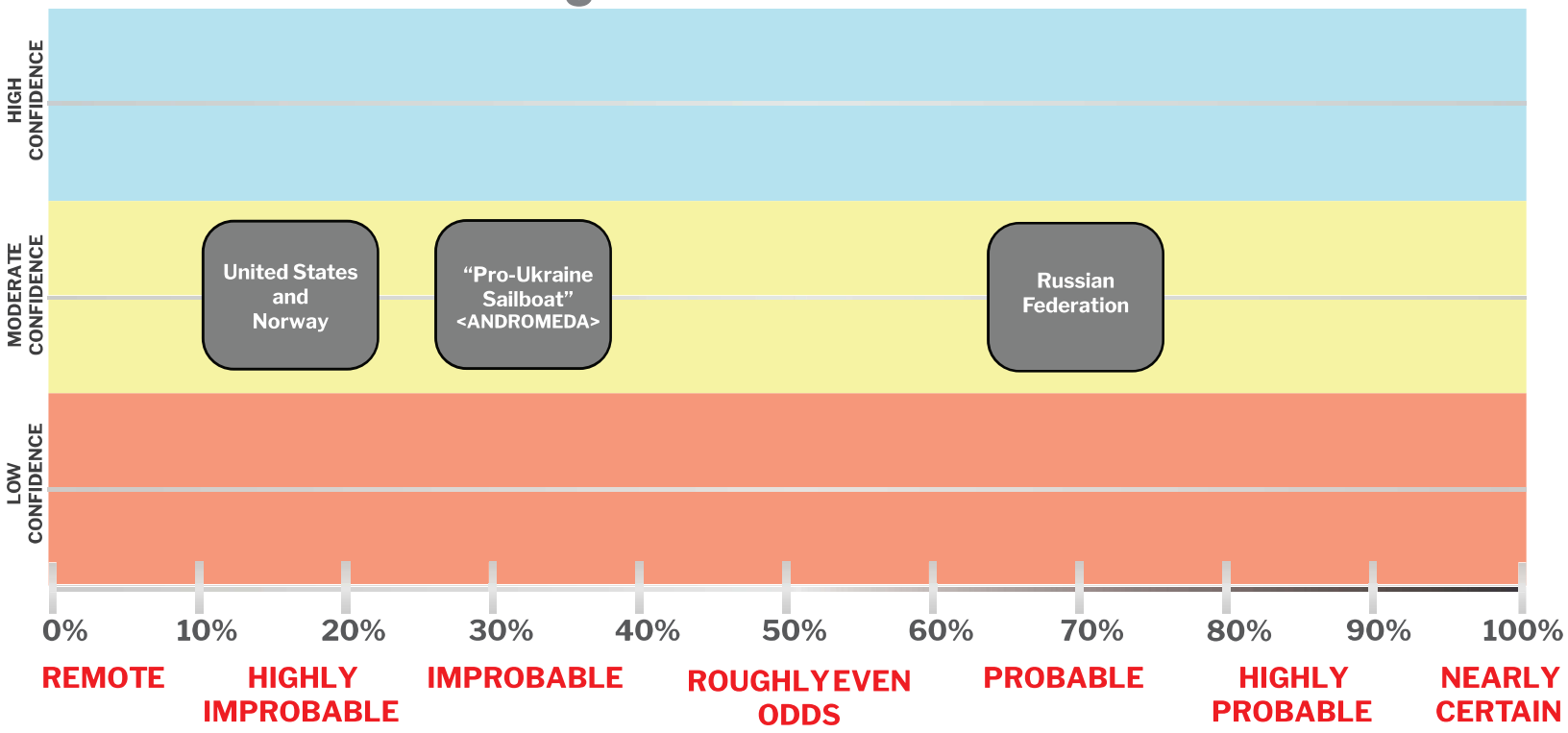
- We have a ***moderate level of confidence*** in these three judgements. A wide range of open questions regarding the Nord Stream incidents that we identify in this report preclude us from increasing beyond 'probable' the judgement of the Russian Federation's potential role in the incident and likewise cannot decrease beyond 'improbable' for the 'pro-Ukraine rental sailboat' or beyond 'highly improbable' for the 'United States and Norway' theories.

- The basis for these judgements and our confidence in them, is driven by significant questions regarding the technical feasibility, circumstances, and geopolitical motivation of the 'pro-Ukraine sailboat' explanation of the bombing, as well as the largely-publicly-debunked nature of the United States and Norwegian military explanation of the bombing. These questions were combined with the significant open-source data showing the extensive seabed warfare capabilities that the Russian Federation had at what would become the blast sites both months and then days ahead of the attack, the presence of Russian construction vessels directly over one of the eventual blast sites for significant periods of time in 2021, as well as the geopolitical and economic motivations that may have driven Moscow, among other data which is presented in this case study.

- We note that as of the writing of this report volume, public attribution for the culpability of the Nord Stream 1 and Nord Stream 2 sabotage incidents has still not been made by investigators in any jurisdiction of the Transatlantic community.

NORD STREAM CASE STUDY ASSESSMENT:

Estimative Judgements and Confidence Levels



▲ ***[FIGURE 09] Nord Stream Case Study Assessment with Estimative Judgements and Confidence Levels based on metrics set forth and cited earlier in this volume.***

FIGURE DESIGN: B. L. Schmitt as adapted from an Unclassified U.S. National Intelligence Council Intelligence Community Assessment document from March 10, 2021[24]

In the case study, which follows, we provide a deep dive into the wide spectrum of expert interviews, first-hand accounts, and open-source data analysis that have contributed to our key assessments associated with the September 2022 Nord Stream 1 and Nord Stream 2 natural gas pipeline sabotage incidents.

While deeper detail is provided throughout the case study, a top line summary of just some of the central findings of our research that led us to these key assessments are:

- The Russian Federation has been demonstrated to regularly recruit and use non-Russian nationals, including those from Eastern European nations, to carry out vandalism and sabotage attacks against critical infrastructure across Europe in recent years.

- The Russian Federation has been shown via open-source AIS data and commercial satellite imagery to have deployed military vessels, some with subsea warfare capabilities at the eventual site of the Nord Stream 1 sabotage northeast of Bornholm just days before the incident, as well as at the same site months earlier in June 2022. Furthermore, the Russian Federation had construction vessels stationed over the exact spot southeast of Bornholm already for lengths of time in the first half of 2021, in which the Nord Stream 2 incident would take place. In this context, we also present the findings of an October 2021 think tank report suggesting that Russian "military personnel" had been observed aboard Russian vessels "in the work zone" in 2021.

- Combined open-source AIS and

commercial satellite analysis completed for this report found that there were vessels observable as "dark vessels" (without their AIS enabled) within the immediate vicinity of the Russian construction fleet for Nord Stream 2 in 2021.

- The marina in which the eventual alleged "pro-Ukraine" rental sailboat would be rented from in Germany, is physically located in close proximity within the same port as a logistical deployment facility utilized by the Russian Nord Stream 2 construction fleet in 2021.

- Open-source AIS monitoring demonstrated that after the Nord Stream sabotage incident, at least three Russian-flagged vessels attempted to approach the blast site investigation areas, which appear to have been intercepted and escorted away from the sites by Swedish, Danish, and United States naval and coast guard assets. All three of these Russian-flagged vessels were later observed at the October 2023 Balticconnector natural gas pipeline damage site in the Gulf of Finland, either during the incident (in the case of the Russian-flagged nuclear class icebreaker <SEVMORPUT>), or in the days following that incident.

- Multiple commercial and military technical divers and subsea demolitions experts who were interviewed for this study raised significant questions regarding the assertion that it would be technically feasible (though not impossible) for the rental sailboat <ANDROMEDA> to have been used as the platform for an operation of this scale, as alleged by multiple media reports in the recent past.

- While media reports have suggested that the alleged <ANDROMEDA> sabotage operation was directed by the former Chief of the Ukrainian General Staff Valeriy Zaluzhnyi, a current U.S. government official raised concerns with this claim, citing that such an operation would not have been under the operational capacity of Zaluzhnyi, a point echoed by several experts.

- Senior Polish national security officials interviewed for this study claimed that "Poland's intelligence shared data on the Nord Stream sabotage case with German officials, and the findings suggested Russian actors may have been behind the attacks."

- Investigative journalists have publicly reported on the details surrounding some of the individuals that have been reported in, e.g., public German media accounts, to have been behind the <ANDROMEDA> operation, showing that at least one of the alleged team appeared to be freely living within the Russian Federation in 2023 after the attacks took place, as well as others reportedly "under investigation for trying to overthrow the Ukrainian government."

- Experts interviewed as a part of this study have commented on past instances of suspected Russian damaging of its own energy infrastructure as a potential means of creating a *force majeure* scenario for Gazprom and other Russian entities.

- Despite the recent prevalence of the rhetorical question "why would Russia destroy its own pipeline?" expert interviews and analysis conducted for this study suggest that the Russian Federation arguably did have possible motivation to sabotage the Nord Stream pipelines, including on

economic, security, and legal grounds.

- The Russian Federation had launched a disinformation campaign in the hours after the Nord Stream blasts took place, and continued to place blame in a variety of directions simultaneously in the months after the incident.

- The Biden Administration had demonstrated zero policy actions or statements before or after the attacks that suggest that the United States had anything to do with the Nord Stream sabotage.

- Concerns about the Russian Federation potentially using energy infrastructure deployments to mask the installation of intelligence or military equipment in the Baltic Sea has been a concern for decades.

Incident Brief

While deeper detail is provided throughout the case study, a top line summary of just some of the central findings of our research that led us to these key assessments are:

Infrastructure Name:

Nord Stream 1 and Nord Stream 2

Infrastructure Type:

Dual Subsea Natural Gas Pipelines (comprised of concrete-weight-coated steel pipe segments of over 1 meter in diameter)[97]

Capacity:

Four Trunklines of combined 110 billion cubic meters per year (bcma) nameplate capacity (27.5 bcma per trunkline)

Geographic Details:

Nord Stream 1 - Vyborg, Russian Federation to Lubmin, Germany.

Nord Stream 2 – Ust-Luga, Russian Federation to Lubmin, Germany.

Length:

Nord Stream 1 – 1224 kilometers[98]
Nord Stream 2 – 1230 kilometers[99]

Ownership:

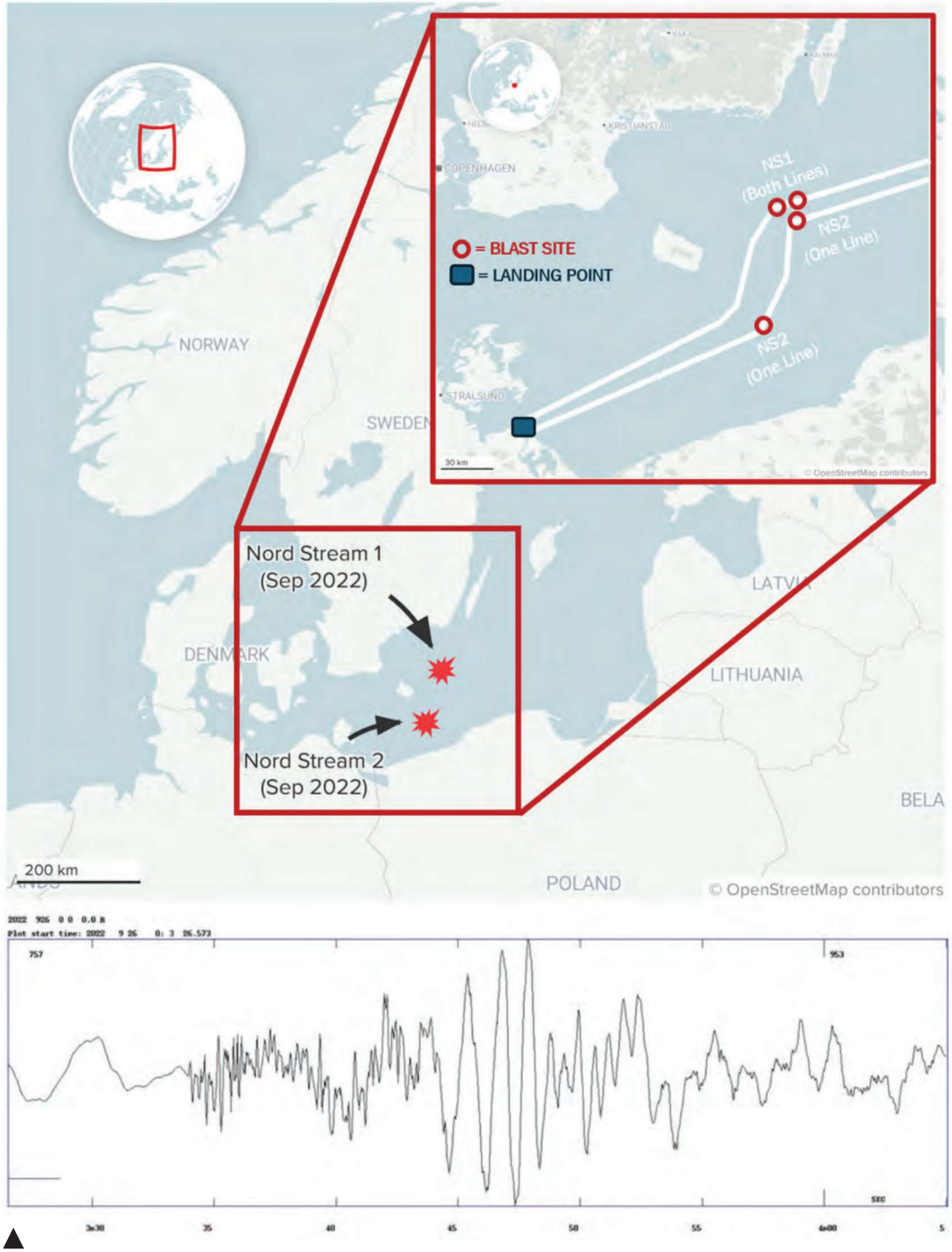
Nord Stream 1 – Nord Stream AG, a Zug, Switzerland based project operator owned by Russia's (Kremlin-controlled) Gazprom, Germany's Wintershall DEA and E.ON, The Netherlands Gasunie, and France's Engie.[100]

Nord Stream 2 – Nord Stream 2 AG, a Zug, Switzerland-based project operator, fully owned by Russia's (Kremlin-controlled) Gazprom.[101]

Operational Status at Time of Incident:

Nord Stream 1 – Between mid-June and the beginning of September 2022, Gazprom had steadily cut gas flows via Nord Stream 1, citing dubious technical issues, first by 40% in mid-June 2022, then by 80% in late-July 2022, and finally by 100% beginning in early September 2022. As such there were no commercial gas payloads being transited via the pipelines at the time of blast, however residual pressurized gas volumes would have been present in both trunklines.[102,103,104]

Nord Stream 2 – While the Nord Stream 2 pipeline construction had been completed in late 2021, the pipeline was sanctioned by the United States and had its certification removed by Germany in late-February 2022 just hours before Russia's full-scale invasion of Ukraine. As such, the Nord Stream 2 project never came into operation, and the project company had been facing insolvency by the time of the incident. While there were no commercial payloads flowing via the pipeline at the time of the blast, test gas had



[FIGURE 10] An illustration of the Nord Stream 1 and Nord Stream 2 blast sites along with seismic data from The National Geological Surveys for Denmark and Greenland (GEUS) from the first blast on Nord Stream 2 southeast of Bornholm at 02:03 hours Danish local time on September 26, 2022.

FIGURE DESIGN: B. L. Schmitt as based on published map data from Deutsche Welle on April 25, 2025, map created in Datawrapper[109,185,186]

already been flowed into the pipeline and residual pressurized gas volumes would have been present in both trunklines.[105,106,107]

<u>Incident Timeline</u>:

The explosions that damaged both of the Nord Stream 1 and one of the two Nord Stream 2 trunklines took place within the span of 18 hours on September 26, 2022, Danish local time. The first public indication of the incidents were statements made by both pipeline operators over that time frame who indicated a precipitous drop in the measured internal pipeline pressure. For example Reuters reported that Nord Stream 2's pipeline operator issued a statement on September 26, 2022 that "pressure in the pipeline, which had contained some gas sealed inside despite never becoming operational, dropped from 105 to 7 bar overnight."

By September 27, 2022, The National Geological Surveys for Denmark and Greenland (GEUS), had issued preliminary seismic analysis that had pinpointed the times of both explosion events, the first taking place at 02:03 Danish local time with a magnitude of 2.3 on the Richter scale, and the second taking place roughly 17 hours later at 19:03 Danish local time with a magnitude of 2.1 on the Richter scale. The first blast site was centered over the Nord Stream 2 trunklines southeast of the Danish island of Bornholm just outside the edge of the Danish territorial sea, while the second blast took place northeast of Bornholm generally located over the course of both Nord Stream projects in the Swedish exclusive economic zone. Further seismic analysis was reported by The Guardian in September 2023 from the Norwegian national data center for the comprehensive nuclear test ban treaty (CTBT) – Norsar – refined earlier analysis to pinpoint four distinctive seismic events, corresponding to what would be found to be four damage locations: one in a single Nord Stream 2 trunkline southeast of Bornholm, one in the same Nord Stream 2 trunkline northeast of Bornholm, and one each in both Nord Stream 1 trunklines northeast of Bornholm.[108,109,110]

It should also be noted that Danish seismic survey data analysis was at the time reviewed by GEUS with a daily cutoff of 02:00 hrs Danish local time. It is therefore notable that the first blast took place at 02:03 hrs local time – just three minutes after the daily data analysis cutoff – possibly suggesting that a premeditated actor may have timed this to maximize the time between the first blast and the corresponding daily data analysis schedule by GEUS. Danish media reported that following this incident, the GEUS analytical schedule was altered in response to a 24/7 operation. An illustration of the Nord Stream 1 and Nord Stream 2 blast sites along with seismic data of the incident provided by GEUS is illustrated in **[FIGURE 10]**.[111]

First images of the Nord Stream 2 outgassing site were released the Danish military on September 27, 2022, as taken by a Danish F-16 interceptor fighter jet that was scrambled from Bornholm, and the Danish military commented that the same F-16 interceptor response unit had at that point identified two leak sites associated with Nord Stream 1 northeast of Bornholm. Outgassing from all four leak sites continued for days after the attacks, before eventually ceasing in early October 2022, with Danish officials reporting that Nord Stream 2 had stopped outgassing as of October 1, 2022 and Nord Stream 1 as of October 2, 2022. While response vessels from Sweden and Denmark had already been dispatched to the scenes to keep vessels away from the outgassing sites (establishing isolated danger buoy AIS beacons, in addition to physical patrols), shortly after the outgassing had ceased, formal investigations began to be launched: first by Sweden on October 2, 2022, then by Denmark on October 6, 2022, and finally by Germany on October 13, 2022. NOTE: A good timeline summary of these events and continued news and official statement updates has been assembled by BNE Intellinews (details in endnote 114).[112,113,114]

Suspected Sabotage Mechanism:

According to media reports, German investigators found traces of the "military-grade" explosive HMX Octogen at the pipeline site. Furthermore, German investigators searching the rental sailboat <ANDROMEDA> in northeastern Germany found the same explosive material "on a table inside the boat's cabin."[115,116,117]

Suspected Perpetrators:

As of the writing and publication of this report, no official attribution has been made by European authorities as to the perpetrator of the Nord Stream 1 and Nord Stream 2 sabotage incidents. However, three main narratives have emerged to explain the

▲ *Concrete weightcoating detail of public display of Nord Stream 2 pipeline pipe segment in Hanko, Finland. (April 2025) / CREDIT: B. L. Schmitt*

incidents over the past 32 months, including:

- A largely debunked account by the Pulitzer Prize winning journalist Seymour Hersh published on Substack on 08 February 2023 claiming that the United States, with the help of Norway, had "executed a covert sea operation" to destroy the Nord Stream pipelines.[118,184]

- A narrative that has been the focus of German and other Western media claiming that a group of Ukrainian nationals used the aforementioned rental sailboat <ANDROMEDA> to conduct a covert diving operation over the course of September 2022 to place explosive devices on the Nord Stream pipelines, resulting in their destruction, based mostly on anonymously-sourced accounts from German investigators and allegedly-involved individuals in Ukraine.[119,120]

- A narrative that the Russian Federation itself had possibly destroyed the pipelines using a set of subsea warfare capable military vessels, who were confirmed via satellite data (and in some cases, images from the Danish military) to have been operating at what would eventually become the Nord Stream blast sites both in June 2022 and just days before the blast took place in late-September 2022.[121,122,123]

Primary Accounts of Incident

As with Svalbard cable cut case study, one of the areas of academic focus for this report series has been to better understand and, when possible, publish firsthand accounts from law enforcement, coast guard, national security officials, and military officers that often serve as the first responders to these European offshore energy and critical infrastructure sabotage incidents, as well as civilians that had firsthand experience being impacted in some way at or near the incident sites contemporaneous to the events and in the aftermath.

This section provides full on-the-record statements in boxes, that follow, from five such individuals related to the Nord Stream sabotage incidents:

- ***Martin Preisz Gravesen**, Police Commissioner of Bornholms Politi, with legal jurisdiction over the Danish island of Bornholm, and who was serving in this capacity during the September 2022 Nord Stream sabotage incidents.*

- ***Alexander von Buxhoeveden**, Head of the Environmental Assessment Unit at the Blekinge County Administrative Board in Karlskrona, Sweden, and who coordinated the Swedish Coast Guard's response to the Nord Stream sabotage incidents in September and October of 2022 out of Karlskrona, Sweden.*

- ***Mattias Lindholm**, Spokesperson for the Swedish Coast Guard, based in the Port of Karlskrona, Sweden.*

- ***Dr. Jakub Seerup**, naval historian, curator of Bornholm's Museum, and longtime resident of the island of Bornholm.*

- ***Kim Finne**, owner of Eastside Marine Company in the Port of Nexø, Bornholm, who also was hired to captain the offshore research expedition to obtain preliminary sonar data from the Nord Stream 2 blast site southeast of Bornholm discussed later in the report.*

BOX 04

Martin Preisz Gravesen, Police Commissioner of Bornholms Politi, with legal jurisdiction over the Danish island of Bornholm, and who was serving in this capacity during the September 2022 Nord Stream sabotage incidents.

"As soon as we learned of the explosions having taken place near Bornholm, it was clear from the very beginning that something very extraordinary had taken place. We reported on the incident from the Bornholm police headquarters to authorities in Copenhagen immediately, and then called in all relevant personnel to coordinate a rapid response.

The first step was to assess what the danger to lives and property might be, which needed to take place even before the beginning of the investigation for cause. Copenhagen dispatched a team from the Danish National Emergency Management Agency with personnel and equipment to detect air quality and if the gas cloud posed any acute danger to the local population centers on Bornholm due to the wind direction. Thankfully, the wind was friendly at the time, and the gas cloud didn't get pushed from over the blast site to the shorelines of Bornholm. As a result, the team assessed that there was no immediate danger to the citizens on Bornholm, and a rapid civilian evacuation did not need to be ordered on the island.

By the next morning, the Bornholm police force was reinforced by the Copenhagen police, and at that point, the lead response authority was transferred to that agency, since they have the investigative authority over the Danish offshore. From that point on in the investigation, the Bornholm police were only used in a backup capacity and were no longer directly looped into the larger national investigation that proceeded the weeks and months that followed."

BOX 05

Alexander von Buxhoeveden, Head of the Environmental Assessment Unit at the Blekinge County Administrative Board in Karlskrona, Sweden. Mr. von Buxhoeveden was previously with the Swedish Coast Guard and coordinated the Coast Guard's response to the Nord Stream sabotage incidents in September and October of 2022 out of Karlskrona, Sweden

According to Buxhoeveden, "jurisdictionally, the Swedish Coast Guard generally deals with major crises along the Swedish shoreline and within its territorial waters related to safety and environmental crises. Given the environmental nature of the Nord Stream leaks, it was deemed necessary to have Coast Guard asset help with the investigation and with protecting the safety of mariners nearby. Given that Coast Guard support in the Swedish exclusive economic zone is sometimes considered a legal grey zone, state prosecutors were brought on board to assist in real time legal assessments of the aid being provided."

Regarding the Swedish response to specific Russian vessels in the area after the incident, von

Buxhoeveden commented on research completed for this report with AIS data showing <SWEDISH WARSHIP M75 VINGA> and related vessels respond to the Russian nuclear class icebreaker <SEVMORPUT> leaving the main shipping lane and moving toward the Nord Stream 1 blast site, by saying: "These vessels responded to <SEVMORPUT> and other Russian ships that left the traffic pattern near Bornholm and began to approach the blast site danger areas. Both suspicions regarding the capability and activity of these vessels likely contributed to the responses by Swedish naval and coast guard assets seen on public AIS to ensure these Russian vessels did not enter the danger area around the investigation site."

Regarding the response to the Nord Stream 1 incident in Swedish waters, von Buxhoeveden explained that:

- *Two of the blast sites were located in the Swedish EEZ.*

- *The first notification that the [Swedish] Coast Guard [received] to respond were eyewitness reports from civilian vessels in the area that saw the outgassing area, and a Swedish Coast Guard Air Patrol plane was dispatched to the scene.*

- *The Swedish <KBV 003 AMFRITIE> was dispatched to keep other vessels away from the blast site, both during the pipeline active outgas phase and afterward during the investigation. The <KBV 003 AMFRITIE> remained on the scene until the outgassing from the pipeline stopped, and then traded off with <KBV 002 TRITON> for monitoring of the investigation site. It ultimately took some time between the incident and when Nord Stream management was in touch with Swedish authorities.*

- *The Swedish naval submarine rescue ship <A214 BELOS> was dispatched to the site to investigate the blast site using a combination of divers and subsea sonar and imaging equipment.*

-The Swedish investigation utilized a wide array of Swedish air and maritime assets, including:
Swedish Coast Guard Vessels: <KBV 003 AMFIRITE> and <KBV 002 TRITON>
Swedish Coast Guard Air Patrol: <KBV 502>
Swedish Navy Vessels: <SWEDISH WARSHIP M75 VINGA>; <SWEDISH WARSHIP M14 STURKÖ> <SWEDISH WARSHIP A214 BELOS>

BOX 06

Mattias Lindholm, spokesperson for the Swedish Coast Guard, based in the port of Karlskrona, Sweden

"We had gotten information already in the morning from a merchant vessel that a large outgassing site had formed in the Danish exclusive economic zone, but Swedish authorities didn't respond as there was not an immediate request from Danish authorities. However, hours later, there was a report of a similar incident taking place in the Swedish exclusive economic zone, so the Swedish Coast Guard immediately deployed a vessel. And if the incident also involved an ongoing emission of gas it is the Coast Guard's jurisdiction given that it is an environmental issue.

Swedish Coast Guard responders thought immediately the incident might have involved Nord Stream since they could see a huge bubbling cloud that had formed. The sea was boiling! By radio, the Swedish Coast Guard established danger zones to ensure that other ships would be kept out of the outgassing area, especially larger ships operating on autopilot.

Given that Russia was a country of interest related to Nord Stream, the response rapidly went from an environmental issue to a geopolitical and security issue, since it would now have to do with defense as well. The Swedish Coast Guard supported an interagency response team that included a wide number of Swedish agencies, including police and naval assets. From the Coast Guard perspective, the response was considered an operational success as it was able to provide a platform for personnel including police investigators and prosecutors who would otherwise have no fleet to work offshore. For example, the Swedish Coast Guard vessel <KBV 003 AMFIRITE> had the capacity to house a large number of interagency responders to the Nord Stream blasts.

[After the danger zones were established, for safety reasons], Swedish response vessels would radio any vessel that had a course moving in the direction of the danger zone to not approach. In this case, the other motivation can be to show an adversary that responders know what they are doing and have particular capabilities, so moving up to a potentially adversarial ship, such as the Swedish Navy approaching the <SEVMORPUT>, could do that.

There is still no clear jurisdictional authority for any Swedish agency to lead offshore critical infrastructure protection. For example, a gas leak is an environmental issue, so the Coast Guard is involved, but the question remains what the role of the Coast Guard would be if, for example, a telecommunications cable was cut, as there would be no clear environmental nexus. Protection of critical infrastructure remains an issue of the companies, but this needs to be addressed as there are clear state interests.

Although it was first declared in 2015, Russia's 2022 invasion of Ukraine has sped up the Swedish Total Defense Strategy. We need to continue to move fast on total defense as there is now an active war in Europe."

BOX 07

Dr Jakob Seerup, naval historian and curator of Bornholm's Museum and longtime resident of the island of Bornholm, Denmark

"The reports about the subsea explosions and disruption of the Nord Stream pipeline and the subsequent footage of the bubbling blast sites just off the coast of Bornholm were a wakeup-call. It really brought it home to me and most other people here on our island in the Baltic, how there really is a war going on geographically very close to us. It felt like the war now was coming almost too close for comfort. This reminded many Bornholmers of how vulnerable we are to disruptions of critical infrastructure. The power cable from Sweden to Bornholm had been cut just two days after Russia's full-scale invasion of Ukraine on February 24 2022. That had been a scary event in the light of the drama of those days, even if it was later found out not to have been an act of sabotage but rather a badly timed accident. These few months later, there could be no doubt, that this time around the Nord Stream sabotage was no accident but a part of the war."

BOX 08

Kim Finne, Owner of Eastside Marine Company in the Port of Nexø, Bornholm. Captain of Research Expedition for this stuy to Nord Stream 2 blast site in September 2024.

In the days following the Nord Stream 2 sabotage, Kim Finne was hired by SkyNews to help bring a film crew to the Nord Stream 2 blast southeast of Bornholm, while the pipeline was still aggressively outgassing.

"I would say the first thing, the day that it happened, the wind direction was correct, it was blowing from the blast into Bornholm, so we could smell it for the first day. After that the wind direction was changing, but it was only for a small window where we could smell it.

At that time, I was out with SkyNews a couple of days after that, and we were around only 5 nautical miles from the place, when we got a call from a navy ship lying really close, saying that we are now in a restricted area, you need to turn around. And if you don't do it, we will come after you...[was it a Danish navy ship?]...it was, a really big one. At that time, and five nautical miles [away], you could not see anything, [and] at that time the wind had changed and most of it was getting smaller and smaller, what was coming up from the bottom, so at that time, you could not smell [the gas] anymore."

Policy Context of Nord Stream Sabotage Incidents

When we consider any of the suspected sabotage incidents in this research series, it is vital that we consider the context in which they took place. As Finnish investigative journalist Pekka Virkki reminded us, "we have to remember - all of these sabotage incidents have taken place not in a vacuum, but in a much broader context of political, military, and economic events that are impacting the region."

Over the years, much of the policy discussion surrounding the Kremlin-backed Nord Stream pipelines has centered on raising awareness of the significant energy, economic, environmental, and strategic corruption concerns associated with the project (such as the areas of policy focus by Transatlantic leaders highlighted earlier this volume), while debunking what in effect had become mantras of Gazprom and its ideological allies. Variations on "it's just a commercial deal," and "even in the coldest days of the Cold War, Russia has always been a reliable energy supplier," to name but two, were aphorisms that consistently needed factual debunking.

And while the gravest geopolitical consequences for the projects – especially Nord Stream 2 – were rightfully focused on the impacts those pipelines would have on harming Ukraine's economic and strategic stability ahead of Russia's criminal invasion of the country in February 2022, another set of concerns have always been lurking just below the surface – of the Baltic Sea.

Indeed, the project development process of the gas pipelines – starting with Nord Stream 1 two decades ago – have long raised physical, environmental, and military security concerns across Baltic Sea littoral states. Dare to raise this last class of objections to the Nord Stream pipelines in panel discussions and debates in Brussels, Berlin, or Washington? Project supporters

often had a uniform response. “Security!?” or “Military?!,” they would howl, layering on a healthy dose of affected befuddlement for good measure.

Flash forward to late 2022. Climate-destructive methane plumes escaping from damage sites above Nord Stream 1 and 2 turned areas of the Baltic Sea into a churning maw for weeks. Preliminary forensic investigations had uniformly pointed to “detonations” that suggested “gross sabotage” – in the words of the Swedish security services investigating the Nord Stream 1 and 2 leak sites in its Exclusive Economic Zone (EEZ) days after the blasts.[124]

As Mr. Virkki pointed out, these events did not take place inside of a vacuum and therefore we must consider the economic, legal, information environment, as well as security context in which the blasts took place. This section attempts to provide analysis and expert commentary regarding these contextual categories, and highlights four main arguments:

- **Despite the recent prevalence of the rhetorical question “why would Russia destroy its own pipeline?” in fact it can be reasonably argued that the Russian Federation did have possible motivation to sabotage Nord Stream 1 and 2, including economic, security, and legal rationale;**

- **The Russian Federation had launched a disinformation campaign in the hours after the Nord Stream blasts took place, and continued to place blame in a variety of directions simultaneously in the months after the incident;**

- **The Biden Administration had displayed zero policy actions or statements before or after the attacks that suggest that the United States had anything to do with the Nord Stream sabotage;**

- **Concerns about the Russian Federation potentially using energy infrastructure deployments to mask the installation of intelligence or military equipment in the Baltic Sea region has been a concern for decades, and past examples of potential Russian operations destroying its own energy infrastructure exist.**

Economic and Legal Context

The economic and legal context of the Nord Stream pipeline sabotage on the European gas market throws significant light on the incentives for possible Russian self-sabotage. That context also helps one appreciate how economic incentives particularly in Germany may yet see the Nord Stream pipelines being restored to full operation (at least Nord Stream 1).

In the years immediately before the outbreak of the full-scale invasion of Ukraine, the European Union and in particularly Germany significantly increased its dependence on Russian gas. Ever since the understanding between the U.S. and Europe in the early 1980s during the Reagan Administration, Soviet and then Russian gas imports never much exceeded 30% of European imports. However, due to a few factors, despite the Russian invasion of Eastern Ukraine and illegal-annexation of Crimea in 2014, Europe significantly increased its Russian gas dependence.

These factors included the progressive closing down of the Groningen gas field in the Netherlands, which as late as 2013 was producing 50 billion cubic meters of gas per year (bcma); the closing of coal (across Europe) and nuclear plants (in Germany) and the growth of renewables which required flexible back-up which almost always meant on standby combined cycle gas turbines. These three factors pushed Europe in

direction of the sourcing of more gas from Russia so that by the eve of the full-scale invasion of Ukraine in February 2022 the European Union natural gas were roughly 45% sourced from Russia, and for Germany that figure reached roughly 55%.

Even before the February 2022 full-scale invasion of Ukraine the European gas market had become a market absorbing very high prices. By the end of December 2021 prices had crossed the €90 per megawatt hour (p/mwh) level and would in fact reach in August 2022 €342 p/mwh. By contrast the highest price in the century so far for European gas was at the height of the 2008 commodity price boom when prices reach €40 p/mwh. In the period 2009-2019 prices had ranged €9-€29 p/mwh.[125]

So what was going on? It is true that post COVID demand had temporarily increased demand, and there was a demand for additional liquefied natural gas (LNG) from China. However, none of these demand factors could generate such pricing levels. What is clear that from the spring of 2021 Gazprom did not comply with its usual commercial practice, in that as winter ended and European gas demand fell away it would dispatch gas across the trans-continental European pipeline network east to west to fill up storages across the EU for the following winter – including those that were owned by Gazprom itself. In late spring and early Summer of 2021 it became clear that Gazprom was not exporting natural gas at the usual volumes into continental European storage.[126]

Furthermore, when prices accelerated in the European market Gazprom, as the dominant supplier with immense additional production and domestic storage capacity, did not respond commercially by exporting more gas into the European spot markets. Worse still as the winter heating season 2021-2022 got underway Gazprom began emptying its gas storages it owned in the EU to supply its existing long term supply contract customers, further undermining European supply security.

From the spring of 2021 onward prices on the Dutch Title Transfer Facility (TTF), the main European gas hub, began to accelerate. By the beginning of September 2021 prices had reached €97 p/mwh. Given Gazprom's behavior in refusing to resupply storage in the spring and depleting gas from its own storages to sustain long term supply customers in the fall, while refusing to supply additional gas into the spot market as gas prices accelerated this price acceleration was not surprising. The question why Gazprom was taking these unprecedented (at least for Western Europe) measures was unclear. Some commentators initially thought it was Moscow seeking to bring pressure on the EU and its Member States to waive Nord Stream 2 through EU regulatory procedures, and partly that was indeed the case.[126,127]

We had our answer as to the reason for Gazprom and the Russian state to abandon its role as the base supplier of natural gas to Western Europe in February 2022- with the onset of the full-scale invasion of Ukraine. Moscow was seeking to soften up Europe to deter it from supporting Ukraine, while temporarily ramping up Gazprom's revenues as the full-scale invasion got under way (possibly in the fashion of a "shaping operation" by Russia that Lt. Gen. Hodges described in the previous case study).

Once it became clear in the spring of 2022 that the full-scale war was not going to end in a couple of weeks, Moscow sought to bring more pressure to bear on the European economy by depriving it of access to Russian gas. It sought to do this in a manner which would minimize Gazprom's liability for terminating its long-term supply contracts with its customers. The Kremlin adopted a Presidential Decree under which Gazprom's customers were required to pay for gas in rubles at an account held at Gazprombank. However, this was set up under the Decree

▲
View from the southern coastline of Bornholm looking toward the location where the September 2022 Nord Stream 2 sabotage incident took place southeast of Bornholm in the Baltic Sea. (August 2023) / CREDIT: B. L. Schmitt

so that at least five different Russian authorities were required to accede in formally clearing payment. Clearly customers could argue that their contracts specified they should pay in US dollars not rubles.

Gazprom then sought further to tighten the screw with a series of moves claiming first that the Siemens turbines to run Nord Stream 1 needed to be repaired were in the hands of the Canadians and subject to sanctions. This Gazprom argued resulted in reduced gas flow across the Nord Stream 1 pipelines. This was despite the fact that Gazprom had sufficient spare Siemens turbines available, especially with Nord Stream 2 under sanctions. Additionally, over the summer of 2022 Gazprom also reduced gas flows by claiming a series of maintenance and repair operations were needed on the pipelines. On 31 August 2022, Gazprom fully cut off the route so that no natural gas was actually flowing through either of the Nord Stream 1 pipelines.[128,129]

During this entire saga over Summer 2022, Russian officials, led by Russian President Vladimir Putin made statements attempting to use the energy weaponization represented by these gas cutoffs as leverage to get sanctions on Nord Stream 2 lifted. On July 20, 2022, speaking in Tehran, Putin stated that, "we have another route ready – it's Nord Stream 2 which can be launched." By the time the pipelines were fully cut off, the refrain was the same, with Kremlin spokesperson Peskov blaming sanctions "introduced against our country by western countries including Germany and the UK" – rather than technical issues with the turbines it had previously claimed – as the reason for the cutoff, doubling down by stating that "other reasons that would cause problems with the pumping don't exist."[130,131]

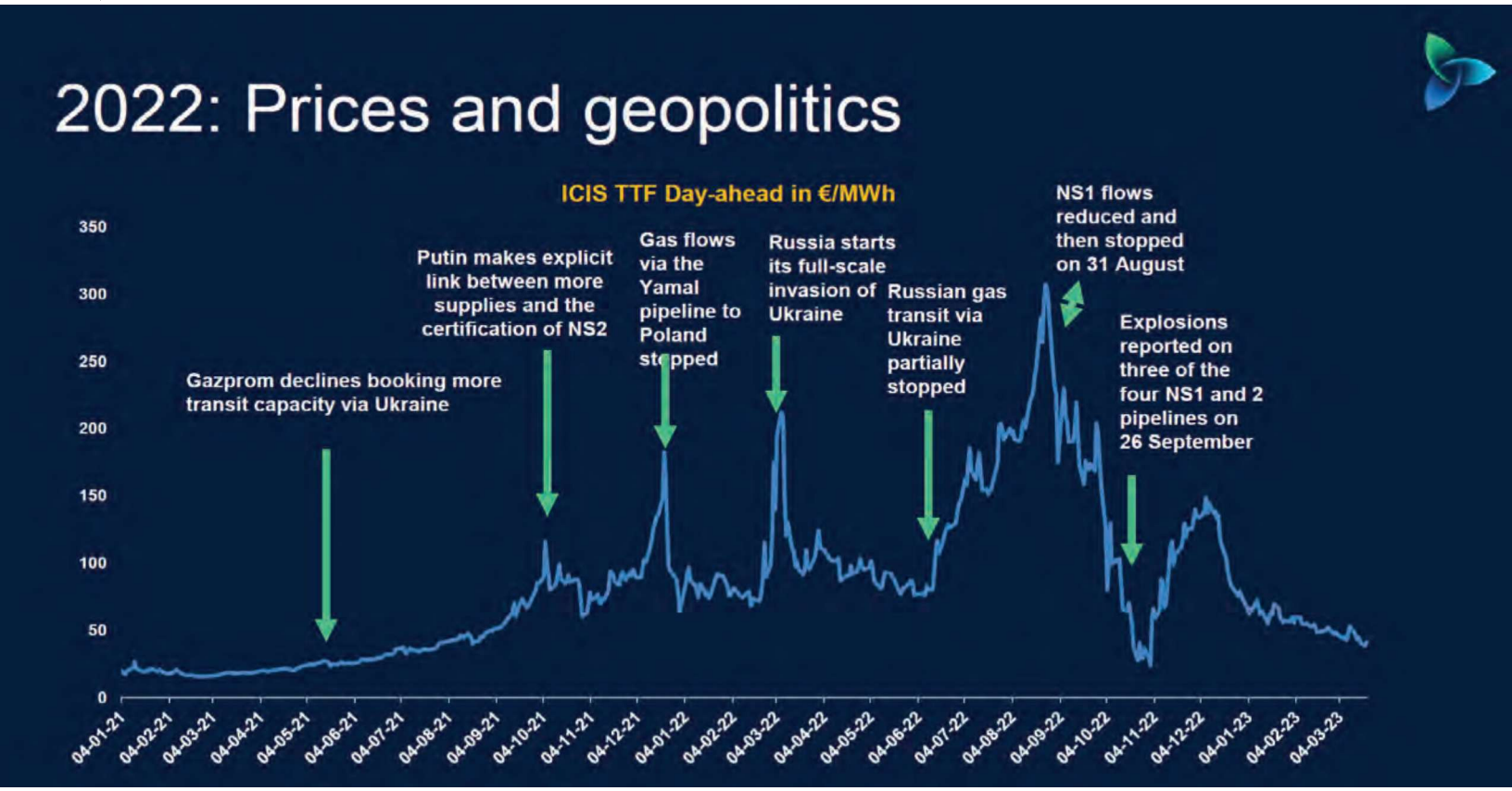
During the turbine saga, the Biden Administration took steps to back German government calls for Canada to waive sanctions on the Siemens turbines undergoing maintenance in Canada. This came even though some senior German officials publicly stated that the Russian technical claims were unfounded and were in fact based on political motives, and Germany's energy network agency – the Bundesnetzagentur - pointed out that it

"could not identify any causal connection between the missing gas compressor on the Russian side and the big reduction in supplies." Ultimately, Canada acceded to German and U.S. pressure and issued a sanctions waiver that allowed the return of a sanctioned Siemens turbine to Germany – where it was offered to be transferred to Gazprom – an offer that was never taken up by the Russian side.[132,133,134,135]

In other words, the Biden Administration pursued a policy course that in fact would weaken technology export controls on the Russian Federation, and, presumably, result in the extension of Nord Stream 1 operations even while it had simultaneously had Nord Stream 2 under sanctions at that point. Moreover, it is useful to recall that the Biden Administration had also during the height of the aforementioned 2021 undersupply by Gazprom of European storages, come to an agreement with Germany to waive Congressionally mandated sanctions on the Nord Stream 2 project, releasing a joint statement on July 21, 2021 with Germany in which Berlin agreed to "take action at the national level and press for effective measures at the European level, including sanctions, to limit Russian export capabilities to Europe in the energy sector, including gas, and/or in other economically relevant sectors" should "Russia attempt to use energy as a weapon or commit further aggressive acts against Ukraine."[136]

Despite this agreement – and with Russia actively weaponizing energy in Summer 2021, and continually until it's full-scale invasion of Ukraine in February 2022, it was not until just hours before that invasion that the Biden Administration revoked its waiver and allowed full sanctions to be applied to Nord Stream 2. Likewise, the German government never took any of its vowed actions at any level "including sanctions, to limit Russian export capabilities to Europe in the energy sector." Historians will assess what the biggest motivation was for these actions of the Biden Administration to

[FIGURE 11] Contextual overlay of TTF Day-ahead natural gas price and geopolitical events involving corresponding actions by the Russian Federation and Gazprom in the months ahead of the Nord Stream sabotage incidents. */ CREDIT: A. Sabadus, ICIS*



preserve first Nord Stream 2 (through the waiver of Congressionally-mandated sanctions), and then Nord Stream 1 operations (by supporting Germany's pressure on Canada to waive technology export controls on aforementioned Siemens turbines) - possibly out of a focus the Administration consistently took to focus on specifically strengthening U.S.-German relations after years of strife during the first Trump Administration. However, the notion - as suggested in the Hersh account – that the Biden Administration suddenly took action to order a clandestine kinetic strike against the Nord Stream pipelines in late September 2022 – while the Biden Administration's national security team simultaneously fretted over "escalation" vis-à-vis Russia in Ukraine – is highly illogical in this context.[137]

Moreover, the overall economic consequence of Gazprom's continual summer 2022 squeeze of gas flow through Nord Stream 1 was to push natural gas prices ever higher reaching €342 p/mwh in August 2022. Ultimately, these same prices, as shown in **[FIGURE 11]**, which shows the correspondence of the European TTF gas price along with key events in Russia's energy weaponization push between 2021 and 2022, would then rapidly tumble during September before the actual explosions on 26 September 2022.

This context strengthens the case that the explosions on the Nord Stream pipelines were self-sabotage. The Russian Presidential Decree only provided a relatively legally flimsy defense to failure to provide natural gas under existing long term supply contracts. By September 2022 almost all Russian natural gas flows save via the Ukrainian transit and Turk Stream 2 had stopped and Gazprom was in breach of its contracts with dozens of its long-term customers. At this point Gazprom needed a stronger argument to shield itself from damages claims for non-delivery. The explosions on the pipelines provided a much stronger force majeure argument which would at least stem the damages claims to the period before 26 September 2022, capping the damages claims against Gazprom to that date. At the same time, the scale of the damage was not so great that repairs would ultimately be possible on the pipelines making it feasible to bring them back into operation and revive many of the long-term contracts.

Gazprom has already faced the termination of its long-term supply contract with Uniper and the award of €13 billion in compensation for its failure to supply in 2022 for breach of contract and consequential damage. It is understood multiple additional energy customers are bringing claims against Gazprom along these lines. These claims are all brought under their long-term supply contracts, the majority of which are based on Swedish law as the law of the contract and the arbitration forum are either the Swedish Court of Arbitration or the International Chamber of Commerce. These claims appear (the awards when made do not usually result in publication of the ruling) to be currently based on damages and consequential loss for Gazprom's nondelivery before the 26 September explosions. Should the Russian state be responsible for the explosions, the scale of potential damage claims against Gazprom would be significantly expanded.

Such an economic motivation for Gazprom was highlighted by Aura Sabadus, a European gas market expert and Senior Fellow at the Center for European Policy Analysis, who explained that, "while it is, indeed, difficult to accept that Russia may have sabotaged its own infrastructure, in hindsight, we know that the country had been engaging in a hybrid war against Europe since spring 2021, even as it was preparing to mount its full scale invasion of Ukraine in February 2022. Throughout most of 2021 and then after the start of war, Russia cut gas exports, which pushed up gas prices across European markets, creating panic and market volatility. By the summer of 2022 it had unilaterally cut around 80%

of its total exports to Europe, a fact that resulted in multiple arbitration cases initiated by European buyers. Russia knew that by unilaterally cutting supplies, it would be liable to pay penalties for non-delivery which would result in awards of around $40 billion, according to calculations by UK-based consultants Wood Mackenzie. The cost of arbitration would be around 80 times greater than the estimated $500 million repair bill for the ruptured pipelines."

Furthermore, after weaponizing energy through undersupply and then major gas cutoffs against the European Union for nearly 18 months straight leading up to September 2022, the Russian Federation may have been motivated to further increase pressure on Europe to relent in its support for Ukraine's defense. At the time, the Russian military had not yet embarked on its most serious campaign of energy and critical infrastructure strikes within Ukraine, and to the extent that it had, it had so far spared the Ukrainian gas transmission system, which – following the Nord Stream sabotage – became one of the only major gas transit routes still operating to Europe. With the first European winter beginning just weeks after the Nord Stream sabotage, the motivation of Russia to increase the stakes on European policymakers to relent in weapons deliveries to Ukraine may have been front of mind for the Kremlin, since, in the absence of functional Nord Stream pipelines, they could easily further escalate by destroying the Ukrainian gas transmission system in an overt military strike within the Ukrainian theatre.

These points were reinforced by Arild Moe, a research professor focused on the Russian energy sector and geopolitical issues in the high north at the Fridtjof Nansen Institute in Lysaker, Norway. For a potential Russian motivation to damage the Nord Stream projects at that time, however, Professor Moe argued that the Kremlin "could have been motivated by wanting to put the EU on notice that it could damage energy and critical infrastructure, especially if Russia was - as it now seems - in the process of at least temporarily "abandoning" the EU as a market." Moreover, Moe pointed out that by late 2022, Gazprom might have viewed damaging the Nord Stream trunklines "would provide a force majeure situation to shield it from inevitable lawsuits owing to its non-delivery of gas throughout the year." After all, Moe dryly quipped, "the Russians had already killed the Golden Goose, so why not shoot it in the neck as well?"

From the Ukrainian point of view, launching an attack against Nord Stream at that particular time in the war would also have questionable utility. Especially with Nord Stream 1 having already been fully cut off by Gazprom for pseudo "technical reasons" at the start of September 2022, and with Nord Stream 2 fully sanctioned and not operating, Professor Moe questioned why it would have been in the Ukrainian state interest to attack the pipelines at that time, even if they could be considered legitimate targets of war. "You have to remember that at the time Nord Stream was sabotaged, there was already a huge level of concern among European leaders that Russian gas and electricity cuts throughout 2022 were jeopardizing Europe's energy security ahead of winter. For the Ukrainian government to willingly jeopardize European - and in particular, German - support for the war with such an act is simply not rational," Moe explained.

Indeed, by Fall 2022, the Ukrainian cause was being significantly bolstered by the delivery of western weaponry, and Kyiv in particular viewed Germany agreeing to deliver Leopard tanks as near existential to the defense of Ukrainian sovereignty. Taking any action to endanger those weapons delivery decisions by sabotaging what by late September 2022 were inactive and sanctioned pipelines, was raised by multiple experts interviewed in this study.

For example, Niklas Granholm, deputy director of studies in the Division for Defence

View from the eastern coastline of Bornholm looking toward the location where the September 2022 Nord Stream 1 and 2 sabotage incidents took place northeast of Bornholm in the Baltic Sea. (August 2023) / CREDIT: B. L. Schmitt

Analysis at the Swedish Defence Research Agency (FOI), argued that "the claims that a pro-Ukrainian sailboat was used to sabotage the Nord Stream pipelines borders on the absurd, especially as the claims are not simply that some rogue element was used to carry out the attack, but rather that it took place under the command of Zelensky and Zaluzhnyi. You have to remember, Ukraine was trying to get further support from the west at that time, and in particular Leopard tanks from Germany, which was an existential need for Ukraine at that time in the war. Russian motivation to continue to increase pain in Germany through energy cuts and then this explosion is clear as it could erode public support for Ukraine at that critical moment in the conflict." To this point, Granholm reminded us that "Sweden has been sitting next to Russia for 700 years, so we have picked up a thing or two about how Russia operates."

The illogical nature of Ukraine taking actions to jeopardize its own military equipment support from European partners including Germany was also a point raised by Jacob Kaarsbo, a Copenhagen-based independent security policy advisor and former Chief Analyst for the Danish Defence Intelligence Service. As Kaarsbo explained, "The Ukrainian intent to conduct the sabotage is also very dubious. There was no gas flowing in the pipeline and due to EU sanctions, there was no income for Russia in sight. Furthermore, Ukraine's drive to get tanks and more advanced weaponry started in earnest in the preceding months. It's highly unlikely that Ukraine would put arms deliveries from Europe (namely Germany) and the US (according to the latest German media reports, CIA had warned Zelensky against the alleged attack plans) in jeopardy. The [August 2024] allegation from Wall Street Journal that it was a rogue operation carried out by former Defence Chief Zaluzhnyi has so many loose ends and is also highly unlikely."[120]

As for possible Russian motivation, Kaarsbo also saw potential rationale, explaining that, "Regarding intent, Russia had already used the gas weapons to inflate prices and there was no gas flowing through the pipeline. The subsequent Russian insurance claim was way higher than the Russian "offer" to restore the pipeline. So besides likely seeking a deterring effect vis-à-vis Germany, Sweden

▲
Aerial view taken in September 2024 of Rønne harbor on the Danish island of Bornholm near the Nord Stream 1 and Nord Stream 2 sabotage incident sites that took place in September 2022. (September 2024) / CREDIT: B. L. Schmitt

and Denmark, Russia also had an economic incentive."

Jakub Godzimirski, Research Professor at the Norwegian Institute of International Affairs (NUPI) focused on the role of energy resources in Russian grand strategy summed up the question of motivation, arguing that "the question that continues to be rhetorically asked: "Why would Putin blow up Nord Stream?" is the same logically as asking "Why would Putin invade Ukraine?" Both hurt Russia and go against self-interest."

Information Environment

In terms of the information environment in the aftermath of the sabotage of Nord Stream 1 and Nord Stream 2, the Russian Federation also appeared to have a well-worn disinformation strategy at hand to sow doubt about the perpetrators and European investigations. Ivana Stradner, an adjunct lecturer of International Law and Cybersecurity at the Johns Hopkins University School of Advanced International Studies explained that "Russia's most effective weapon is information because it allows the Kremlin to accomplish its security objectives below the threshold of war using influence operations. Moscow has been weaponizing energy to blackmail Europe while using propaganda to shape perceptions and positioning Russia as a reliable gas supplier."

Stradner who also specializes in studying the dynamics of how the Russian Federation uses disinformation campaigns to undermine Western democratic resilience as a research fellow at the Foundation for the Defense of Democracies think tank in Washington, D.C., continued by explaining that mixing disinformation campaigns with energy is nothing new for Putin's Kremlin. "The Kremlin has also deployed disinformation regarding energy security to blame the West for gas prices in order to undermine Western support for Ukraine. Who has information superiority will win this "energy information warfare"..." she said.

Eero Kytömaa, Ministerial Advisor at the National Security Unit of the Finnish Ministry of the Interior noted that "a hallmark of Russian disinformation strategy connected to hybrid threat events like the Nord Stream and Balticconnector incidents is to rapidly spread multiple, often contradictory theories about the cause of the given event. Countering this Russian approach is vital, and that's why it is particularly important for European authorities to publicly reveal as many verified facts about a given incident, as quickly as possible."

Indeed, in the hours that followed the Nord Stream blasts, social media accounts on platforms like Twitter, many of which fit the characterization of typical Russian bot and troll behavior, were suddenly found to be retweeting a similar, out of context clip of an early-February 2022 joint press conference held at the White House between President Biden and German Chancellor Olaf Scholz, in which Biden is asked how he would stop Nord Stream 2 if Russia would invade Ukraine weeks later. The clip of Biden's response was circulated by these accounts, focusing on the lines from Biden, in which he stated, "if Russia invades, that means tanks or troops crossing the ... border of Ukraine again, then there will be ... no longer a Nord Stream 2. We, we will bring an end to it." A follow up question of how the project could be stopped resulted in Biden simply stating "I promise you, we'll be able to do it."[138,139]

Of course, the context in which the question was asked, when placed in contemporaneous context, was one in which Biden and Scholz had also vowed a united approach on Russia sanctions, and just weeks after a majority of U.S. Senators on a bipartisan basis voted in favor of imposing sanctions on Nord Stream 2. Clearly at the time of the press conference, the discussion was focused on sanctions actions to stop Nord Stream, rather than a kinetic strike, but this didn't stop disinformation from spreading, falsely amplifying Biden's comments as indicative that the United States had been behind the attack.[140]

The narratives favored by the Kremlin in the months that followed were themselves conflicting and various, in line with Kytömaa's analysis, in which the Kremlin went from initially claiming (without evidence) that the United Kingdom was behind the sabotage, to their current trend of settling on the United States as the culprit.

The coordinated release and rapid reaction of Russian disinformation trends related to the Nord Stream sabotage does little to suggest a lack of Russian involvement in the case, and conversely, could suggest that the information operations Russia likely launched were in tandem with the act of sabotage itself.

Security Context

In terms of security context, it is important to remember that Gazprom itself has a track record in this sort of scenario involving the damage of Russian energy infrastructure investments. In 2006 a series of explosions on the Russian side of the Russia-Georgia border took out part of the North Caucasus-South Caucasus main pipeline and in parallel explosions hit the high voltage power cables providing Georgia with electricity. In 2009, following the 2008 economic crash Gazprom suddenly found itself with surplus natural gas supplies, including surplus imports from Turkmenistan. Gazprom first reduced the gas flow from Turkmenistan and then in April 2009 there was an explosion on the Russian side of the border, which disrupted all supplies and which was not repaired. This led to Gazprom claiming force majeure with more gas flowing under the existing Turkmenistan gas contract. Godzimirski also pointed out that he had written papers on explosions that damaged gas pipelines in Central Asia, that he suspects Gazprom may have been behind, creating a force majeure scenario for the company. "So this sort of action is certainly in the Kremlin's

repertoire."[143,144]

Another such example of potentially similar Kremlin activity was highlighted by Piotr Krawczyk, former Chief of the Polish Foreign Intelligence Agency, who said, "Remember that in 1999, there were a series of apartment bombings in Russia that were almost certainly carried out by the Russian government itself. These acts have since been widely assessed to be effective false flag operations that helped then Prime Minister Putin gain in popularity and take the Russian Presidency months later, and also to justify the Russian military's subsequent brutal aggression against Chechnya. If it is indeed shown that Russia was in some way behind the Nord Stream sabotage, it would match such a playbook. In Fall 2022, the Russian government was having major issues with the mobilization of Russian society for its war against Ukraine, and the Nord Stream attack, and blaming it on the West, could have been calculated to be useful to amp up public support for the war across Russia."

Moreover, since the outset of the development of the Nord Stream 1 pipeline two decades ago, there have been consistent concerns about Russia using the deployment of the pipeline system for military or intelligence means. For example, a 2007 working paper by the CIVPRO Civil Protection Network in Sweden already raised such concerns about the deployment of Nord Stream 1, which at that time was still called the "North European Gas Pipeline." In the report, statements at the time from Putin in a TV interview quoted the Russian President as stating that the Russian Baltic Fleet's "role is to protect our economic interests in the Baltic Sea region [...] Protecting the Northern European Pipeline [which was later renamed Nord Stream 1], which brings energy resources to our Western European customers, is one of our most important priorities."[146]

These statements, in which Putin linked the energy project with Russia's naval capacity, was at the time happening in parallel with decisions made by Baltic Sea littoral states on the project, such as Sweden, who ultimately blocked the construction of a proposed offshore compressor station for the pipeline near the island of Gotland, citing intelligence and military concerns.[146]

Granholm underscored this point by explaining that Sweden was able to block a proposed Nord Stream 2 logistics port on Slite, while regional authorities in the municipality of Karlshamn succeeded in hosting a Nord Stream 2 logistics center despite national security concerns from Stockholm. As Granholm described, "as a result, Swedish authorities monitored the activities in Karlshamn to make sure that no "little green men" showed up in "orange Gazprom jumpsuits." Since then, Granholm explained that there was a move in Sweden for legislation to ensure that foreign investment screening on policy grounds can be decided at the national level instead of by individual municipalities, in which municipal leaders can often be influenced by enticing offers of [local] job creation and foreign direct investment.

And speaking on the attack on Nord Stream itself, Granholm added that "In terms of who would have the capability to carry out such an attack, well of course you can first look to all of the great powers, but for Russia they have GUGI, who reports directly to the General Staff in Moscow outside of the direct naval command, and is a unit that is specifically built to carry out these sort of subsea operations globally."

Tarmo Soomere was one of those Baltic Sea littoral state experts that was already concerned about the Nord Stream 1 pipeline. Soomere, who served as President of the Estonian Academy of Sciences from 2014 until 2024, and who continues to serve as a Professor of Coastal Engineering at the Tallinn University of Technology in Estonia, explained that "The Estonian Academy of

Sciences played a key role in vetting the technical application and environmental impact assessment that Gazprom and its partners first submitted for the Nord Stream 1 pipeline - and we found significant deficiencies that led to our advisement to the government to block the project's construction in Estonian waters. In fact, the successful support of the Nord Stream 1 technical review process established our Academy of having a multidisciplinary capacity that can support the national security of Estonia itself." As for military and intelligence concerns with Russia's deployment of the Nord Stream pipelines? Soomere explained that he, "would be shocked if Russia didn't use the deployment of the Nord Stream pipelines for intelligence purposes, such as the installation of hydroacoustic arrays. This has been a longstanding concern."

Concerns about such potential also were prominently raised during the Nord Stream 2 construction process. From the United States perspective, senior officials had raised similar concerns about Nord Stream 2 in 2018, including U.S. Deputy Assistant Secretary of State for Energy Diplomacy Sandra Oudkirk, who warned that the deployment of the pipeline "could become a pathway for Russia to install high-tech monitoring and listening equipment in the Baltic Sea."[146]

Also concerned was Mykhailo M. Gonchar, Founder and President of the CGS Strategy XXI think tank in Kyiv, Ukraine, the editor of the Black Sea Security Journal, and former Advisor to the Secretary of the National Security and Defence Council of Ukraine, authored a report in October 2021 entitled "Concealed Activity of the Russian Navy in the Area of the Nord Stream 2 Pipeline at Completion Stage," based on maritime data sourced from "private communications with ship tracking experts around the Baltic Sea region" according to Gonchar. The report claimed that as Russia was completing the construction of Nord Stream 2 using its own fleet (which needed to take over after western construction service providers exited the project owing to the passage of U.S. sanctions in December 2019), Russian maritime multipurpose vessels and military personnel had been observed aboard Russian vessels "in the work zone," including "a group of seven servicemen from the Russian Navy's Baltic Fleet Separate Special Purpose Detachment No. 313 for countering underwater diversionary forces."[147]

According to Gonchar, "The covert presence of military personnel on board civilian vessels is fully consistent with Soviet/Russian practice of performing special operations. Given that over the past ten years, the Main Directorate of Deep-Sea Research of the Russian Ministry of Defense (GUGI) has been extremely active in various areas of the World Ocean, and especially in the seas around Europe, this means that they have been preparing the ground for special operations. Also, in the case of Russia's aggression against Ukraine, on the example of the Black Sea, we have observed Russia's actions to use civilian infrastructure (in particular, drilling rigs on offshore gas fields seized in Ukraine) for military purposes – to install radars and sonar devices on them, providing control over sea, air and underwater spaces."[147]

Gonchar points out that, in his opinion, "the special mission of the joint detachment [as described in the report] under the command of the GUGI on board the Salvage/Rescue vessels <BAKHTEMIR> and <SPASATEL KAREV> was to determine the locations for installing hydroacoustic devices to control the movement of submarines and surface ships of NATO member states, the locations for potential deployment of underwater anti-submarine mine complexes, as well as for laying explosive devices at "H" Time, when the Kremlin will make a decision to destroy underwater gas pipelines, power and telecommunications cables to bring chaos to Europe."[147]

OSINT and Field Analysis

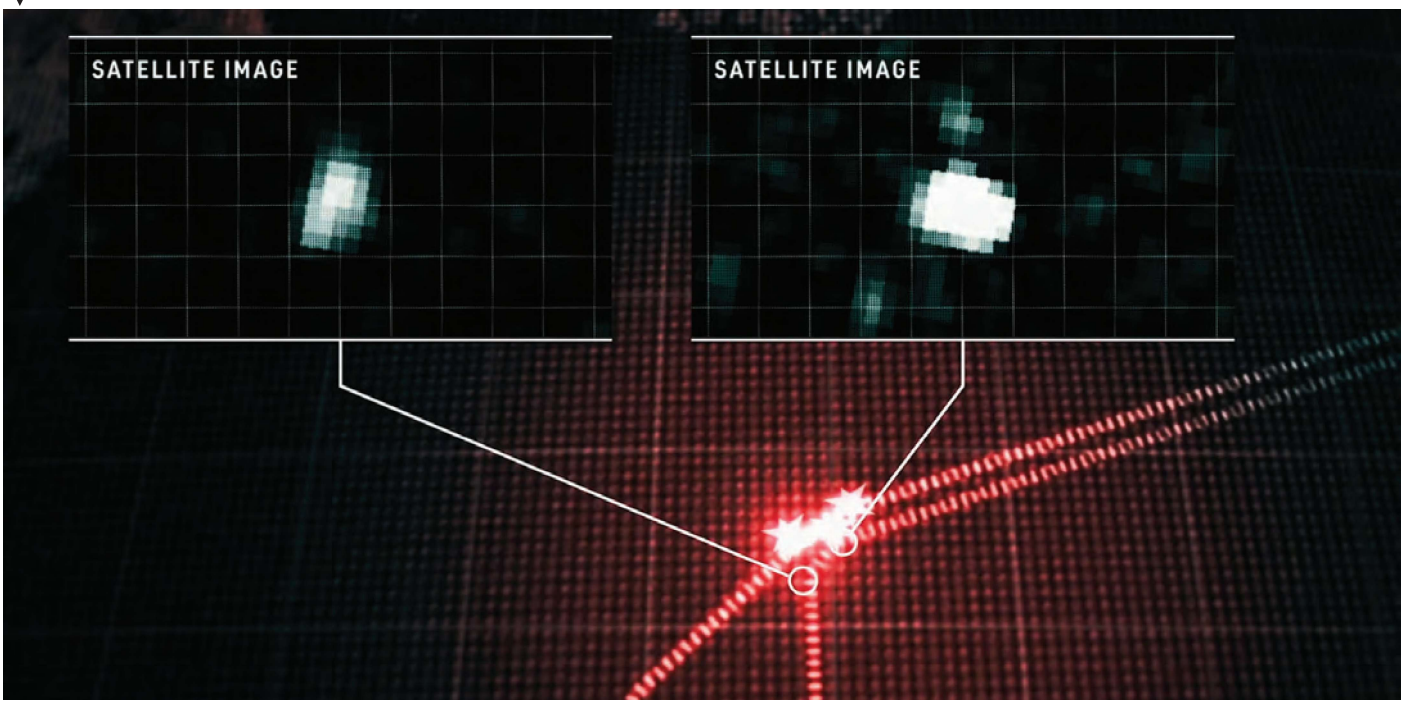
With the economic, legal, energy security, information environment, and national security context in mind, as described in the previous sections, this research project also undertook significant OSINT data analysis, as well as field analysis during visits to the Island of Bornholm, the Ports of Warnemünde and Hohe Düne near Rostock, Germany, as well as a chartered research expedition to the Nord Stream 2 blast site southeast of Bornholm in September 2024.

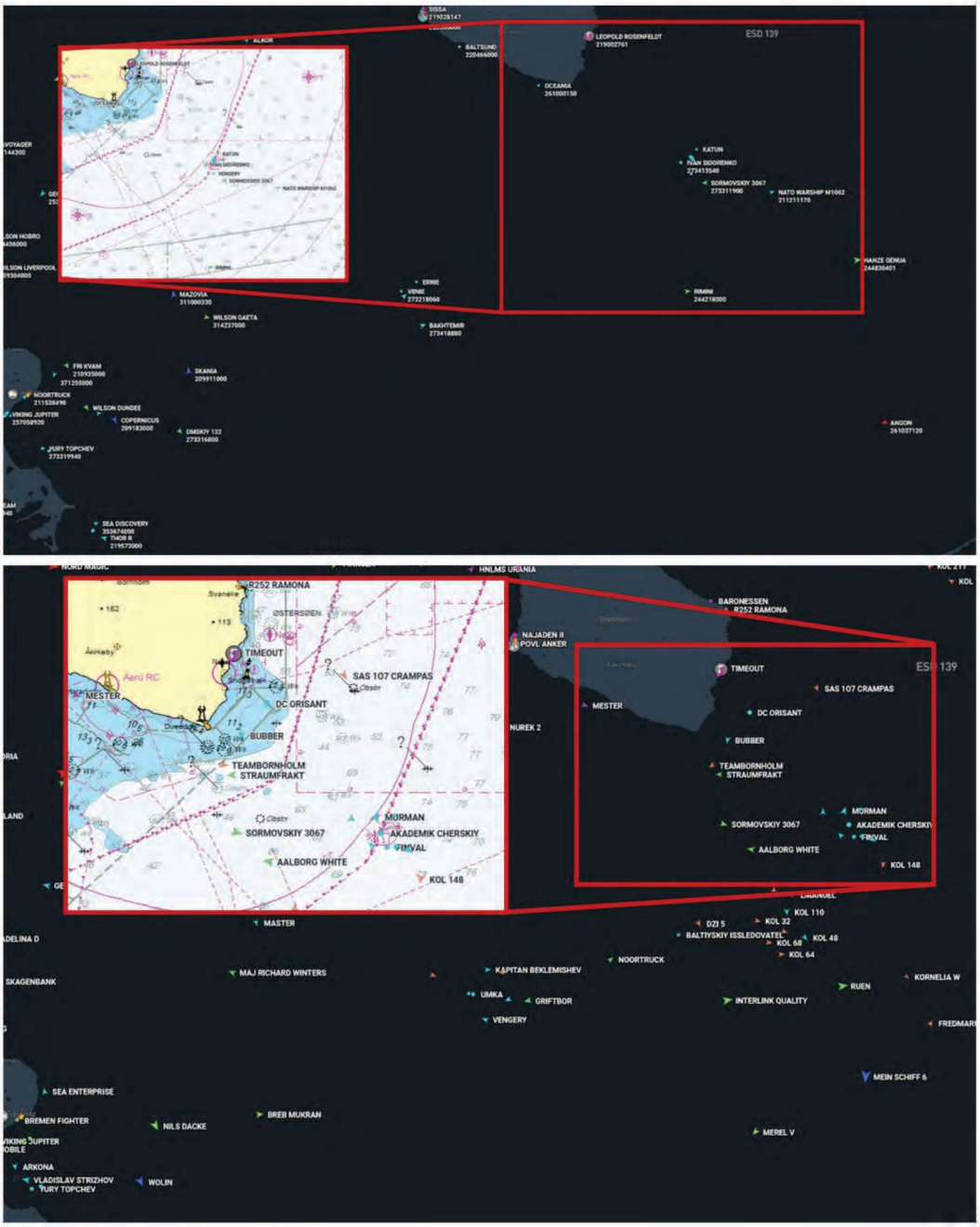
The aim of the OSINT data analysis in this case study was to build on knowledge already made public from other researchers and investigative journalists. Furthermore, this OSINT also builds on years of open-source maritime AIS-based Situation Reports (SitRep) updates that had been developed by Schmitt between 2020 and 2022 related to the tracking of potential sanctionable activities during the construction of Nord Stream 2, and then to document the forensic investigation and response process following the sabotage incidents. A selection of open-source AIS-based mapping these SitRep updates over these years produced by Schmitt is included in **[APPENDIX C]** of this volume.

Most notably this project has also built on research aimed at expanding on the data analysis presented in a pan-Nordic public broadcasting documentary "Skyggekrigen: Brennpunkt" which was released in Spring 2023 from DR, NRK, SVT, and YLE, in which a team of Nordic journalists looked at open source satellite data, including optical and Synthetic Aperture Radar (SAR) sources combined with radio frequency analysis, to identify a group of Russian military and subsea warfare vessels that were observable at the site the Nord Stream blasts northeast of Bornholm already in June 2022, as Gazprom was simultaneously decreasing the gas flows via Nord Stream 1 as described in the previous section.[122]

This OSINT maritime analysis, led by Håvard Gulldahl (who was consulted during the development of this report) and colleagues from the Norwegian public broadcaster NKT included the identification of several

[FIGURE 12] Still image from the pan-Nordic public broadcasting documentary "Skyggekrige: Brennpunkt" which was release in Spring 2023 from DR, NRK, SVT, and YLE. Still image shows SAR data shown over an illustration of the pipeline route from June 2022 (provided by KSAT) of what the investigators identified as multiple Russian military vessels stationary at what would become the Nord Stream blast sites northeast of Bornholm nearly three months later in September 2022. */ CREDIT: DR, NRK, SVT, YLE, KSAT*[122]





[FIGURE 13] MarineTraffic AIS data of the Nord Stream 2 construction zone southeast of Bornholm on April 25, 2021 at 09:03:36 UTC showing Russian flagged pipeline construction vessels, including the <AKADEMIK CHERSKIY> operating directly above what would become the Nord Stream 2 blast site in September 2022. (Above) AIS data from April 16, 2021 at 00:12:03 UTC. (Below)AIS data from April, 25 2021 at 09:03:36 UTC.

FIGURE DESIGN: B. L. Schmitt / AIS DATA: MarineTraffic

Russian military vessels operating as "dark vessels," with their Automatic Identification System's disabled, and thus untrackable via AIS platforms like MarineTraffic. These included the Russian naval research vessel <SIBIRYAKOV>, the tugboat <SB-123>, and other vessels that were not able to be identified at the time, operating near the blast sites northeast of Bornholm on 14 June, according to a BBC report of the analysis. Furthermore, Gulldahl and colleagues were able to identify further Russian military vessels back in the same area of the Nord Stream blast site northeast of Bornholm, including the Russian <SS-750> submarine rescue ship, and the tugboat <SB-123> between 21 and 22 September, just four days before the sabotage incidents took place. According to the report, the <SIBIRYAKOV> is, for example, "believed to be capable of underwater surveillance and mapping as well as launching a small underwater vehicle." **[FIGURE 12]** provides illustration of some of this analysis that appeared in "Skyggekrigen:

[FIGURE 14] (Left) MarineTraffic AIS data of Russian Nord Stream 2 construction fleet south of Bornholm. (Right) Planet commercial geospatial imagery taken with a Planet Dove satellite with 3 meter per pixel resolution. Both the AIS and satellite data show the same location and timestamp of May 29, 2021, illustrating the presence of a "dark vessel" operating in close proximity to the Nord Stream 2 construction fleet without AIS enabled. Additional examples of vessels operating without AIS on in the construction fleet were found during AIS and satellite data comparative analysis during this study.

FIGURE DESIGN: B. L. Schmitt / AIS DATA: MarineTraffic; SATELLITE DATA: Planet

Brennpunkt." [149]

Additionally, reporting from WIRED in November 2022 described data suggesting that "satellite monitors discovered two vessels with their trackers turned off in the area of the pipeline prior to the suspected sabotage in September" in which a commercial satellite data firm reported finding two large-format vessels "each measuring around 95 to 130 meters long, passed within several miles of the Nord Stream 2 leak sites" in the "days immediately before" the leaks were detected.[165]

Extending the "Skyggekrigen: Brennpunkt" (and other media-reported) data sets was a key objective of this report. Therefore, OSINT data analysis focused on observations in the areas proximate to the Nord Stream sabotage sites earlier than the timeframe covered in the Nordic report was deemed essential. This included comprehensive AIS and commercial optical satellite monitoring of the Russian construction fleet for the Nord Stream 2 pipeline over the first half of 2021. It also builds on two previous reports published by Schmitt on the Nord Stream 2 maritime construction process and related sanctions policy for the Jamestown Foundation in March 2020 entitled "They're Gonna Need a Bigger Boat: The Curious Voyage of the <AKADEMIK CHERSKIY>", and the Harvard-Ukrainian Research Institute in May 2020 entitled "Don't Cross the Streams: Why the Ghost of Putin's Pipeline Continues to Haunt Transatlantic Security." MarineTraffic was used as the primary AIS source, and Planet was used as the primary satellite data source.[22,23,150,151]

Using the MarineTraffic and Planet platforms, multiple results were found that raised questions about the particular activities of the Russian construction fleet in 2021 in light of the location and nature of the September 2022 sabotage events, including:

- **That the exact location at which Russian vessels took over construction of the Nord Stream 2 pipeline in early 2021 (after U.S. sanctions forced Western firms, and in particular, Swiss pipelaying firm Allseas to depart the project in late 2019), and over which these Russian vessels would loiter for days at a time during 2021, would eventually be the collocated with the site that**

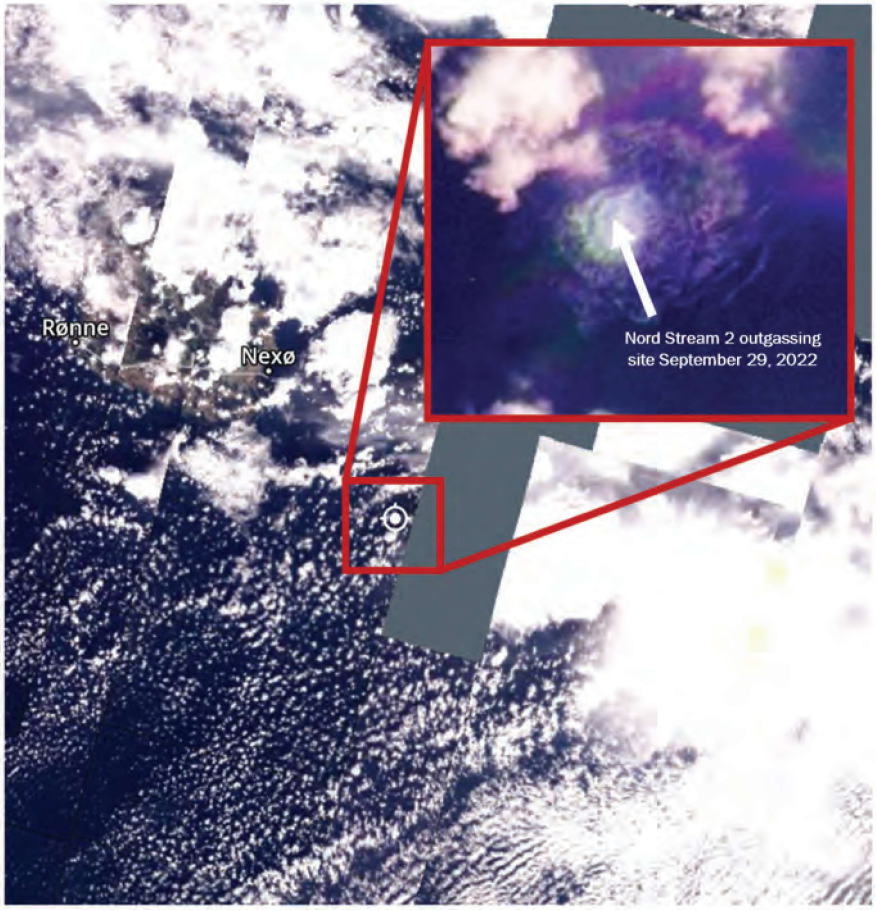
▲

[FIGURE 15] (Above, Left) MarineTraffic AIS data with commercial Planet satellite data illustrating the same location and time - port of Warnemünde, Germany (near Rostock) on April 19, 2021 at 09:35:49 UTC (satellite data from Planet Dove satellite with 3 peter per pixel resolution). Shows an example of a Russian-flagged Nord Stream 2 construction fleet vessel, in this case the <ARTEMIS OFFSHORE> operating at the Nord Stream 2 logistical deployment center in Warnemünde in 2021. (Above, Right) GoogleEarth image showing the close proximity (~1 kilometer) between the Nord Stream 2 logistical deployment center used for construction of the pipeline in 2021, and the reported marina in which the alleged Nord Stream 'pro-Ukraine sailboat sabotage platform was rented from. (Below) Images of rental sailboat <ANDROMEDA> taken by Schmitt on a visit to the marina of Hohe Düne in September 2023.

FIGURE DESIGN: B. L. Schmitt / AIS DATA: MarineTraffic; SATELLITE DATA: Planet, GoogleEarth

the Nord Stream 2 blasts would take place southeast of Bornholm in September 2022. AIS and satellite examples of such activity are found in [FIGURE 13].

- That there were vessels observable via commercial satellite data operating as "dark vessels" without their AIS enabled within the immediate vicinity of the Russian construction fleet for Nord Stream 2 in 2021. [FIGURE 14] provides an example of such activity through a comparison of AIS data and Planet



[FIGURE 16] The outgassing field of the Nord Stream 2 blast site southeast of Bornholm (arrow indicating approximate center of site) as viewed from space. Planet commercial satellite imagery obtained on September 29, 2022.

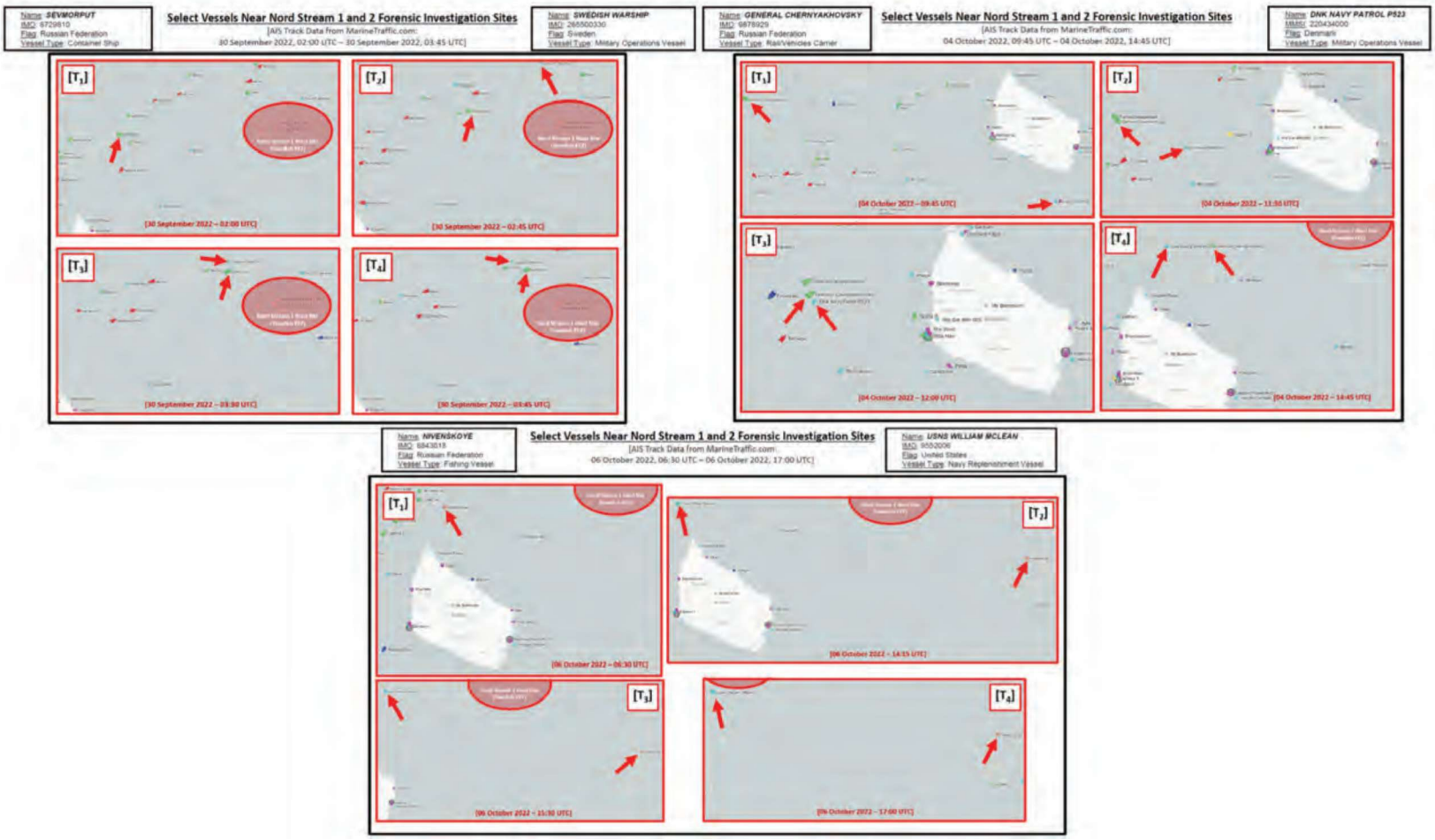
FIGURE DESIGN: B. L. Schmitt / SATELLITE DATA: Planet

imagery;

- **That the marina where the eventual suspect "pro-Ukraine" rental sailboat would be rented from in the marina of Hohe Düne, is in very close proximity to a logistical deployment facility utilized by the Russian Nord Stream 2 construction fleet throughout 2021. [FIGURE 15] provides correlated AIS and satellite imagery showing Russian vessels in the Nord Stream 2 construction fleet utilizing that harbor in 2021, and a visit by Schmitt to find the suspected "pro-Ukraine" sailboat sabotage suspect vessel <ANDROMEDA> in the port of Hohe Düne in September 2023. The visit to the suspect vessel <ANDROMEDA> underscored the relatively small scale of this rental sailboat and further reinforces the skepticism raised by diving and subsea operations experts later in this case study regarding the limited equipment storage space and likely unsuitability of using this sailboat as a platform for the Nord Stream sabotage attacks.**

Additionally, close AIS and satellite monitoring was also focused on the same area in the weeks after the Nord Stream blasts took place, in which Planet imagery shown in **[FIGURE 16]** shows the extent of the Nord Stream 2 outgassing event as viewed from space, and providing results including:

- **That at least three Russian-flagged vessels attempted to approach the Nord Stream 1 blast site in the days following the incident, which appear to have been intercepted and escorted away from the sites by Swedish, Danish, and United States naval and coast**

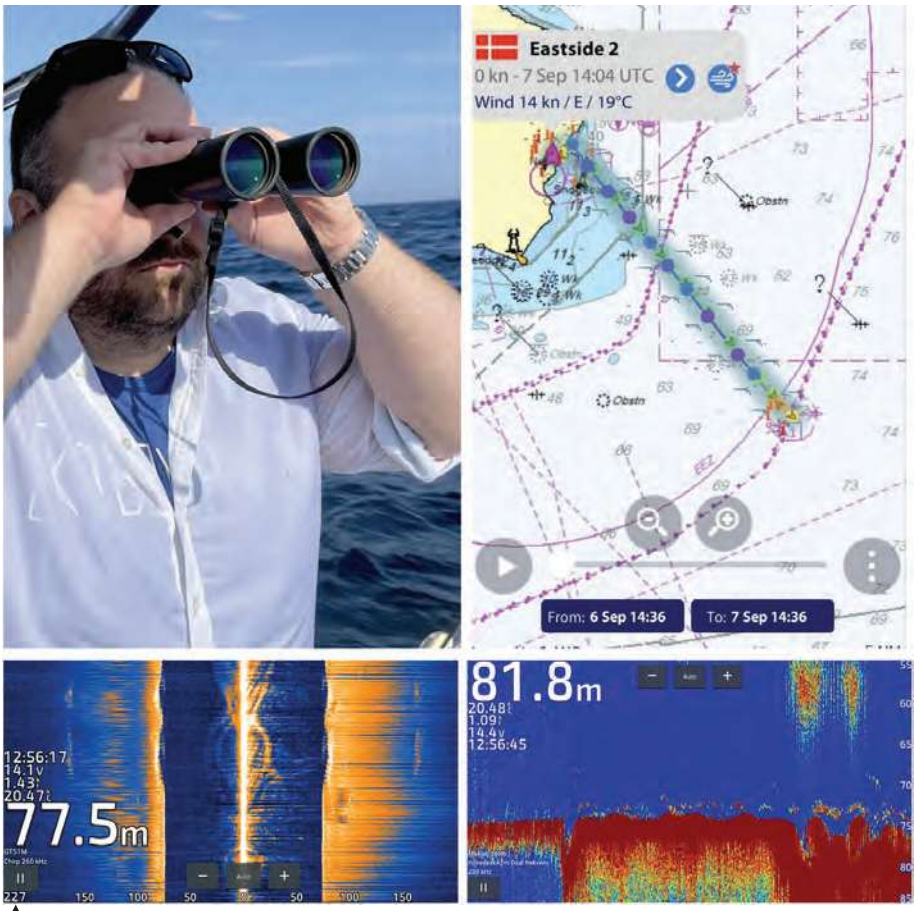


▲ *[FIGURE 17] Examples of at AIS data of least three Russian-flagged vessels that approached the Nord Stream 1 blast site in the days following the incident, which appear to have been intercepted and escorted away from the sites by Swedish, Danish, and United States naval and coast guard assets, all three of which were found at the October 2023 Balticconnector damage site either during the incident, or else in the days immediately following. The earlier interview with Matthias Lindholm from the Swedish Coast Guard confirmed that the Russian nuclear class icebreaker <SEVMORPUT> was among the Russian vessels escorted away from the Nord Stream blast site in the Swedish exclusive economic zone following the Nord Stream sabotage – a vessel who would be found escorting the Chinese-flagged container ship <NEWNEW POLAR BEAR> in October 2023 at the time and location of the Balticconnector pipeline incident.*

FIGURE DESIGN: B. L. Schmitt / AIS DATA: MarineTraffic

guard assets, all three of which were found at the October 2023 Balticconnector damage site either during the incident, or else in the days immediately following. The earlier interview with Matthias Lindholm from the Swedish Coast Guard confirmed that the Russian nuclear class icebreaker <SEVMORPUT> was among the Russian vessels escorted away from the Nord Stream blast site in the Swedish exclusive economic zone following the Nord Stream sabotage – a vessel who would be found escorting the Chinese-flagged container ship <NEWNEW POLAR BEAR> in October 2023 at the time and location of the Balticconnector pipeline incident, which will be highlighted as the main case study in the next volume of this series. [FIGURE 17] provides AIS analysis of these intercept and escort incidents of Russian vessels near the Nord Stream blast sites around Bornholm in early-October 2022.

Finally, **[FIGURE 18]** provides details of an offshore research expedition aboard the chartered fishing vessel with sonar equipment, the <EASTSIDE 2> on September, 7 2024. The vessel was owned by Eastside Marine Company in the Port of Nexø, Bornholm, and captained by Kim Finne,



[FIGURE 18] Research expedition conducted for this study to obtain sonar data of the Nord Stream 2 blast site southeast of Bornholm on the chartered fishing vessel <EASTSIDE 2> on September 7, 2024.

FIGURE DESIGN: B. L. Schmitt / AIS DATA: MarineTraffic

owner of Eastside Marine. Analysis of this preliminary sonar data shows significant damage to the Nord Stream 2 trunkline at the blast site southeast of Bornholm, as well as significant blast craters in the normally flat Baltic seabed roughly five meters in depth.

The expedition also illustrated first hand just how close to the boundary of the Danish territorial sea the blast took place, in the Danish exclusive economic zone just hundreds of meters from the boundary, potentially suggesting the selection of the location as one in which Denmark would have more limited response options under the UN Convention on the Law of the Sea than if it were in the territorial sea. This possibility also holds for the blast sites northeast of Bornholm, which reside in the Swedish exclusive economic zone, rather than territorial sea.

Climate Consideration

Climate considerations also have been significantly tied to the Nord Stream sabotage attacks. The estimates of how much methane was released in the attack varies from 40,000 tones, as estimated in the lowest possible range by the Norwegian Institute for Air Research immediately after the incident on September 29th, based on date available at that time, and then immediately upgraded to at least 80,000 tones, with the analysis performed the day after. NIAR concludes at that time that this volume is more than four times the Norwegian national annual methane emission from the oil and gas industry. However, this early simulation was based on data from available monitoring stations and it did not show the total gas cloud, only the part of it that is close to the surface. Danish Energy Agency estimated that the escaped methane amounted to 370,000–500,000 tones and was equivalent to 0.1% of the annual emission of methane. And PBS News estimated that the amount released was to 500,000 tones, which is five times

▲
[FIGURE 19] Offshore renewable energy infrastructure protest signs on the island of Bornholm, Denmark (August 2023). Translations: Left - "Bomb Target No." Right - "Energy Island No".

PHOTO CREDIT: B. L. Schmitt

the size of gas released from Aliso Canyon underground gas storage leak— largest terrestrial release of gas in US history. A comprehensive overview of these and other studies has been published in January 2024 together with multi-phase pipeline modeling with conclusion that Nord Stream blast, estimated at 478,000 tones, was the world's largest natural gas leak.[153,154,155,156]

The leak impacted also GHG accounting for countries concerned by territorial ownership of the damaged pipeline. As the major gas leak from the sabotaged section of the pipeline happened in Sweden's territorial waters, its greenhouse gas emissions has risen in 2022 by 7%, i.e. by 5.8 million tones of carbon dioxide equivalents (MTCO2EQ), as evaluated by the Swedish Environmental Protection Agency. The same Agency estimated that the amount the leaks in the Danish exclusive economic zone, which are not included in the Swedish data, equaled to 8.5 MTCO2EQ, meaning the Nord Stream leaks had a total impact of around 14 million.[157]

The impact of sabotage goes much beyond the environmental or economic sphere. It impacts deeply concerned populations as well as politics. The protection of offshore energy and critical infrastructure is vital to ensure that citizens of democracies continue to support deepening the European energy infrastructures, including the deployment of renewable energy systems, so that worries about infrastructure insecurity doesn't lead populations to reject the development of new energy infrastructure. Just few of days after the Nord Stream sabotage occurred, an unexpected power outage was registered on the island of Bornholm adding to worries that further energy systems being developed in the offshore due to the Nord Stream blasts creating worries that the more infrastructure is developed in the offshore, whether or not it is "green" is too much of a risk for citizens to accept since it would provide a target for Russian sabotage. In November 2024 the Swedish government decided to reject 13 Baltic Sea wind farms, citing defense concerns.[158,159,160]

▲ ***[FIGURE 20] Protest buttons that were placed at booths around the COP28 conference in Dubai, United Arab Emirates in December 2023 espousing what this study assesses is a highly improbable view that the United States was behind the Nord Stream sabotage incidents.***

PHOTO CREDIT: Received by B. L. Schmitt from a colleague attending COP28 the day after Schmitt departed the same conference.

The continuous pressure against European critical infrastructures and interconnectors between countries not only exposes its fragilities but also weakens the case for further integration of European energy networks. In the absence of sufficient domestic energy resources, solidarity and interoperability of the energy infrastructures are critical for Europe to survive. Uncertainty around the offshore and critical infrastructures adds important weight on future energy projects linking the European countries.

For example, **[FIGURE 19]** provides photos from Bornholm where a farmer had put up in their field, protest signs against the renewable Bornholm energy island development, based on the fact that Nord Stream had been attacked, and that, presumably, they were concerned with any further offshore energy infrastructure developments since they could become targets of (presumably Russian) sabotage incidents. The sign pictured on one side reads "Bombemål NEJ" - "Bomb Target No" (meaning that the farmer does not want Denmark to develop more offshore energy infrastructure that could be a target of bombing, and includes a drawing of the map of Bornholm, with a red dot illustrating the Nord Stream 2 blast site southeast of Bornholm) and the other side reads "Energi-Ø NEJ" - "Energy Island No" (meaning a rejection of the Danish Energy Island project on the same grounds as previously described).

Furthermore, during the United Nations Framework Convention on Climate Change (UNFCCC) COP28 summit in Dubai, United Arab Emirates in December 2023, the Nord Stream saga made a subtle appearance. Protest buttons were found distributed and left at booths around the conference, pushing what we assess is the highly improbable view that the United States was behind the Nord Stream sabotage. In particular, the buttons led with the slogan: "CLIMATE CRIME – U.S. blew up the Nord Stream Pipeline." **[FIGURE 20]** provides a photo of one of the protest buttons that were found left behind on unrelated booths in the COP28 "Blue Zone" in Dubai.[161]

Expert Analysis and Commentary

Building on the contextual, OSINT, and field research analysis that has been provided as a part of this study of the Nord Stream 1 and Nord Stream 2 sabotage incidents, we conclude this case study with a series of expert commentary responses, nearly all of which were provided on the record and raise significant questions about some of the current media narratives related to the Nord Stream blasts, while providing further context bolstering the likelihood that the Russian Federation was involved in the incident. Those responses include:

- **Multiple commercial and military technical divers and subsea demolitions experts that were**

interviewed as a part of this study significantly questioned the technical feasibility that the rental sailboat <ANDROMEDA> would have been a practical platform to launch even a covert diving operation of this scale, as has been described in publications cited at the outset of this case study. Multiple naval officials and experts echoed the claims of the divers interviewed as a part of this study. Many of these experts also questioned why divers would be used at all for such an operation, regardless of the party or motivation behind the attack given the risk involved compared to the use of an ROV or similar system. One of the commercial divers pointed out that while they reject the notion that <ANDROMEDA> was used to conduct the attack, they also reject that Russia could have been behind the action.

BOX 09

Eyk-Uwe Pap, the general manager of the commercial diving firm Baltic Taucher in Rostock, Germany. Mr. Pap has decades of experience performing and overseeing commercial technical diving and related deployments in the Baltic Sea and elsewhere, developing diving techniques, and technologies to help construct and maintain subsea infrastructure projects in the region.

"To me the sailboat story is just that - a story - and a pure science fiction one. I consider it to be very unlikely that the <ANDROMEDA> could have been used as the platform for the Nord Stream pipeline sabotage, and furthermore such an operation would have likely required significant investment in professional equipment and technical divers."

Mr. Pap underscored his conviction by pointing out that since the incident took place, he was brought onto the <ANDROMEDA> two times to study the vessel, which is located close to Baltic Taucher's offices, and is all the more convinced that this is nothing more than a rental sailboat that in his opinion would have been an unsuitable platform for such an operation.

At the same time, Pap pointed out that he also doubted that the Russian Federation would have targeted their own pipeline, given that he assessed it as unlikely that Russia would "shoot themselves in their own knee rather than receive millions for gas via the project."

BOX 10

Kaido Peremees, Commercial diver and CEO of Tuukritööde OÜ, a commercial diving company based in Tallinn, Estonia, that focuses on a wide variety of maritime industrial areas, including subsea drilling and demolition of metal and rock, underwater structural investigations, maritime search and rescue, marine sonar surveys, and hull surveys for maritime classification societies. Kaido has been working in commercial diving since 1996, and has been involved in complex subsea security and industrial operations, including the demolition of World War 2 depth charges on the Baltic seabed, harbor clearance operations including boulder and rocky bottom demolition. Mr. Peremees holds a professional certificate as a subsea explosive materials handler.

"While it is technically possible to use of a sailboat like the <ANDROMEDA> for the Nord Stream sabotage, like that being described in German media, it is however not feasible that it was the platform used for the attacks.

If we go on the assumption that the quantity of explosives needed to carry out the attack was 150-300 kilograms, as suggested by some of the early seismic evaluations, then such an operation launched from the <ANDROMEDA> seems unlikely. Such an explosives payload would be difficult to handle on board, the barrels would be difficult to move over the side of the sailboat and be manipulated by the divers, and its buoyancy would need to be correctly accounted for. It would ultimately be a lot easier to drop these barrel sized objects onto the pipeline with the help of a real-time kinematic GPS system, and then determine the placement of each dropped charge using a small downline with a side scanning sonar or else a small, cheap ROV – with this quantity of explosives, they could be a couple of meters from the pipeline, and still damage the pipes.

On the other hand, if smaller charges, of 15-25 kilograms were used then it would be more straightforward for these to be carried to the seabed by divers. However, I would question in this case why a diver would even be used, since you could simply use a cheap ROV, or downline coupled with sonar or cameras to help guide the placement of the charge. This would be both faster and lower risk than making a dive to the seabed.

Furthermore, if the idea is that this would be a covert operation, then sailing on a sailboat is in fact a highly visible platform, even more so since it is a rental sailboat – and one that would have a large radar cross-section that could be easily detected.

For a dive of 80 or more meters in depth, a downline would need to be deployed to preserve as much time on the seabed as possible to carry out a possible operation. Without a downline, a diver would waste a lot of time on the seabed searching for the pipeline even if you had a good surface sonar read of the location.

Diving with personnel at all for such an operation would be a stupid plan, and highly risky. You could mitigate a lot of risk by simply using a smaller side scanning sonar, locate the pipeline, and then use a down line to guide a depth charge to the seabed with a delay time. Or you could use a larger ship moving along the pipeline to simply drop some plastic barrels of explosives overboard with delay timers.

If you are following the rules, then everything below 50 meters would be treated as a technical dive that would require a lot of supporting equipment including a large number of mixed gas bottles and possibly a portable decompression chamber. Of course, if an operation disregards the lives of its own team, then it is theoretically possible to attempt a bounce dive to 70 or 80 meters in depth on air, but the risk would be extremely high, especially if SCUBA is used. That's why assessing this operation is dependent on the risk tolerance and acceptance of higher probability of loss of life – something that is unthinkable in commercial diving might be considered normal in war.

From my experience working in commercial subsea demolition, the explosives used here would have been provided in a container. So it wouldn't make sense that there would be explosives residue found inside the sailboat as those materials should have already been packaged and contained before loading them onto the sailboat. What are you doing, waiting until you get out on the sea and then building the explosive packages on the kitchen table of the sailboat? This would be utterly unprofessional for such an operation."

BOX 11

Oskar Frånberg, Associate Professor of Marine Systems Engineering at the Blekinge Institute of Technology in Karlskrona, Sweden. Frånberg additionally is an accomplished diver, having previously served as an Explosive Ordnance Disposal (EOD) diver for the Swedish Navy

"It is unclear what would be gained by using a sailboat as the platform to launch such an operation from - you could still use a motorized vessel with a more stable platform and remain largely undetected, so it appears to have been an unnecessary risk. Generally speaking, an operation like this would be aimed at risk reduction, but using a sailboat would actually increase that risk and unnecessarily so given the wide range of options that could have been used to plant the explosives on the Nord Stream pipelines. These include using a pipeline inspection gauge (PIG) if the blast took place internally, or if explosives were planted externally an ROV from a surface ship, using technical divers, or even simply dropping explosive devices."

BOX 12

Captain (Ret.) Jukka Savolainen, who served as the Commander of the West Finland Coast Guard district from 2012 to 2017, and is currently an expert on hybrid threats to critical infrastructure and maritime security at the European Center of Excellence for Countering Hybrid Threats in Helsinki, Finland.

From his operational experience in maritime security in the Baltic Sea, Savolainen explained that he remains "very skeptical about the <ANDROMEDA> reports - a recreational sailboat of that size would be very difficult to keep steady and while not impossible, it would be an unfit delivery vehicle for a technical diving operation transporting potentially hundreds of kilograms of explosives to the seabed." Captain Savolainen underscored his skepticism in both of the current media narratives, including the pro-Ukrainian <ANDROMEDA> sailboat as the sabotage vessel with reports mostly emerging in German press, as well as the 2023 Seymour Hersch account that the United States was behind the attack.

The <ANDROMEDA> and Hersch stories are truly hybrid masterpieces," claimed Savolainen, whose research often focuses not only on Russian hybrid maritime security threats, but also the vectors of disinformation associated with Russian gray zone tactics.

BOX 13

Hans Liwång, Professor and Deputy Head of the Department of Systems Science for Defence and Security at the Swedish Defence University

"For an operation like this, to evade attribution, it would be stupid for an actor to use official state vessels for such an operation, whatever country they might be from. While a sailboat is closer to the sort of an operation needed to reduce risk of attribution, it still would not be the type of vessel that would be needed for such an operation. In this case, a larger commercial or fishing vessel would offer a better platform. Liwång added that he had spoken with divers that have special operations experience, and in their opinion the Nord Stream "job can have been performed without divers".

Moreover, Liwång pointed out that the divers he spoke to say a sailboat is an unlikely platform since "a sailboat would not be a good platform for divers as it would likely require a lot of technical equipment" for such an operation. Commenting in late December 2024, Liwång stated that "Right now, I still have problems with all of the various theories that have been reported to be potential explanations for the sabotage of the Nord Stream pipelines."

In term of the pathology of the Nord Stream blast sites themselves, he thinks that the pathology of each blast site is driven less by the initial explosions themselves, and more by the resultant gas escape pressure and resultant hydrodynamics at play. Professor Liwång assesses that the gas pressure escaping the ruptured trunklines would have bent the pipes and made the pipe joints force apart and create secondary blast areas around the adjacent seabed.

BOX 14

Johannes Riber, an active-duty Commander in the Royal Danish Navy and a Ph.D. Fellow at the University of Copenhagen focused on sea power

Commander Riber expressed a level of exasperation with the continued focus, mostly by German media, solely on the <ANDROMEDA> account. "The so-called 'pro-Ukraine sailboat' explanation of the Nord Stream sabotage is possibly the most stupid thing I've ever heard - except for the Seymour Hersh account that suggested that the U.S. and Norway teamed up to take out the pipeline - that is stupider."

Commander Riber explained that Swedish media investigations of the seabed around the Nord Stream blast sites showed pipe material scattered roughly a hundred meters from the pipeline route. For this to happen, explained Riber, "you would likely have the explosion blow parts of the pipe segments upward in the water column and then drift until they re-settled on the seabed, given the hydrodynamics and currents at play, with the outgassing from the pipeline itself contributing to the drift effect."

Riber also stressed the difficulty of any diving in the deeper areas of the Baltic Sea, such as where these sabotage incidents took place. According to Riber, "at the depth the explosions took place, there is no natural light and the visibility in the Baltic Sea is generally horrific - it's like diving in a soup with no lights on." He also pointed out that for a diving operation, "one would expect that a shallower section of the pipeline would have been targeted." He added that the selection of a deeper target site would make sense from an attribution-avoidance perspective, but also could point to other delivery scenarios, such as a minisub or ROV having been used rather than divers - capabilities that the Russian military vessels observed in the area of the Nord Stream blast sites ahead of the explosions would have had, while a sailboat would lack.

The extent of equipment that could feasibly be loaded and transported on a sailboat like the <ANDROMEDA> also was highlighted by Riber. "For example, the Danish Navy wouldn't mount a diving operation below 29 meters in depth in the absence of a decompression chamber, full stop. Clearly any large decompression chamber would be impossible to fit on the <ANDROMEDA>, and would require significant support equipment and power needs to generate sufficient internal pressure for treatment. Of course, if you accepted significantly higher operational risk, you could proceed without a decompression chamber, but if anything went wrong, it would risk attribution of the attack since a sick crew member would need to be rapidly transported to a coastal hospital for treatment."

Riber also questioned how a significant cargo of explosives, detonators, and related equipment could be driven and loaded on the sailboat without a significant risk of detection.

BOX 15

Jacob Kaarsbo, a Copenhagen-based independent security policy advisor, and former Chief Analyst for the Danish Defence Intelligence Service

"The bottom line is that it is documented that Russia had both the intent and the capability to carry out the Nord Stream attacks. It fits the pattern of Russian hybrid attacks and Russian preparations for attacks against subsea infrastructure is amply documented. When we examine the media allegations that Ukraine carried out the attacks both intent and capability are highly dubious".

Danish Defence Command has confirmed that it is in possession of 122 photos of 6 Russian Navy vessels at the blast sites four days prior to the blasts. One of the vessels was the SS-750 which had a mini-submarine for subsea warfare onboard. It's also been documented that a flotilla of Russian vessels had been loitering in the area, likely for reconnaissance, already in June. So Russian capabilities were in place.

It's highly unlikely that the Andromeda (a plain sailing yacht) could serve as a platform for an operation of this magnitude and complexity, especially with a flotilla from the Russian Navy in the area at the same time. The alleged two divers doing multiple dives at that depth, with both a small and sophisticated blast requiring precision and a large blast requiring a large and have payload of explosives is highly unlikely. So several question marks about Ukrainian capabilities."

BOX 16

Peter Doran, Adjunct Senior Fellow at the Foundation for the Defense of Democracies who has studied Russian energy weaponization tactics for decades.

"The problem with a suicide mission is that it is suicidal. The operational requirements of the alleged "Ukrainian sailboat" theory were just that: certain death for the divers. The deep-water with the knowledge, training, and experience to complete such a mission would have known that the hairbrained scheme and conditions violated the first rule of diving: don't die."

- **Media reports claiming that the <ANDROMEDA> sailboat operation was directed by the former Chief of the Ukrainian General Staff Zaluzhnyi need to be analyzed in the context of Ukrainian military and security operations and chain of command.**

A current U.S. government official with extensive expertise in NATO and Ukraine security issues raised concerns with this point, arguing that "Most proponents of the "six Ukrainians on a sailboat," theory agree that a unit reporting directly to former Chief of the General Staff Valeriy Zaluzhnyi carried out the operation but without the knowledge of President Zelenskyy. Setting aside the many discrepancies and inconsistencies regarding the individual operatives alleged to be involved, none of these reports actually reflect our understanding of how Ukraine carries out overseas covert action and sabotage. Military covert operations and sabotage or other direct action generally fall under the purview of Ukraine's Main Directorate of Intelligence of the Ministry of Defense (HUR). HUR does not actually report to the Ukrainian Chief of the General Staff; it reports through the Ministry of Defense to the President of Ukraine. None of the other Ukrainian intelligence services notionally capable of conducting complex sabotage operations such as the SBU, Ukraine's domestic security service, or FISU, the Foreign Intelligence Service report to the Chief of the General Staff either; they too report directly to the President. While the Ukrainian military's Special Operations Forces include units specializing in underwater demolitions, it is highly unlikely that such elite units would have relied on the amateur operators--many of whom have been publicly identified either living in Russia or with links to pro-Russian activity--alleged in news reports."

- **Poland shared intelligence with German officials suggesting Russian actors may have been behind the attacks, and that the transport of explosive materials would have been a difficult and high risk within the EU, according to senior Polish national security and intelligence officials, respectively. Additionally, media reports of a search of the <ANDROMEDA> in a Polish port in September 2022 before the Nord Stream blasts was allegedly due to a noise complaint, undermining the covert nature of the possible sailboat operation.**

According to Stanisław Żaryn, National Security Advisor to the President of Poland, "Poland's intelligence shared data on the Nord Stream sabotage case with German officials, and the findings suggested Russian actors may have been behind the attacks." Furthermore, speaking on the motivation for the Polish search of <ANDROMEDA> in September 2022, Żaryn explained that, "Polish Border Guard searched the sailboat <ANDROMEDA> during a brief visit to a Polish harbor in September 2022, but the motivation for the search was fairly ordinary - allegedly a noise complaint that was called in against the passengers of the <ANDROMEDA> who appeared to have been throwing a party. The Polish Border Guard inspection of the sailboat yielded nothing unusual, with the sailboat appearing to be nothing more than a typical tourist vessel."

Żaryn also underscored Poland's assessment that "Russia's military intelligence, the GRU, has been

known to use the tactic of recruiting non-Russian nationals via Telegram channels to do easy jobs to earn easy money, ranging from spray painting anti-Poland and anti-NATO slogans, to physical sabotage against rail lines that transported materials to support Ukraine, all the way to proposed political assassinations. This tactic especially increased after Poland acted to expel as many Russian intelligence agents as possible earlier in Russia's war against Ukraine."

Furthermore Piotr Krawczyk, former Chief of the Polish Foreign Intelligence Agency pointed out that, "we need to remember that there haven't been any major terrorist attacks that have used explosive materials in this way for several decades in Europe. This is due to the tight controls that European governments have placed on sourcing such materials within the EU, and also strong border detection capabilities and enforcement - there is a high chance that an actor would be detected and apprehended if trying to move illicit goods like drugs and explosive materials across the EU border and within the EU - so while this is not impossible to imagine, it would be operationally very risky."

- **The communications approach by the Swedish and Danish investigations differed from the German investigation, with very few media leaks emanating from the Swedish and Danish investigations, whereas many anonymous leaks had emanated from the German investigation. Outside of the recent arrest warrant announcements by German prosecutors for at least one Ukrainian national, German security officials have been cautious to message to the public that a possible false flag operation may be at hand in this case.**[162]

  - This includes a statement in March 2023 in which German Defense Minister Pistorius cautioned the public that "We have to make a clear distinction whether it was a Ukrainian group, whether it may have happened at Ukrainian orders, or a pro-Ukrainian group (acting) without knowledge of the government," adding that the likelihood was "equally high" that it could have been a "false flag operation staged to blame Ukraine."[163]

  - Furthermore, while not an active official at the time, it should be noted here that speaking just days after the Nord Stream sabotage took place, Gerhard Schindler, former president of the German Federal Intelligence Service was quoted in Politico as having explained to Welt that "an unnoticed, conspiratorial damage to pipelines at a depth of 80 meters in the Baltic Sea requires sophisticated technical and organizational capabilities that clearly point to a state actor. Only Russia can really be considered for this, especially since it stands to gain the most from this act of sabotage." [167]

  - Experts raised a similar possibility of the <ANDROMEDA> as a diversionary operation, such as Jakub Godzimirski. Recalling his initial reaction to the emergence of the <ANDROMEDA> reports, "my first reaction was that this could be a false flag operation by Russia." Godzimirski added that he still considers it likely that Russia was behind the attack, and that "even if the reports that Ukrainian nationals might have been operating the sailboat, Russian security services could have organized this in an attempt to blame Ukraine for the incident."

- Tom Røseth, Associate Professor of Intelligence Studies at the Norwegian Defence University College, Command and Staff College, also pointed out that "Even if tracks ultimately lead to Ukrainian actors being involved in the sabotage of the Nord Stream pipelines, investigators need to have an open mind on the potential that Russia could have staged the attack using Ukrainian actors – to the very least not exclude it. The crux is to find out who ordered the operation. Russian intelligence has a significant capability for intelligence and sabotage operations in Ukraine who certainly would have the connections, means, and money to get Ukrainian actors involved – whatever motivation these might have. Even with the current reports out via media sources, rather than government statements, significant questions need to be answered."

- **Furthermore, for the few public statements that have been made related to the investigations, a UN joint statement on the state of play of the three investigations to the UN Security Council issued on July 10, 2023 indicated an unwillingness to supply one, merged statement of current conclusions, rather the investigations were summarized separately. Additionally, of the three statements, only the German investigation statement mentioned the <ANDROMEDA>**.

  This is a public United Nations document posted online, and is included, in full, in the supplementary **[APPENDIX B]** materials following this report.

- **Questions have also been raised regarding the timeline and personnel alleged to have been involved in the <ANDROMEDA> operation according to media reports, contradictory reports of military and intelligence assessments, as well as further irregularities regarding assessments of the feasibility of the alleged operation.**

- While there have been German media reports citing leaks from German government sources claiming the identities of several Ukrainian nationals that are allegedly suspected of taking part in the <ANDROMEDA> expedition, significant questions have been raised by investigative journalists in Germany. This includes Germany's N-TV, which detailed claims surrounding a Poland-based shell company that was allegedly used as a front to rent the <ANDROMEDA>. According to the N-TV report, the "commercial register extracts" for this company "list an address in Kerch, a city in Crimea, which has been occupied by Russia since 2014." One of the alleged owners of this shell company was listed as "Diana B., who, according to the commercial register holds 95 percent of the company's shares" and whose Russian passport is reportedly registered to the same address in Kerch. While N-TV cites reports from Süddeutsche Zeitung claiming that "Diana B." also holds a Ukrainian passport, N-TV also shared findings that this same individual posted photos on social media placing her "in front of the football stadium in Krasnodar, Russia" in 2023. As German CDU political Roderich Kiesewetter wisely questioned in the N-TV report "she wouldn't be able to stay in Russia or move freely if she had acted against the Russian state. After all, millions of dollars in assets were destroyed there."[164]

- A team of investigative journalists

Port of Nexø on the island of Bornholm, Denmark. (September 2024) / CREDIT: B. L. Schmitt

from German broadcaster ARD attempted to recreate the alleged <ANDROMEDA> mission by renting the actual <ANDROMEDA> sailboat (the same vessel found in the aforementioned Hohe Düne marina by Schmitt) to sail to the Nord Stream blast sites to try to dive to the seabed. According to an English language CBC report written by one of the ARD journalists that took part, the skipper engaged by the ARD team claimed that <ANDROMEDA> was "one of the worst boats I've ever sailed with." Furthermore, the ARD-hired skipper warned of risks of diving from such a vessel given the state of the swim platform in which "the platform moves up and down, punching into the sea. A diver trying to get back on the boat could be slammed on the head by the platform, causing serious injury." Given this, the article claims that the ARD team deemed that the "risk was too high" to carry out such a demonstration, resulting instead in the ARD team chartering "a professional diving vessel with a crew that usually recovers Second World War explosives from the bed of the Baltic Sea." The article goes on to explain that the dives were difficult, yet possible from such a platform, but therein lies the issue – the experts consulted in this report have not claimed that the concept of diving to the Baltic seabed itself is not feasible, but rather that proper equipment, provisions, and a suitable diving platform is required for such an operation. Late in the article, the ARD team reported that the technical diver hired for the demonstration trip claimed that "I would use the <ANDROMEDA> for a vacation, but not a sabotage mission."[166]

- A Washington Post report from June 6, 2023 that described U.S. intelligence leaks allegedly illustrating

that the "U.S. had intelligence of detailed Ukrainian plan to attack Nord Stream pipeline" that claimed that initial intelligence suggested that such a team was set to attack the pipeline in June 2022, however that action had been called off. In this Washington Post report, the CIA is depicted as taking the intelligence seriously enough to warn European allies of the possible plot, while also harboring its own assessment of the intelligence source itself, in which the Post claims that "the CIA initially questioned the credibility of the information, in part because the source in Ukraine who provided the details had not yet established a track record of producing reliable information, according to officials familiar with the matter. The European service, a trusted U.S. partner, felt that the source was reliable." Despite these reported leaks, the U.S. Government itself has not yet publicly assessed any culpability for the Nord Stream sabotage.[168]

- According to a 2024 report from the Wall Street Journal that claimed the pro-Ukrainian <ANDROMEDA> sailboat mission was culpable for the Nord Stream sabotage, German investigators had ascertained the location of the <ANDROMEDA> during the alleged sabotage operation by identifying the team's "mobile phone numbers and their Iridium satellite phone" and then "analyzed all mobile phone traffic in the areas where the boat was located, trawling thorough thousands of connections to distill the relevant data." Likewise a 2025 report from The New Yorker also made a similar claim about the <ANDROMEDA>'s alleged culpability in the sabotage. Also like the Wall Street Journal report, The New Yorker report claims (as stated as a leading narrative earlier in this case study) that Ukrainian General Zaluzhnyi had informed Ukrainian President Zelensky about the operation, and that Zelensky had called to "cancel the mission." Nevertheless, the New Yorker claimed that a source told them this would have been impossible for Zelensky to do in order to call off for this manner of dark operation, since "when you enter the zone of operations, you activate a regime of total silence" and the article claimed that "a single connection, a ping from a phone to a cell tower, can be enough to give away not only your location but whom you're talking to." Taken as written, both the Wall Street Journal and New Yorker claims result in a logical discordance – that the sailboat's position was established by the crew's cell phone tracking across the Western Baltic Sea, while simultaneously the President of Ukraine would have been unable to call off the operation that wouldn't be able to risk a "single connection, a ping from a phone to a cell tower." (It should be noted that both Zelensky and Zaluzhnyi have strenuously denied involvement in the Nord Stream sabotage incident.)[169,170]

- A March 2025 report from the Danish newspaper Berlinske on the topic of potential German revival of the Nord Stream projects included a statement that suggested that sources in the office of German Chancellor Olaf Scholz made public that some of the alleged Nord Stream saboteurs may have had Ukrainian passports, while downplaying the Russian passport ownership of other suspects. A key section of that report claimed that "The gray areas are well-known and accepted at the highest political level. According to a source with knowledge of the matter, back in

2022, shortly after Russia's invasion of Ukraine, Germany's outgoing Chancellor, Olaf Scholz, is said to have urged German business not to sever ties with Russia. The implication is: You'll need them again soon. The same source points out that it was also from Scholz's people in the chancellor's office that it emerged that some of the actors behind the sabotage of the Nord Stream pipelines had Ukrainian passports. The fact that others suspected of being involved in the operation had Russian passports has not been much of a public concern."[171]

- Moreover, in a Sunday Times article in the United Kingdom, suggestions were published in April 2025 of Royal Navy sources suggesting that the nature of the Nord Stream sabotage "had all the hallmarks of a Kremlin greyzone operation." As the Sunday Times reported: "By the time President Putin sent tanks into Ukraine three years ago, Russia had already begun setting the stage for a much wider conflict with NATO, engaging in surveillance and sabotage of the underwater internet connections, energy pipelines and military cables that are vital to the functioning of western democracies. These activities are at the heart of Putin's "greyzone" doctrine. The blowing up of the Nord Stream gas pipeline in 2022 was the first major incident; Royal Navy insiders maintain that its "military precision" had all the hallmarks of a Kremlin greyzone operation."[172] ■

BOX 17

Bo Elkjaer, investigative reporter, writing for the Danish daily newspaper Dagbladet Information

"Different media have established that the Andromeda yacht left Rostock on September 6, 2022 and returned on September 23. The yacht was sighted in different ports in Germany, Denmark, Sweden and Poland before returning to Rostock. The Greek tanker <MINERVA JULIE> was drifting above the Nord Stream 1 blast zone from September 6 to September 13. The weather conditions were harsh with strong winds and high waves from September 12 to September 18. The yacht was inspected in Poland on September 19. The Russian navy vessels including the SS-750 arrived in the area on September 21.

We know when and where the tanker <MINERVA JULIE> was drifting above the Nord Stream 1 blast zone and we know when the weather conditions in the area would render the diving operations impossible or at least very difficult with up to three meter high waves, we know when the yacht was inspected in Poland and we know when the Russian navy vessels arrived in the area.

This leaves an extremely narrow time frame of more or less 24 hours for the Ukrainian dive team to sail out to the two areas and perform all the different dives down to the pipelines.

On top of this we now know that the yacht was hired by persons, one of which was under investigation for trying to overthrow the Ukrainian government and another who had been on a public Ukrainian list of traitors for years, and who is living freely in Kerch in the Russian occupied Crimea.

In my view we need explanations for these circumstances before it is possible to accept the theory that the attack was performed from the <ANDROMEDA> yacht."

BOX 18

Jessica Berlin, Senior Fellow with the Transatlantic Defense and Security Program at CEPA.

Why have we not seen a more strenuous pushback against these incidents from the German government thus far, especially when many of these activities appear to have taken place on German soil in the past year or so?

"The German government has failed to recognize the severity of the threat Russian sabotage represents to Germany's national security. This is in part due to Germany's weak strategic culture regarding security and foreign policy. The German state lacks strategic planning and operational capacity to rapidly assess and respond to threats, and pressure from the public to develop this capacity is low. Furthermore, these attacks are politically inconvenient for the Scholz government. The SPD has long historical ties to Russia was instrumental in shaping and strengthening German-Russian economic ties since the collapse of the Soviet Union. Scholz personally has also been a longstanding Russian ally within the German political establishment, as well as his political mentor, the former German SPD chancellor and current Russian lobbyist Gerhard Schröder. To respond strongly against Russia's attacks on German energy and critical infrastructure would ultimately highlight numerous German political leaders' past failure to understand the true nature and intentions of the Russian Federation, their complicity in enabling these attacks by enabling increased expansionist Russian aggression over the past twenty years, and their continued failure to protect Germany from Russian threats. Standing up to Russia and decisively defending German long-term national security is not in the political interest of numerous German political and industry decisionmakers, who would prefer a return to 'business as usual' with the Russian state."

Are there concerns about "escalation" likely to be at play here or other geopolitical/geoeconomic concerns?

"Russia is highly likely continue to escalate their attacks on German and other NATO members' critical infrastructure. Having suffered no serious consequences for their acts of sabotage so far, they have, quite simply, no reason to stop. Russia's successful sabotage campaign will also likely encourage other adverserial states, in particular China, to carry out sabotage campaigns of their own."

In your view, what should Germany and other EU/NATO Member States that have experienced these sabotage incidents be doing differently from a policy perspective?

"Germany and other states must deter future acts of sabotage by inflicting serious consequences for any further acts of sabotage. This should include the expansion of and stricter enforcement of sanctions against Russia, travel bans for Russian citizens other than asylum seekers, and liquidation of Russian assets seized in EU/NATO member states and using the resulting funds to finance Ukrainian defense and humanitarian aid."

▲
Public display of Nord Stream 2 pipeline pipe segment in Hanko, Finland. (April 2025) / CREDIT: B. L. Schmitt

Royal Danish Navy Frigate <HDMS TRITON> on patrol as a part of Joint Arctic Command Denmark near the coastline of Greenland. (November 2022) / DESIGN: B. L. Schmitt / PHOTO CREDIT: NATO Flickr

Swedish Naval CB-90 fast assault boats operating on the Norwegian coastline near Tovik, Norway before NATO Exercise Nordic Response 24. (February 2024) / PHOTO CREDIT: NATO Flickr[P11]

RECOMMENDED POLICY ACTIONS

The pace of energy and critical infrastructure sabotage across the European continent has only grown since the 2022 bombings of Nord Stream 1 and Nord Stream 2. If policymakers on both sides of the Atlantic fail to elevate the policy, technological, and defense steps needed to deter physical sabotage threats from the Russian Federation (or any other actor), then there will be significant public degradation in the confidence in authorities to ensure energy security across the Transatlantic community.

Such an outcome will have direct negative impacts on a much wider array of policy areas, including support for European defense and Ukrainian victory, and countering Russian malign influence across the European energy sector.

If insufficient action is taken to deter further energy infrastructure sabotage, we can also expect less public support for renewable energy infrastructure deployment. In the previous section, we highlighted a real-world example of this: following the Nord Stream attack, local farmers on Bornholm began opposing offshore wind power over concerns that new installations might become targets of sabotage.

Moreover, an insufficient response will likely embolden other authoritarian nations around the world, most notably the People's Republic of China, to use similar subsea infrastructure attacks to undermine the national

security of democratic states across East Asia, including in the run up to any possible future military action taken by Beijing against Taiwan. In fact, the ***Underwater Mayhem*** project will review multiple subsea telecommunications cable damage incidents that have taken place since the events covered in this volume in and around the Taiwan Strait. Clearly, the multidisciplinary nature of the energy infrastructure sabotage threat in Europe requires a cross-cutting policy and technological response to enhance deterrence and ensure that broader risks associated with these attacks are mitigated to the greatest extent possible. Based on these findings, we recommend several multidisciplinary policy actions to respond to these sabotage acts against European energy and critical infrastructure:

- **NATO member states should invoke Article 4.**

  NATO Member States who have sustained energy and critical infrastructure sabotage attacks in which an official attribution to Russian government actors or non-Russian actors recruited and paid for by Russia's military intelligence (GRU) or other intelligence services should collectively invoke NATO's Article 4 provision.

  Unlike NATO Article 5, in which direct actions are expected to support a Member State that is victim of a military assault, Article 4 is a consultative mechanism, which states that "the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence, or security of any of the Parties is threatened."

  Enacting NATO's Article 4 provision would serve as a public reminder to the Kremlin that NATO's political leadership is taking steps to counter and deter further Kremlin-backed actions to undermine Alliance support for Ukrainian victory via sabotage attacks against Member States.[92]

- **The European Union should continue to phase out Russian energy imports – and take measures to ensure there cannot be a return to energy "business as usual" with Putin's Russia on energy or critical infrastructure investments.**

  The EU has demonstrated significant policy resolve to phase out Russian energy imports, most notably within the natural gas sector over the past decade, and especially since Russia's full-scale invasion of Ukraine took place in February 2022. These policies should continue and be accelerated. Policy decision making at the EU institutional and member state level should continue to prioritize legislative and regulatory measures to disincentivize actors across the Transatlantic community that would favor a rapid return to "business as usual" with Putin's Kremlin on energy imports to succeed in doing so. Among the most urgent policy priorities to mitigate any chance of reintroducing Russian energy dependence and associated national security risks, is for the U.S. and EU to pass permanent joint sanctions measures to ensure that Russian natural gas pipelines like Nord Stream 1 and Nord Stream 2 aren't able to be revived.

  Furthermore, as a part of deterrence against potential future offshore energy or critical infrastructure sabotage, the U.S. and EU should work together to introduce sanctions measures on vessels and entities that have been shown to have deliberately damaged subsea energy and critical infrastructure across Europe since

The authors recommending energy policies.. (TOP) Prof. Michał Kurtyka celebrating the close of COP24 after serving as COP President in Katowice, Poland. (2018) (MIDDLE) Prof. Alan Riley lecturing on European energy law in Oslo, Norway. (2018) (BOTTOM) Dr. Benjamin L. Schmitt testifies before the joint U.S. House and Senate Commission on Security and Cooperation in Europe (U.S. Helsinki Commission) on Capitol Hill, Washington, D.C. (2024) / PHOTO CREDITS: (TOP) UNFCCC Flickr, (MIDDLE) A. Riley, (BOTTOM) U.S. Helsinki Commission Website on September 2024 Hearing: "Russia's Shadow War on NATO."[P12]

2022, regardless of vessel flag state.

- **Russian disinformation campaigns associated with suspected European energy and critical infrastructure attacks should be countered by consistent and transparent strategic communications strategies by European authorities.**

This report has shown that the Russian Federation has coupled disinformation strategies to coincide with suspected energy and critical infrastructure sabotage events across Europe in recent years. Early, consistent, and transparent statements and briefings by strategic communications authorities across European states is vital to counter these disinformation trends. Furthermore, public attribution can help inspire societal confidence in government responses to these incidents, when possible. As Finnish investigative journalist Pekka Virkki explains, not doing so encumbers risk since, "there remains a big concern across the Central and Eastern European region that many hybrid threat incidents likely involving Russia are going unresponded to. Attribution is very important to counter sabotage events and hybrid threats, and so far we are not doing enough across the West to contain these threats from the Kremlin."

- **More effort needs to be placed on creating cross-competency coordination on European energy and critical infrastructure protection.**

Oskar Frånberg, Associate Professor of Marine Systems Engineering at the Blekinge Institute of Technology in Karlskrona, Sweden emphasized that "given the current subsea threat environment across Northern Europe, it is more vital than ever to create a cross-competency forum to discuss

NATO special forces divers participate in exercise BOLD MACHINA 24 focused on protecting critical subsea infrastructure from hybrid threats near La Spezia, Italy (November 2024) / PHOTO CREDIT: NATO Flickr[P13]

maritime infrastructure protection issues from all relevant stakeholders."

Since the Svalbard cable cut and Nord Stream incidents took place, NATO has begun to respond to this call, through the creation of several bodies, including the Critical Undersea Infrastructure Coordination Cell based at NATO Headquarters in February 2023 and has stood up related operational competences and exercises. However, further fusion of commercial, military, law enforcement, academic, and investigative resources to build up multidisciplinary competencies for the monitoring, protection, and response aspects of critical offshore infrastructure protection is essential.

Moreover, Baltic Sea littoral states should continue to review and, when necessary, issue updated legal guidance for military, coast guard, and law enforcement first responders on regulatory norms for competencies and response techniques to these incidents going forward. Such legal guidance and any legislative or normative updates that are needed should be completed at the national level and coordinated closely among bordering nations.[93,94]

- **Transatlantic political and commercial leaders should take steps that support the wider development and coordination of OSINT monitoring technology hardware and data analysis tools.**

Open-source intelligence data sources such as commercial AIS and satellite imagery can offer considerable insights regarding the nature of any of these offshore energy and critical infrastructure attacks. Indeed, this study would have been incomplete without these data sets. However, these systems are not a standalone panacea to fully characterize any given case and should be considered as vital supplemental systems to bolster existing government clandestine intelligence tools. A key advantage to OSINT and commercial-based AIS and geospatial imaging systems is that they are by their very nature unclassified and can increase the speed at which U.S. and EU security officials can provide high-resolution satellite imagery or detailed AIS assessments of suspected sabotage incidents for use in strategic communications efforts. Nevertheless, commercial multiwavelength satellite platforms often focus on the publication of data sets from onshore areas, leaving critical offshore environments often sparsely covered in commercial satellite databases.

While coverage of the entire global

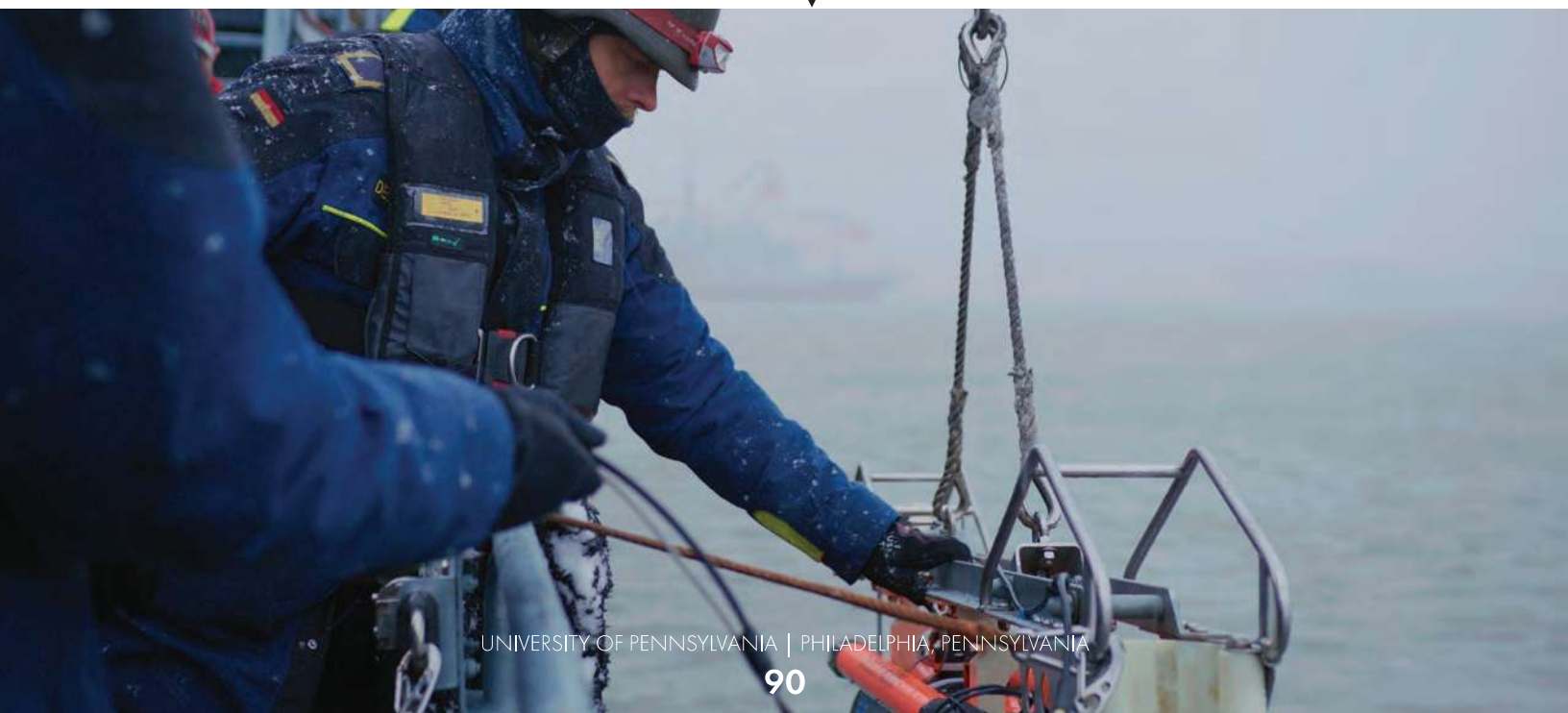
ocean system may present cost and data constraints for commercial satellite providers (after all, roughly 70% of the Earth's surface is covered in water), offshore energy and critical infrastructure operators should increase their contact with commercial satellite providers to ensure that at the very least, coverage of maritime-based surface and subsea infrastructure sites is prioritized in commercial geospatial data sets to aid in monitoring and potential attribution. Such cross-industrial contact will also demonstrate to commercial satellite firms that there is indeed a market for at least certain regular coverage of select maritime environments.

- **Climate leaders need to more fully integrate national security risks associated with energy security and critical infrastructure protection into policy analysis and prescriptions.**

Ensuring a just energy transition that adequately responds to the current climate crisis is among the forefront of analysis areas focused on by climate policymakers, academics, and thought leaders today.

This study has emphasized that any energy intermittency or security of supply issues related to geopolitically motivated cutoffs or physical sabotage of energy infrastructure can result in loss of support by electorates worried about the vulnerability of energy systems to attack. If inadequately addressed, climate leaders may lose support for the deployment of the very onshore and offshore renewable energy installations that will be needed to ensure a rapid and just energy transition as soon as possible.[95] Enacting these measures will not only significantly push back on the current scourge of Russia-linked energy and critical infrastructure sabotage across NATO Member States, but will also support the future resiliency of a free Ukraine. Such measures will also make it abundantly clear to those that advocate otherwise – to the detriment of European security – that there can never be a "return to business as usual" with Putin's Kremlin on energy or critical infrastructure investment. ■

German Naval team deploying the unmanned underwater vehicle SEAFOX-I into the Baltic Sea during Exercise Freezing Winds 24 focused on the protection of subsea energy and critical infrastructure in the Baltic Sea. (December 2024) / PHOTO CREDIT: NATO Flickr[P14]



Facade of Bornholms Museum on the Island of Bornholm, Denmark, with Special Exhibition banner "RUSSERNE KOMMER!" (Translation: "The Russians are Coming!) (August 2023) / CREDIT: B. L. Schmitt

ACKNOWLEDGEMENTS

The authors would like to thank the leadership of the University of Pennsylvania's Kleinman Center for Energy Policy for providing the research funding to undertake this project, and the work of a stellar editorial and publications team—especially Lindsey Samahon and Mollie Simon—without which this project would not have been possible. The authors would also like to extend a special thanks to the University of Pennsylvania's Perry World House for supporting the research project programming and commercial satellite data license that were integral to the successful completion of this work.

The authors wish to thank University of Pennsylvania student research assistants Annibelle Paradise, Amelia Pilot, Liam LaBarge, Rachel Bina, and Axel D'Amelio for their help in tracking and compiling a list of suspected hybrid activities, including involving suspected European energy and critical infrastructure sabotage between 2022 and 2024, an excerpt of which is provided in **[APPENDIX A]**. The authors would also like to thank personnel in the University of Pennsylvania Experimental Cosmology Laboratory for their moral and analytical support, most notably Prof. Mark J. Devlin and Saianeesh K. Haridas.

Schmitt would also like to wish a special thanks to Dr. Jakob Seerup, curator of the Bornholms Museum in Denmark, for invaluable logistical support and fruitful policy and history discussions during the Schmitt's three visits to the Danish Island of Bornholm during this research study.

Schmitt would also like to wish a special thanks to the Harvard-Ukrainian Research Institute, especially both Prof. Serhii Plokhii and Dr. Emily Channel-Justice for their support of the years of preliminary research conducted while at Harvard University that served as the basis from which this project was launched, and to the Center for European Policy Analysis (CEPA) and the Atlantic Council, who supported both Chatham House rules and public launch events for this report in Washington, D.C. in Spring 2025. ■

View of the Taiwan Strait from the Tamsui District of Taipei, Taiwan. People's Republic of China flagged container vessels visible on horizon. (June 2024) / CREDIT: B. L. Schmitt

UNDERWATER MAYHEM WILL RETURN

Looking ahead to Volume 02

The next volume in this series will primarily focus on assessing the current state-of-play regarding major policy actions that have been taken by democracies in response to the ongoing trend of suspected sabotage activities against energy and critical infrastructure across the European continent and East Asia.

Underwater Mayhem: Volume 02 will highlight the national and multinational responses taken, including new policy and operational structures that were stood up within NATO and at the EU member state level. Volume 02 will also highlight some of the leading technology options to support enhanced monitoring and OSINT data analysis related to these incidents, including AIS and multi-wavelength commercial satellite data, and how artificial intelligence can provide enhanced infrastructure surveillance and vessel attribution capabilities – all of which is vital to provide policymakers with the best possible assessments for pragmatic decision making going forward.

The case studies in ***Underwater Mayhem: Volume 02*** will continue to consider further subsea cable cut incidents in the Baltic Sea region, as well as emerging subsea infrastructure damage incidents in the Taiwan Strait and Canada's Atlantic Provinces.

PHOTO: (Below) Isbjørn - Polar Bear (shot 23 March 1992 near Minkinfjellet) from lobby of Radisson Blu Polar Hotel Spitsbergen, Longyearbyen, Svalbard, Norway (Opposite) Polar Bear warning sign near Svalbard Airport, Longyearbyen, Svalbard, Norway (September 2023)
CREDIT: B. L. Schmitt

AUTHORS

Dr. Benjamin L. Schmitt

Dr. Benjamin L. Schmitt is a senior fellow at the University of Pennsylvania, where he holds a joint academic appointment between the Department of Physics and Astronomy and the Kleinman Center for Energy Policy. He is also a senior fellow at Penn's Perry World House. At Penn, Schmitt focuses on the project development and field deployment of the Simons Observatory, a new set of experimental cosmology telescopes and energy support infrastructure under construction at a high-altitude site in the Atacama Desert of Northern Chile. In his joint role at Penn, he also pursues research and teaching with the Kleinman Center related to European energy security, critical infrastructure protection, export controls policies, and modern sanctions regimes. At Perry World house, Schmitt focuses on national security analysis focused on the transatlantic community and the Indo-Pacific, as well as emerging space security challenges. Dr. Schmitt completed his postdoctoral work at the Harvard-Smithsonian Center for Astrophysics where he supported the technical design, deployment, and project management of instrumentation and infrastructure for next-generation experimental cosmology telescopes at the South Pole. For this work, he traveled to the Amundsen-Scott South Pole Station in 2020 and received the U.S. Antarctica Service Medal. Schmitt remains an affiliate of the Harvard-Smithsonian Center for Astrophysics, and an associate of the Harvard-Ukrainian Research Institute. Dr. Schmitt is a term member of the Council on Foreign Relations, a co-founder of the Duke University Space Diplomacy Lab, and is also a senior fellow for Democratic Resilience at the Center for European Policy Analysis in Washington, D.C. He previously served as European energy security advisor at the U.S. Department of State and received his Ph.D. in Experimental Physics from the University of Pennsylvania under the advisement of Professor Mark J. Devlin.

Prof. Michał Kurtyka

Professor Michał Kurtyka is Visiting Professor at the College of Europe in Natolin and Akademia Leona Koźmińskiego in Warsaw. He also serves as Distinguished Fellow with the Atlantic Council Global Energy Center. Kurtyka served as the first minister of Poland's Ministry of Climate, responsible with energy and climate, which later expanded to become the Ministry of Climate and Environment. During his tenure starting in 2019, the Polish government adopted its 2040 Energy Policy, opening a new era for the Polish energy transition. He modernized the Polish Nuclear Strategy, and oversaw record increases in registration for the development of renewable energy sources, reaching thousands of megawatts of installed capacity in photovoltaics and one million prosumers. In 2018 Kurtyka was appointed as Government Plenipotentiary for the Presidency of COP24—the United Nations Climate Change Conference of the Parties in Poland. From July 2018, he also held the position of Secretary of State in the Ministry of Environment. In December 2018, he became the COP24 President, which ended with the effective implementation of the Paris Agreement. In 2019 he assumed the role of Ministerial Chair of the International Energy Agency and in 2021 he was designed as Ministerial Chairman of the United Nations of Food and Agriculture. Kurtyka is a graduate of the École Polytechnique (X94) and earned a scholarship in quantum optics at the National Institute of Standards and Technology (NIST), where he worked under the leadership of Nobel Laureate in Physics William D. Phillips. He defended his PhD at the University of Warsaw on restructuring of energy utilities.

Prof. Alan Riley

Professor Alan Riley is Visiting Professor at the College of Europe, Natolin, Poland, and a Non-Resident Senior Fellow of the Atlantic Council. Recently he has been an EU advisor on energy security and a member of the Advisory Committee (the judicial panel) of the Energy Community. He has written extensively on European energy security, EU and competition law issues and was previously Professor of International Commercial Law at City Law School, City St George's, University of London. He holds a PhD from the Europa institute, Faculty of Law, Edinburgh, and qualified as a Solicitor of the Supreme Court of England and Wales.

APPENDIX A

Examples of Suspected Hybrid Activities Across NATO Territory since 2022

As a component of ***Underwater Mayhem: Volume 01***, our research team has continuously monitored and catalogued a repository of suspected "hybrid" threat activities, cyberattacks, vandalism, as well as damage incidents involving potential sabotage against energy and critical infrastrucure across NATO member states from early 2022 to the present. An excerpt of this larger repository is included in this Appendix.

Date	Location	Possible Hybrid Activity	Media Report
03-FEB-2022	The Netherland and Germany (multiple locations)	Cyberattacks against 17 oil loading terminal facilities in The Netherlands and Germany.	https://www.spglobal.com/commodity-insights/en/news-research/latest-news/crude-oil/020322-cyberattack-causes-chaos-at-key-european-oil-terminals
11-APR-2022	Bremen, Germany	Assessed professional grade cyberattack against wind turbine data monitoring systems.	https://www.deutsche-windtechnik.com/en/news/news/details/cyber-attack-on-deutsche-windtechnik/
31-JUL-2022	Karnobat, Bulgaria	Explosion at an ammunition depot of the Bulgarian arms manufacturer EMKO.	https://www.svobodnaevropa.bg/a/31967635.html
20-APR-2023	U.K. Offshore Wind Farms, North Sea	Report of suspected Russian espionage vessel <ADMIRAL VLADIMIRSKY> monitoring offshore energy infrastructure in the waters of the United Kingdom.	https://news.sky.com/story/russian-ship-spying-around-wind-farms-off-uk-coast-in-possible-sabotage-plot-12861217
26-JUN-2023	Karnobat, Bulgaria	Explosion at an ammunition depot of the Bulgarian arms manufacturer EMKO (a second incident, this time after the firm announced it would supply munitions to Ukraine)	https://www.euractiv.com/section/politics/news/explosions-at-bulgarian-arms-factory-set-to-export-to-ukraine/
28-AUG-2023	Warsaw, Poland	"Hacking attack" against Poland's rail network that resulted in the "emergency stoppage of trains in Northwestern Poland."	https://www.reuters.com/world/europe/poland-investigates-hacking-attack-state-railway-network-2023-08-26/
08-DEC-2023	Tallinn, Estonia	Attack damaging the windows of the personal automobile of Estonian Interior Minister Lauri Läänemets	https://www.delfi.ee/artikkel/120253842/fotod-siseminister-lauri-laanemetsa-isikliku-auto-aknad-loodi-oosel-puruks-politsei-alustas-kriminaalmenetlust
25/26-DEC-2024	Poland, Lithuania, Sweden	Widespread jamming incident against GPS signals.	https://www.gpsworld.com/from-russia-with-love-for-christmas-jamming-baltic-gps/
05-JAN-2024	Hetlingen, Germany	Damage to natural gas pipeline under construction to link the Brunsbuettel LNG terminal to the German grid via the intentional drilling of holes along the pipeline.	https://www.ndr.de/nachrichten/schleswig-holstein/Loecher-in-LNG-Pipeline-Brunsbuettel-Bundesanwaltschaft-ermittelt,lng918.html
19-JAN-2024	Džūkste Parish, Latvia	Vandalism against a Latvian war memorial site.	https://eng.lsm.lv/article/society/crime/20.02.2024-russian-estonian-arrested-over-vandalism-of-memorial-in-latvia.a543655/
31-JAN-2024	Sinimaed, Estonia	Vandalism against Estonian World War II memorial site.	https://news.postimees.ee/7954882/estonia-s-iss-suspects-orders-for-memorial-vandalism-came-from-russia
02-MAR-2024	Courlon-sur-Yonne, France	Russan hacking team shown to have launched a cyberattack against a mill, while claiming they were targeting a more prominent dam installation.	https://www.lemonde.fr/en/pixels/article/2024/04/17/how-sandworm-russia-s-elite-hackers-attacked-a-small-mill-instead-of-dam-they-targetted_6668731_13.html#
20-MAR-2024	East London, United Kingdom	Arson attack against "Ukraine-linked" commercial storage facilities.	https://www.cbsnews.com/news/uk-russia-arson-attack-plot-london-ukraine-man-charged-link-wagner-group/
09-MAY-2024	Vilnius, Lithuania	Arson attack against an IKEA furniture store.	https://madeinvilnius.lt/en/news/Lithuanian-news/there-was-a-fire-in-the-ikea-shopping-center/
04-MAY-2024	Berlin, Germany	Reports of suspected "Russian saboteurs" conducting an arson attack against metals factory owned by German arms manufacturer (and Ukraine ammunition supplier) Diehl.	https://www.politico.eu/article/russia-berlin-fire-diehl-behind-arson-attack-on-factory/
12-MAY-2024	Warsaw, Poland	Arson attack against a large-scale commercial shopping center.	https://kyivindependent.com/lithuania-suspects-russias-military-intelligence-behind-arson-attacks/
07-JUN-2024	Prague, Czech Republic	Attempted arson attack against "public transport depot."	https://www.bbc.com/news/articles/cqeev0d6lp5o
JUL-2024	United Kingdom and Germany	Incendiary devices catch fire at air cargo logistics hubs in the U.K. and Germany and suspected to be part of a Russian plot to move such devices to the United States via cargo planes.	https://www.bbc.com/news/articles/c07912lxx33o https://www.wsj.com/world/russia-plot-us-planes-incendiary-devices-de3b8c0a
09-SEP-2024	Stockholm, Sweden	Unauthorized drone flights result in the closure of the Stockholm Arlanda Airport.	https://www.aftonbladet.se/nyheter/a/B0G1rg/arlanda-dronare-stangde-flygplatsen
17-SEP-2024	Joensuu, Finland	Fiber optic telecommunications cables and connections to fiber equipment installations cut.	https://www.is.fi/kotimaa/art-2000010702478.html

APPENDIX B

Supporting Primary Source Documents and Reference Materials

This Appendix contains two documents..

The first document is a publicly-released document by the United Nations entitled: ***"Letter dated 10 July 2023 from the representatives of Denmark, Germany, and Sweden to the United Nations addressed to the President of the Security Council"*** and provides three separate updates from the three investigations that were ongoing at the time from Denmark, Germany, and Sweden, offering differing levels of detail and description of the status of the respective investigations. It is notable that rather than a single joint statement, three separate summaries from each national authority was included and furthermore, that only the German letter refers to the potential lead of a sailboat being the potential mode of transport for the attacks against the Nord Stream 1 and Nord Stream 2 pipelines in September 2022.[96]

The second document is a single-page excerpt from an unclassified U.S. National Intelligence Council, Intelligence Community Assessment dated 10 March 2021 (ICA 2020-00078D) (labeled "DECLASSIFIED by DNI Haines on 15 March 2021" that fully describes the metrics for estimative language and levels of confidence defined in this Intelligence Community Assessment document, and which has been referenced throughout this ***Underwater Mayhem*** report.[24] (https://www.intelligence.gov/assets/documents/702%20Documents/declassified/ICA-declass-16MAR21.pdf)

United Nations S/2023/517

Security Council

Distr.: General
10 July 2023

Original: English

Letter dated 10 July 2023 from the representatives of Denmark, Germany and Sweden to the United Nations addressed to the President of the Security Council

We have the honour to transmit to you information regarding the ongoing investigations into the explosions on the Nord Stream 1 and 2 pipelines (see annex).

We would be grateful if the present letter and its annex could be circulated as a document of the Security Council in connection with the briefing on Tuesday, 11 July 2023, under the item entitled "Threats to international peace and security".

We would also like to recall our letter and annex dated 21 February 2023 on the matter.

(*Signed*) Marie-Louise Koch **Wegter**
Ambassador
Chargé d'affaires a.i.
Deputy Permanent Representative of Denmark
to the United Nations

(*Signed*) Antje **Leendertse**
Ambassador
Permanent Representative of Germany
to the United Nations

(*Signed*) Anna Karin **Enström**
Ambassador
Permanent Representative of Sweden
to the United Nations

23-13475 (E) 130723

Annex to the letter dated 10 July 2023 from the representatives of Denmark, Germany and Sweden to the United Nations addressed to the President of the Security Council

Denmark, Germany and Sweden would like to provide the following information regarding their respective national investigations of the sabotage against the Nord Stream 1 and 2 pipelines on 26 September 2022, in continuation of the letter dated 21 February 2023 from the Permanent Representatives of Denmark, Germany and Sweden to the United Nations addressed to the President of the Security Council and the letter dated 29 September 2022 from the Permanent Representatives of Denmark and Sweden to the United Nations addressed to the President of the Security Council.

The respective national authorities of Denmark, Germany and Sweden are committed to investigating the sabotage comprehensively and continuing their separate investigations. The investigations are conducted in line with fundamental principles of the rule of law, including independence from political interference.

None of the investigations has been concluded, and at this point, it is still not possible to say when they will be concluded. The nature of the acts of sabotage is unprecedented, and the investigations are complex.

Further information concerning the status of the separate, national investigations is provided below. Given national differences in the criminal procedural rules as well as in the characteristics of the investigations, the amount and nature of information that can be shared at this point differ. The authorities of Denmark, Germany and Sweden have been in dialogue regarding the technical aspects of their investigations, and the dialogue will continue to the relevant extent.

There are no obstacles to visiting the sites of the Nord Stream pipeline explosions. While some activities require permits from the relevant authorities, all vessels enjoy freedom of navigation at the sites of the explosions in the respective exclusive economic zones of Denmark and Sweden, in accordance with the United Nations Convention on the Law of the Sea. We recall that the operators of the pipelines, Nord Stream AG and Nord Stream 2 AG, have carried out their own surveys in relation to the damage to the pipelines.

The authorities of the Russian Federation have been informed about the ongoing investigations.

The following information can be provided with regards to the separate, national investigations:

Denmark

In Denmark, the Copenhagen Police and the Danish Security and Intelligence Service established a joint investigation group in October 2022 to handle the investigation regarding the explosions on the Nord Stream 1 and 2 pipelines in September 2022.

Prior to the establishment of the joint investigation group, the Copenhagen Police, with assistance from the Danish Defence and in collaboration with, among others, the Danish Security and Intelligence Service, carried out a number of preliminary investigations that confirmed that there had been extensive damage to Nord Stream 1 and 2 in the Danish exclusive economic zone, and that the damage had been caused by powerful explosions.

The Danish authorities are working closely with relevant foreign authorities to the relevant extent in connection with the investigation of the gas leaks. There is an

ongoing dialogue between Denmark, Sweden and Germany regarding the technical aspects of the investigation.

The investigations conducted by the Danish authorities have not been concluded, and at this point, it is still not possible to say when they will be concluded.

The operators of the pipelines, Nord Stream AG and Nord Stream 2 AG, have been authorized to carry out surveys in relation to the damage of the pipelines.

On 28 March 2023, the Danish Energy Agency announced that an object near the Nord Stream 2 pipeline in the Danish exclusive economic zone had been salvaged. The salvage of the object was conducted by Danish Defence, and representatives from Nord Stream 2 AG took part in the salvage. Examinations of the object indicated that the object was a visual marker (*røgbøje*) that did not pose a safety risk.

Germany

In Germany, the Public Prosecutor General of the Federal Court of Justice is in charge of the investigations; the Federal Criminal Police Office and the Federal Police have been tasked with carrying out the police investigations.

According to the results of the investigations carried out in the Swedish and Danish exclusive economic zones in cooperation with different German institutions and the competent authorities of Denmark and Sweden, the criminal act is presumed to have been carried out with the use of explosives.

During the investigations on site, a huge amount of data was collected. In addition, water and soil samples were taken in the vicinity of the leak locations. Metal fragments were also collected. This wealth of information must be comprehensively evaluated in order to arrive at a plausible sequence of how the attack was technically carried out. For the findings to be irrefutable, precise and thorough scientific work must be conducted, and this necessarily includes investigative simulations.

In connection with the suspicious charter of a sailing yacht, the investigations found out that the boat had been chartered in the name of a person who had used documents provided in order to hide the identity of the real charterer. Whether this person was in fact subsequently on board has not been established and is the subject of continuing investigations.

The boat's precise course has not been definitively clarified and is the subject of continuing investigations. It is suspected that the boat in question may have been used to transport the explosives that exploded at the Nord Stream 1 and Nord Stream 2 pipelines in the Baltic Sea on 26 September 2022. Traces of subsea explosives were found in the samples taken from the boat during the investigation. According to expert assessments, it is possible that trained divers could have attached explosives at the points where damage occurred to the Nord Stream 1 and Nord Stream 2 gas pipelines, which are laid on the seabed at a depth of approximately 70 to 80 metres.

At this point it is not possible to reliably establish the identity of the perpetrators and their motives, particularly regarding the question of whether the incident was steered by a State or State actor. All information to clarify the matter will be pursued during the continuing investigations.

Sweden

As stated in the letter to the Security Council of 21 February 2023, the Swedish investigation into the Nord Stream events is being conducted by the Swedish Security Service and is headed by a National Security Unit prosecutor. This is an ongoing, independent criminal investigation subject to confidentiality. At this stage, the

following information can be shared with the Security Council based on information from the Swedish investigation:

In September 2022, the Swedish police opened a case regarding the incident at Nord Stream. The investigation is conducted by the Swedish Security Service under the management of the Senior Public Prosecutor Mats Ljungqvist at the National Security Unit at the Swedish Prosecution Authority. Previously, the investigation was able to confirm that this is a case concerning gross sabotage.

The Prosecutor has stated that this crime scene investigation found that there had been detonations at Nord Stream 1 and 2 in the Swedish economic zone. The detonations had caused extensive damage to the gas pipelines, which strengthened the suspicion of gross sabotage.

Later on, the Prosecutor decided on supplementary crime scene investigations in the Baltic Sea, within the Swedish economic zone. Together with the Swedish Security Service, the Prosecutor also requested help from the Swedish Armed Forces to carry out the supplementary investigations. The Swedish Armed Forces were asked to assist, since they were considered to have the right resources and expertise for the task. Following the request, the Swedish Armed Forces assisted the investigation.

During the crime scene investigations carried out in the Baltic Sea, the area was carefully documented and extensive seizures were made. Analyses have revealed explosive residue on several of the foreign objects that have been found. All seized objects and materials are being examined and analysed carefully. The investigation is still carrying out a number of concrete investigative measures. The authorities involved in the investigation have a well-functioning cooperation and are working with joint forces. However, the investigation regarding Nord Stream is very complex and extensive. It concerns a crime where the circumstances are difficult to investigate, since the detonations took place 80 metres under the water on the ocean floor. The ongoing investigation will show whether anyone can be suspected of, and later prosecuted for, this crime.

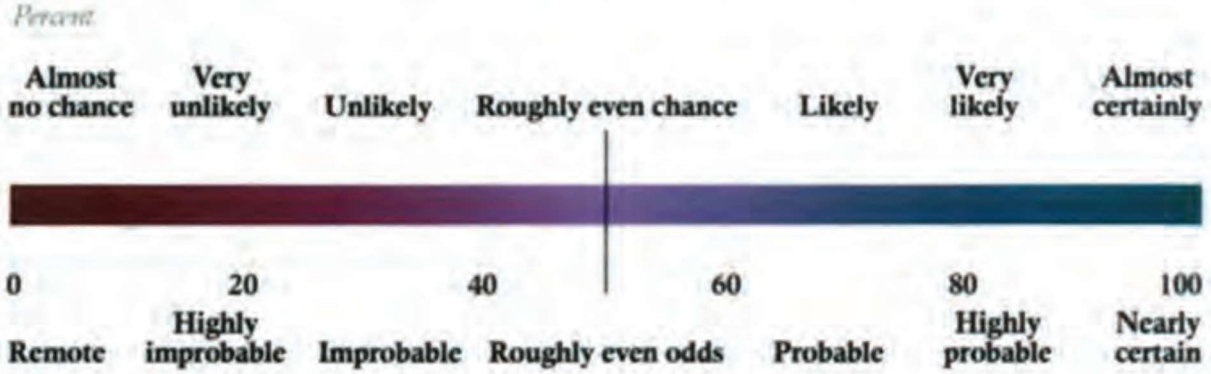
Due to the confidentiality of the investigation, the Swedish Prosecution Authority cannot provide further details regarding the investigation at this point.

Estimative Language

Estimative language consists of two elements: judgment about the likelihood of developments or events occurring and levels of confidence in the sources and analytic reasoning supporting the judgments. Judgments are not intended to imply that we have proof that shows something to be a fact. Assessments are based on collected information, which is often incomplete or fragmentary, as well as logic, argumentation ,and precedents.

Judgments of Likelihood

The chart below approximates how judgments of likelihood correlate with percentages. Unless otherwise stated, the Intelligence Community's judgments are not derived via statistical analysis. Phrases such as "we judge" and "we assess"—and terms such as "probably" and "likely"—convey analytical assessments.



Confidence in our Judgments

Confidence levels provide assessments of timeliness, consistency, and extent of intelligence and open source reporting that supports judgements. They also take into account the analytic argumentation, the depth of relevant expertise, the degree to which assumptions underlie analysis, and the scope of information gaps.

We ascribe high, moderate, or low confidence to assessments:

- **High confidence** generally indicates that judgments are based on sound analytic argumentation and high-quality consistent reporting from multiple sources, including clandestinely obtained documents, clandestine and open source reporting, and in-depth expertise; it also indicates that we have few intelligence gaps, have few assumptions underlying the analytic line, have found potential for deception to be low, and have examined long-standing analytic judgements held by the IC and considered alternatives. For most intelligence topics, it will not be appropriate to claim high confidence for judgements that forecast out a number of years. High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong even though we have a higher degree of certainty that they are accurate.

- **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. There may, for example, be information that cuts in a different direction. We have in-depth expertise on the topic, but we may acknowledge assumptions that underlie our analysis and some information gaps; there may be minor analytic differences within the IC, as well as moderate potential for deception.

- **Low confidence** generally means that the information's credibility and/or plausibility is uncertain; that the inforation is fragmented, dated, or poorly corroborated; or that reliability of the sources is questionable. There may be analytic differences within the IC, several significant information gaps,high potential for deception or numerous assumptions that must be made to draw analytic conclusions. In the case of low confidence, we are forced to use current data to project out in time, making a higher level of confidence impossible.

APPENDIX C

Select Baltic Sea Maritime SitRep Report Open-Source AIS Data Maps Related to Nord Stream

This Appendix provides slect Baltic Sea maritime Situation Report (SitRep) open-source AIS data maps related to the development of Nord Stream 2 pipeline between 2020 and 2021 motivated by tracking potentially sanctionable activities by the Nord Stream 2 construction fleet assembled by the Russian Federation following the imposition of U.S. sanctions in late-2019, and also the maritime forensic response to the Nord Stream 1 and Nord Stream 2 sabotage incidents after they occurred in late September 2022. All of the select maps in this section are based on open-source AIS data from MarineTraffic, with base map public data sources indicated on each page.

Nord Stream 2: Deployment and Possible Support-Related Vessel Status

[Data from MarineTraffic.com, GoogleEarth, Bloomberg/Planet Labs as of: 13 May 2020 – 19:00 EDT (unless otherwise noted)]

Update: Published by Bloomberg on 13 May 2020, Planet Labs 10 May 2020 image shows Nord Stream 2 pipe segments moved to pier adjacent to Russian-flagged pipelayer *Fortuna*

[1] Name: ***Akademik Cherskiy***
IMO: 8770261
Flag: Russia
Owner: Gazprom Flot (Russia)
Vessel Type: Pipelayer (deep water S-Lay capable)
Dynamic Positioning?: Yes (DP3)

[2] Name: ***Fortuna***
IMO: 8674156
Flag: Russia
Owner: MRTS (Russia)
Vessel Type: Pipelayer (deep water S-Lay capable to 200 meters)
Dynamic Positioning?: No

[3] Name: ***Boka Constructor***
MMSI: 211725500
Flag: Germany
Owner: Boskalis (Netherlands)
Vessel Type: Dredging and Seabed Stabilization
Dynamic Positioning?: Yes (DP1)

[4] Name: ***ISA***
IMO: 9688879
Flag: Netherlands
Owner: ISA Towage BV (Netherlands)
Vessel Type: Support Tug and Work Boat Platform

[5] Name: ***Shoalbuster Barney***
IMO: 9740938
Flag: Netherlands
Owner: Herman Sr. BV (Netherlands)
Vessel Type: Support Tug and Work Boat Platform

Nord Stream 2: Deployment and Possible Support-Related Vessel Status

[Data from MarineTraffic.com and GoogleEarth: 28 May 2020 – 13:00 EDT (unless otherwise noted)]

Update: Russian-flagged pipelaying vessel *Akademik Cherskiy* moved to an offshore anchorage between 04:00-06:00 UTC (28 May 2020). Russian-flagged pipelayer *Fortuna* moved into dock position previously occupied by *Akademik Cherskiy* in Port of Mukran. Offshore survey ship *Stril Explorer* continues possible seabed monitoring survey passes.

[1] Name: ***Akademik Cherskiy***
IMO: 8770261
Flag: Russia
Owner: Gazprom Flot (Russia)
Vessel Type: Pipelayer (deep water S-Lay capable)
Dynamic Positioning?: Yes (DP3)

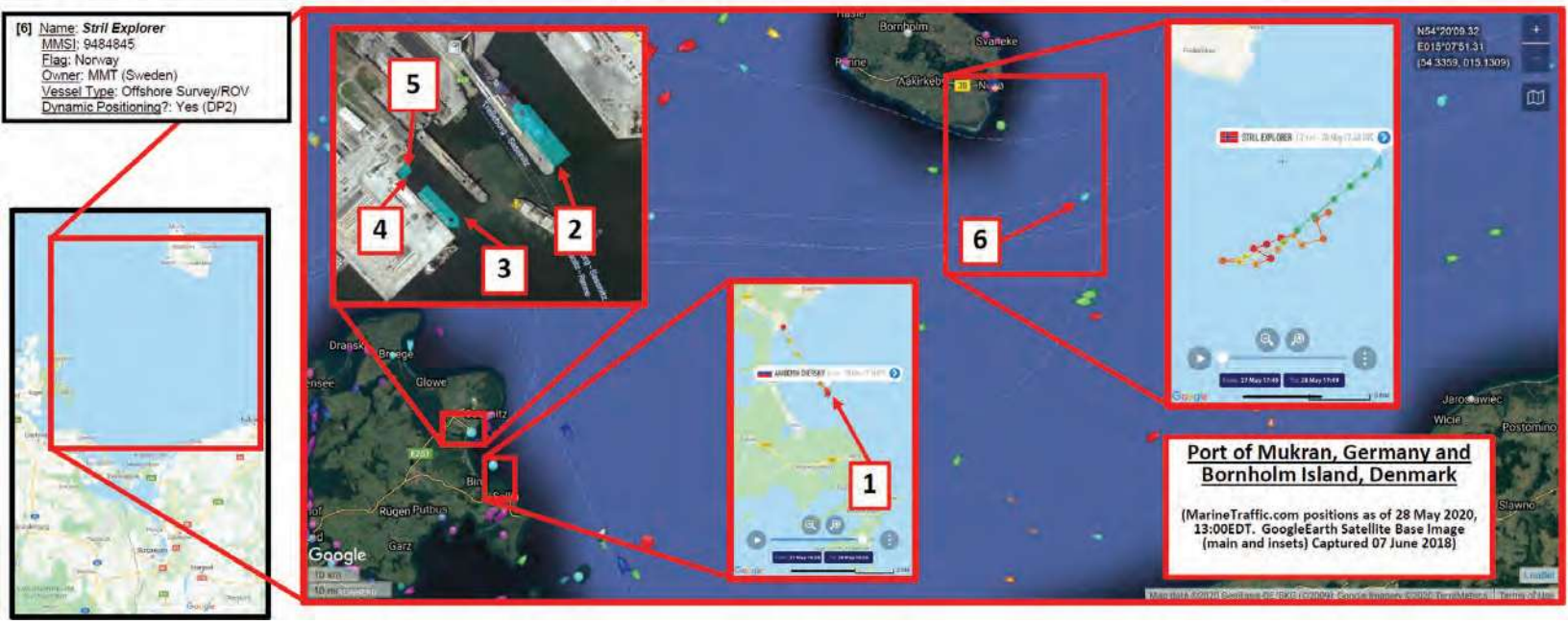
[2] Name: ***Fortuna***
IMO: 8674156
Flag: Russia
Owner: MRTS (Russia)
Vessel Type: Pipelayer (deep water S-Lay capable to 200 meters)
Dynamic Positioning?: No

[3] Name: ***Boka Constructor***
MMSI: 211725500
Flag: Germany
Owner: Boskalis (Netherlands)
Vessel Type: Dredging and Seabed Stabilization
Dynamic Positioning?: Yes (DP1)

[4] Name: ***ISA***
IMO: 9688879
Flag: Netherlands
Owner: ISA Towage BV (Netherlands)
Vessel Type: Support Tug and Work Boat Platform

[5] Name: ***Shoalbuster Barney***
IMO: 9740938
Flag: Netherlands
Owner: Herman Sr. BV (Netherlands)
Vessel Type: Support Tug and Work Boat Platform

[6] Name: ***Stril Explorer***
MMSI: 9484845
Flag: Norway
Owner: MMT (Sweden)
Vessel Type: Offshore Survey/ROV
Dynamic Positioning?: Yes (DP2)



Possible Nord Stream 2 Deployment or Support-Related Vessel Status

[Data from MarineTraffic.com and GoogleEarth: 08 February 2021 – 15:00 EDT (unless otherwise noted)]

NOTE: AHTS = Anchor Handling Tug/Supply Ship

[1] Name: ***AKADEMIK CHERSKIY***
IMO: 8770261
Flag: Russia
Vessel Type: Pipelay Crane Ship

[2] Name: ***MENTOR***
IMO: 8407711
Flag: Cyprus
Vessel Type: Support Tug

[3] Name: ***UMKA***
IMO: 9171620
Flag: Russia
Vessel Type: Offshore Supply Ship

[4] Name: ***DP GEZINA***
IMO: 9295103
Flag: Bahamas
Vessel Type: Offshore Supply Ship

[5] Name: ***KREBS GEO***
MMSI: 261025530
Flag: Poland
Vessel Type: Passenger Transport Ship

[6] Name: ***GLOMAR WAVE***
IMO: 9682617
Flag: Panama
Vessel Type: Accommodation/ROV Ship

[7] Name: ***IVAN SIDORENKO***
IMO: 9624213
Flag: Russia
Vessel Type: Offshore Supply Ship

[8] Name: ***YURI TOPCHEV***
IMO: 933820
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[9] Name: ***FINVAL***
IMO: 9272412
Flag: Russia
Vessel Type: Multi-Purpose Offshore Ship

[10] Name: ***VLADISLAV STRIZHOV***
IMO: 9310018
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[11] Name: ***KATUN***
IMO: 9701126
Flag: Russia
Vessel Type: AHTS Ship

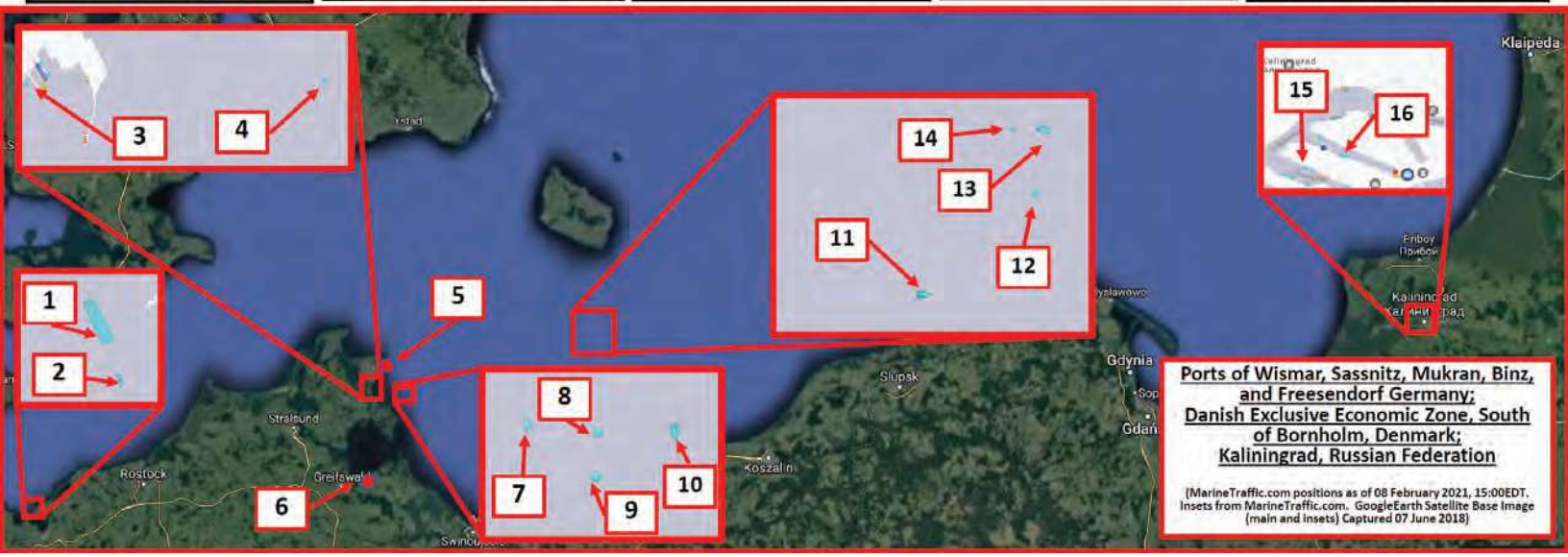
[12] Name: ***FORTUNA***
IMO: 8674156
Flag: Russia
Vessel Type: Pipelay Crane Ship

[13] Name: ***BALTIYSKIY ISSLEDOVATEL***
IMO: 9572020
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[14] Name: ***VENIE***
IMO: 9451654
Flag: Russia
Vessel Type: Offshore Supply Ship

[15] Name: ***MURMAN***
IMO: 9682423
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[16] Name: ***ARTEMIS OFFSHORE***
IMO: 9747194
Flag: Russia
Vessel Type: Offshore Supply Ship



Ports of Wismar, Sassnitz, Mukran, Binz, and Freesendorf Germany; Danish Exclusive Economic Zone, South of Bornholm, Denmark; Kaliningrad, Russian Federation

(MarineTraffic.com positions as of 08 February 2021, 15:00EDT. Insets from MarineTraffic.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Possible Nord Stream 2 Deployment or Support-Related Vessel Status

[Data from MarineTraffic.com, Fleetmon.com, and GoogleEarth: 13 January 2021 – 18:30 EDT (unless otherwise noted)]

[1] Name: ***FORTUNA***
IMO: 8674156
Flag: Russia
Vessel Type: Pipelay Crane Ship

[2] Name: ***KATUN***
IMO: 9701126
Flag: Russia
Vessel Type: Offshore Supply Ship

[3] Name: ***EERIE***
IMO: 9474426
Flag: Liberia
Vessel Type: Offshore Supply Vessel

[4] Name: ***CORVIN***
IMO: 9280433
Flag: Germany
Vessel Type: Support Tug

[5] Name: ***WOLF***
IMO: 9036260
Flag: Germany
Vessel Type: Support Tug

[6] Name: ***MULTRATUG 29***
IMO: 9795816
Flag: Netherlands
Vessel Type: Support Tug

[7] Name: ***WULF 7***
IMO: 9183075
Flag: Germany
Vessel Type: Support Tug

[8] Name: ***WAL***
IMO: 9036258
Flag: Germany
Vessel Type: Support Tug

[9] Name: ***KREBS GEO***
MMSI: 261025530
Flag: Poland
Vessel Type: Passenger Transport

[10] Name: ***VLADISLAV STRIZHOV***
IMO: 9310018
Flag: Russia
Vessel Type: Icebreaker

[11] Name: ***MENTOR***
IMO: 8407711
Flag: Cyprus
Vessel Type: Support Tug

[12] Name: ***DP GEZINA***
IMO: 9295103
Flag: Bahamas
Vessel Type: Offshore Supply Ship

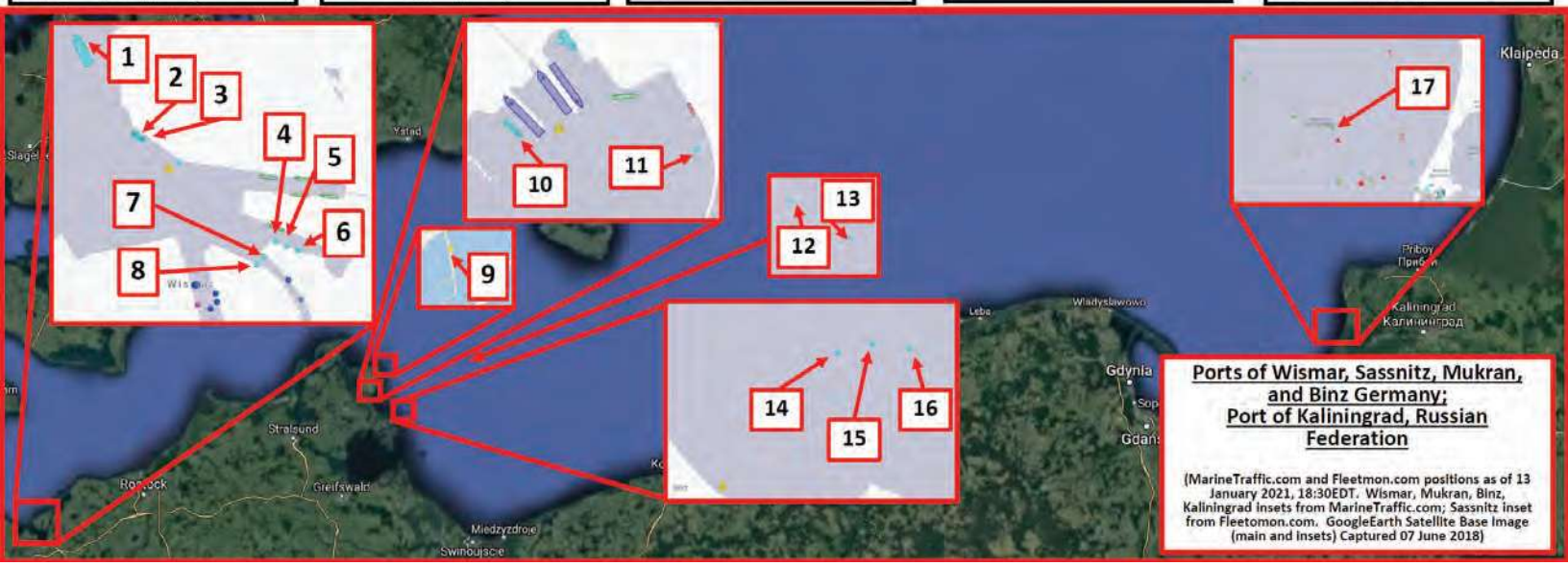
[13] Name: ***BALTIYSKIY ISSLEDOVATEL***
IMO: 9572020
Flag: Russia
Vessel Type: Offshore Supply Ship

[14] Name: ***UMKA***
IMO: 9171620
Flag: Russia
Vessel Type: Offshore Supply Ship

[15] Name: ***IVAN SIDORENKO***
IMO: 9624213
Flag: Russia
Vessel Type: Offshore Supply Ship

[16] Name: ***MURMAN***
IMO: 9682423
Flag: Russia
Vessel Type: Salvage/Rescue Ship

[17] Name: ***Akademik Cherskiy***
IMO: 8770261
Flag: Russia
Vessel Type: Pipelay Crane Ship



Ports of Wismar, Sassnitz, Mukran, and Binz Germany; Port of Kaliningrad, Russian Federation

(MarineTraffic.com and Fleetmon.com positions as of 13 January 2021, 18:30EDT. Wismar, Mukran, Binz, Kaliningrad insets from MarineTraffic.com; Sassnitz inset from Fleetomon.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Possible Nord Stream 2 Deployment or Support-Related Vessel Status

[Data from MarineTraffic.com, Fleetmon.com, and GoogleEarth: 14 January 2021 – 14:30 EDT (unless otherwise noted)]

NOTE: AHTS = Anchor Handling Tug/Supply Ship

[1] Name: ***EERIE***
IMO: 9474426
Flag: Liberia
Vessel Type: AHTS Ship

[2] Name: ***FORTUNA***
IMO: 8674156
Flag: Russia
Vessel Type: Pipelay Crane Ship

[3] Name: ***KATUN***
IMO: 9701126
Flag: Russia
Vessel Type: AHTS Ship

[4] Name: ***KREBS GEO***
MMSI: 261025530
Flag: Poland
Vessel Type: Passenger Transport Ship

[5] Name: ***MENTOR***
IMO: 8407711
Flag: Cyprus
Vessel Type: Support Tug

[6] Name: ***UMKA***
IMO: 9171620
Flag: Russia
Vessel Type: Offshore Supply Ship

[7] Name: ***IVAN SIDORENKO***
IMO: 9624213
Flag: Russia
Vessel Type: Offshore Supply Ship

[8] Name: ***MURMAN***
IMO: 9682423
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[9] Name: ***VLADISLAV STRIZHOV***
IMO: 9310018
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

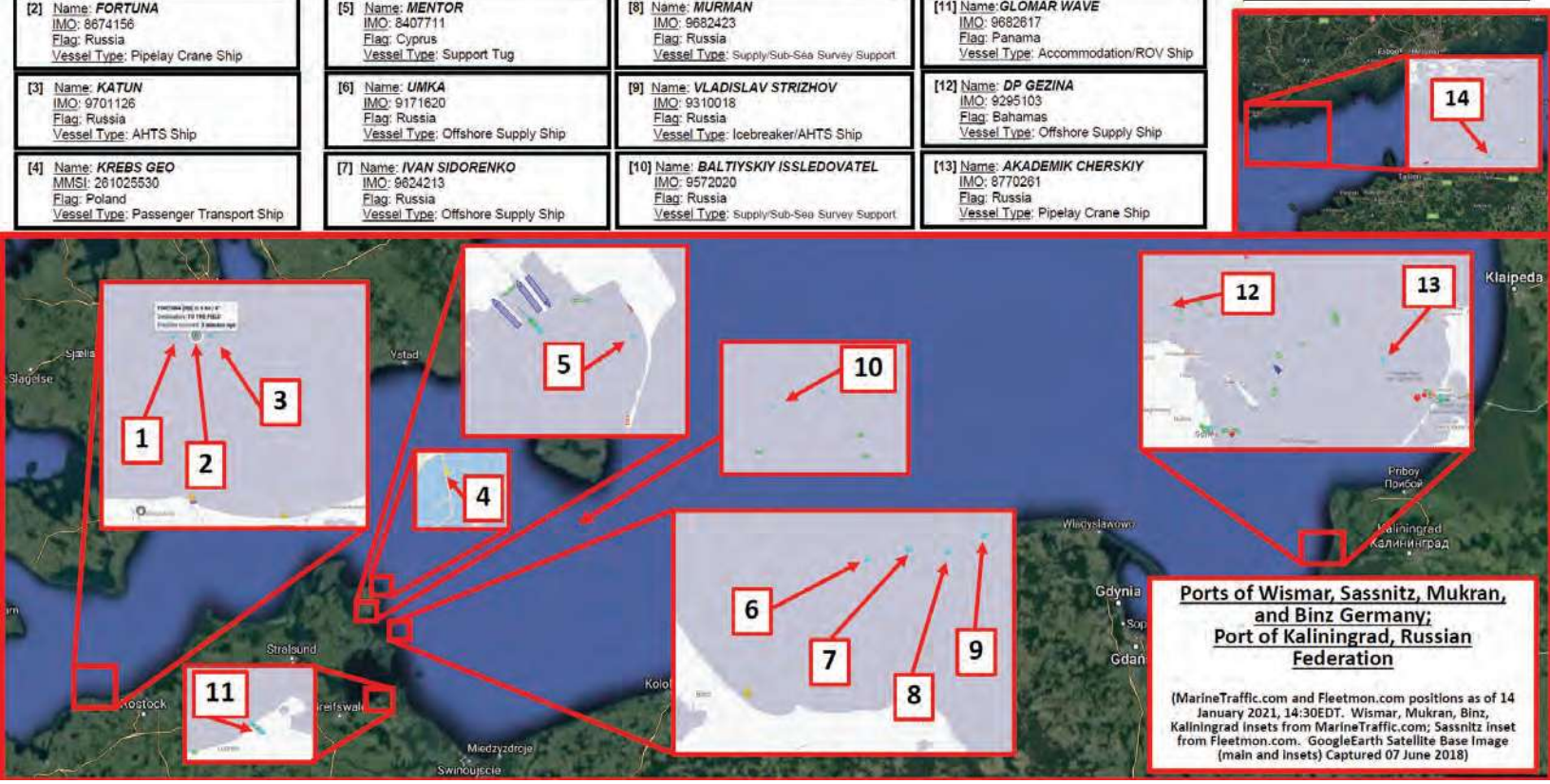
[10] Name: ***BALTIYSKIY ISSLEDOVATEL***
IMO: 9572020
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[11] Name: ***GLOMAR WAVE***
IMO: 9682617
Flag: Panama
Vessel Type: Accommodation/ROV Ship

[12] Name: ***DP GEZINA***
IMO: 9295103
Flag: Bahamas
Vessel Type: Offshore Supply Ship

[13] Name: ***AKADEMIK CHERSKIY***
IMO: 8770261
Flag: Russia
Vessel Type: Pipelay Crane Ship

[14] Name: ***ARTEMIS OFFSHORE***
IMO: 9747194
Flag: Russia
Vessel Type: Offshore Supply Ship



Ports of Wismar, Sassnitz, Mukran, and Binz Germany; Port of Kaliningrad, Russian Federation

(MarineTraffic.com and Fleetmon.com positions as of 14 January 2021, 14:30EDT. Wismar, Mukran, Binz, Kaliningrad insets from MarineTraffic.com; Sassnitz inset from Fleetmon.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Possible Nord Stream 2 Deployment or Support-Related Vessel Status

[Data from MarineTraffic.com and GoogleEarth: 23 January 2021 – 14:00 EDT (unless otherwise noted)]

NOTE: AHTS = Anchor Handling Tug/Supply Ship

[1] Name: ***AKADEMIK CHERSKIY***
IMO: 8770261
Flag: Russia
Vessel Type: Pipelay Crane Ship

[2] Name: ***ARTEMIS OFFSHORE***
IMO: 9747194
Flag: Russia
Vessel Type: Offshore Supply Ship

[3] Name: ***MENTOR***
IMO: 8407711
Flag: Cyprus
Vessel Type: Support Tug

[4] Name: ***KREBS GEO***
MMSI: 261025530
Flag: Poland
Vessel Type: Passenger Transport Ship

[5] Name: ***UMKA***
IMO: 9171620
Flag: Russia
Vessel Type: Offshore Supply Ship

[6] Name: ***MURMAN***
IMO: 9682423
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[7] Name: ***BALTIYSKIY ISSLEDOVATEL***
IMO: 9572020
Flag: Poland
Vessel Type: Supply/Sub-Sea Survey Support

[8] Name: ***VLADISLAV STRIZHOV***
IMO: 9310018
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[9] Name: ***YURI TOPCHEV***
IMO: 933820
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[10] Name: ***FORTUNA***
IMO: 8674156
Flag: Russia
Vessel Type: Pipelay Crane Ship

[11] Name: ***DP GEZINA***
IMO: 9295103
Flag: Bahamas
Vessel Type: Offshore Supply Ship

[12] Name: ***KATUN***
IMO: 9701126
Flag: Russia
Vessel Type: AHTS Ship

[13] Name: ***VENIE***
IMO: 9451654
Flag: Russia
Vessel Type: Offshore Supply Ship

[14] Name: ***GLOMAR WAVE***
IMO: 9682617
Flag: Panama
Vessel Type: Accommodation/ROV Ship

[15] Name: ***IVAN SIDORENKO***
IMO: 9624213
Flag: Russia
Vessel Type: Offshore Supply Ship

Ports of Wismar, Sassnitz, Mukran, Binz, and Freesendorf Germany; Danish Exclusive Economic Zone, South of Bornholm, Denmark; Kaliningrad, Russian Federation

(MarineTraffic.com positions as of 23 January 2021, 14:00EDT. Insets from MarineTraffic.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Possible Nord Stream 2 Deployment or Support-Related Vessel Status

[Data from MarineTraffic.com and GoogleEarth: 26 February 2021 – 17:00 EDT (unless otherwise noted)]

NOTE: AHTS = Anchor Handling Tug/Supply Ship

[1] Name: ***AKADEMIK CHERSKIY***
IMO: 8770261
Flag: Russia
Vessel Type: Pipelay Crane Ship

[2] Name: ***KREBS GEO***
MMSI: 261025530
Flag: Poland
Vessel Type: Passenger Transport Ship

[3] Name: ***IVAN SIDORENKO***
IMO: 9624213
Flag: Russia
Vessel Type: Offshore Supply Ship

[4] Name: ***DP GEZINA***
IMO: 9295103
Flag: Bahamas
Vessel Type: Offshore Supply Ship

[5] Name: ***GLOMAR WAVE***
IMO: 9682617
Flag: Panama
Vessel Type: Accommodation/ROV Ship

[6] Name: ***VLADISLAV STRIZHOV***
IMO: 9310018
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[7] Name: ***YURI TOPCHEV***
IMO: 933820
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[8] Name: ***HAVILA SUBSEA***
IMO: 9505508
Flag: Norway
Vessel Type: Offshore Supply Ship

[9] Name: ***UMKA***
IMO: 9171620
Flag: Russia
Vessel Type: Offshore Supply Ship

[10] Name: ***BALTIYSKIY ISSLEDOVATEL***
IMO: 9572020
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[11] Name: ***FORTUNA*** — US OFAC SDN: CAATSA PEESA
IMO: 8674156
Flag: Russia
Vessel Type: Pipelay Crane Ship

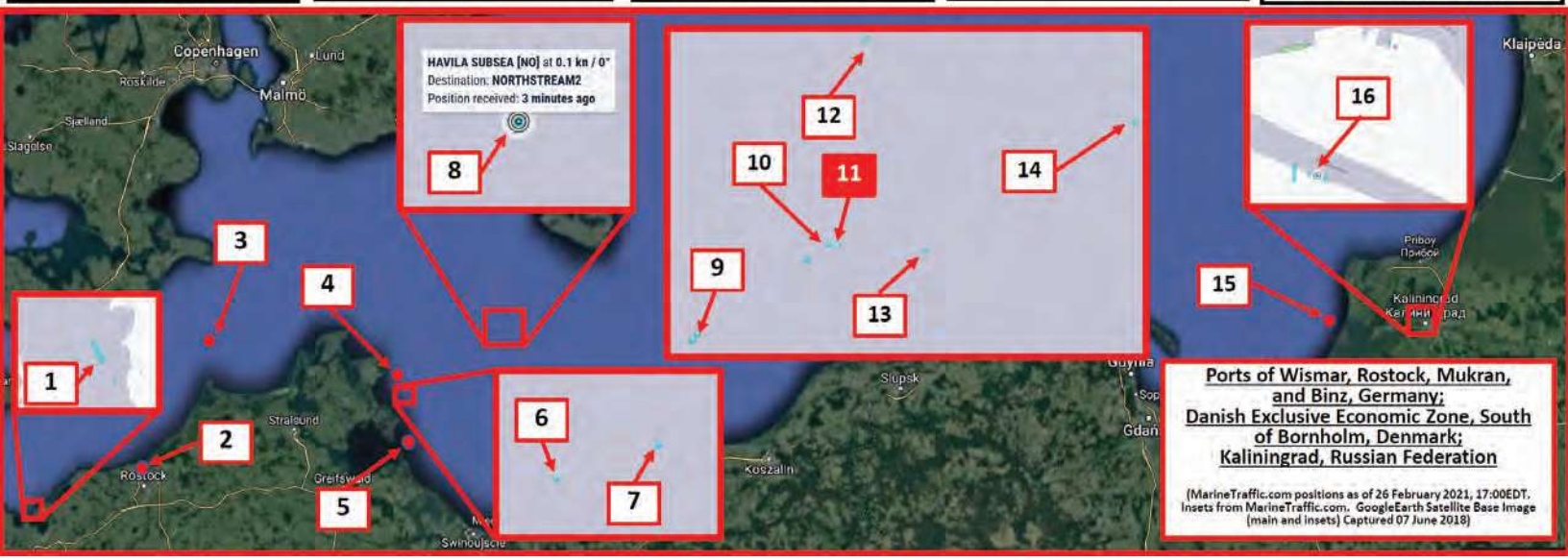
[12] Name: ***FINVAL***
IMO: 9272412
Flag: Russia
Vessel Type: Multi-Purpose Offshore Ship

[13] Name: ***KATUN***
IMO: 9701126
Flag: Russia
Vessel Type: AHTS Ship

[14] Name: ***MURMAN***
IMO: 9682423
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[15] Name: ***VENIE***
IMO: 9451654
Flag: Russia
Vessel Type: Offshore Supply Ship

[16] Name: ***ARTEMIS OFFSHORE***
IMO: 9747194
Flag: Russia
Vessel Type: Offshore Supply Ship



Possible Nord Stream 2 Deployment or Support-Related Vessel Status

[Data from MarineTraffic.com and GoogleEarth: 12 September 2021 – 19:00 EDT (unless otherwise noted)]

NOTE: AHTS = Anchor Handling Tug/Supply Ship

[1] Name: ***AKADEMIK CHERSKIY*** — US OFAC SDN: PEESA-EO
IMO: 8770261
Flag: Russia
Vessel Type: Pipelay Crane Ship

[2] Name: ***KREBS GEO***
MMSI: 261025530
Flag: Poland
Vessel Type: Passenger Transport Ship

[3] Name: ***ARTEMIS OFFSHORE*** — US OFAC SDN: PEESA-EO
IMO: 9747194
Flag: Russia
Vessel Type: Offshore Supply Ship

[4] Name: ***DP GEZINA***
IMO: 9295103
Flag: Bahamas
Vessel Type: Offshore Supply Ship

[5] Name: ***GLOMAR WAVE***
IMO: 9682617
Flag: Panama
Vessel Type: Accommodation/ROV Ship

[6] Name: ***KATUN***
IMO: 9701126
Flag: Russia
Vessel Type: AHTS Ship

[7] Name: ***YURI TOPCHEV*** — US OFAC SDN: PEESA-EO
IMO: 933820
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship

[8] Name: ***FORTUNA*** — US OFAC SDN: CAATSA PEESA
IMO: 8674156
Flag: Russia
Vessel Type: Pipelay Crane Ship

[9] Name: ***MURMAN*** — US OFAC SDN: PEESA-EO
IMO: 9682423
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[10] Name: ***VENIE***
IMO: 9451654
Flag: Russia
Vessel Type: Offshore Supply Ship

[11] Name: ***FINVAL*** — US OFAC SDN: PEESA-EO
IMO: 9272412
Flag: Russia
Vessel Type: Multi-Purpose Offshore Ship

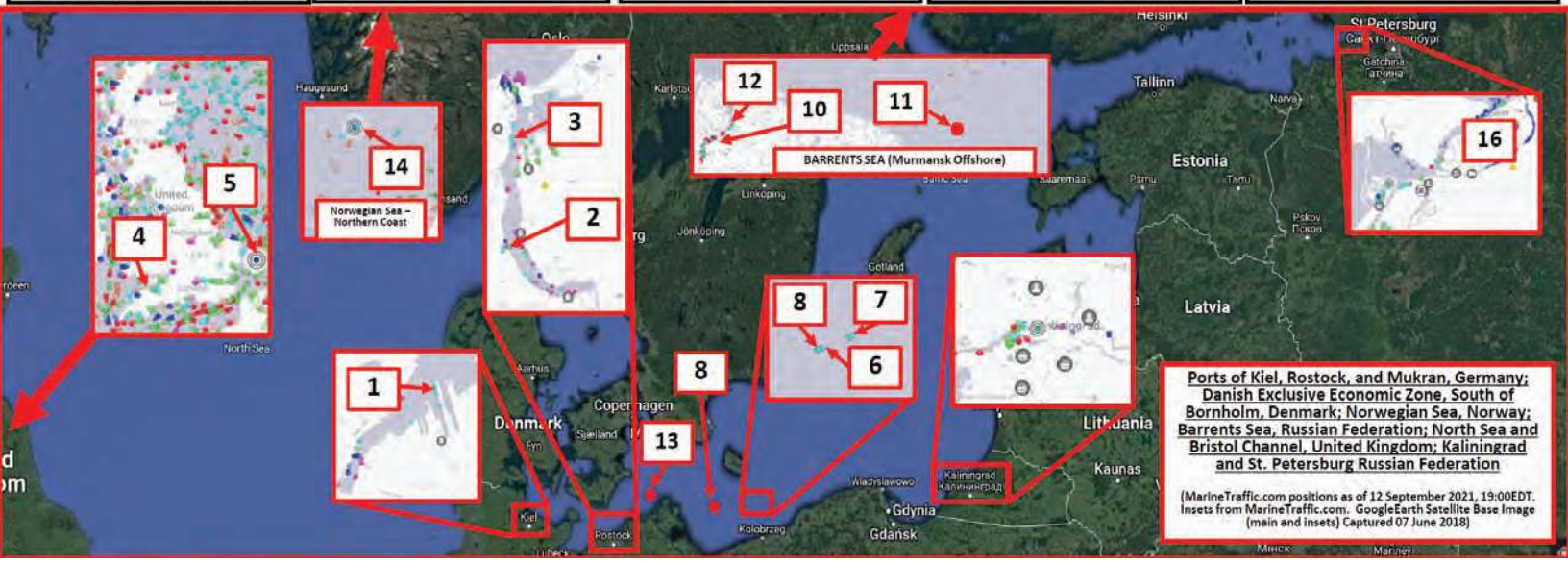
[12] Name: ***UMKA*** — US OFAC SDN: PEESA-EO
IMO: 9171620
Flag: Russia
Vessel Type: Offshore Supply Ship

[13] Name: ***BALTIYSKIY ISSLEDOVATEL*** — US OFAC SDN: PEESA-EO
IMO: 9572020
Flag: Russia
Vessel Type: Supply/Sub-Sea Survey Support

[13] Name: ***HAVILA SUBSEA***
IMO: 9505508
Flag: Norway
Vessel Type: Offshore Supply Ship

[15] Name: ***IVAN SIDORENKO*** — US OFAC SDN: PEESA-EO
IMO: 9624213
Flag: Russia
Vessel Type: Offshore Supply Ship

[16] Name: ***VLADISLAV STRIZHOV*** — US OFAC SDN: PEESA-EO
IMO: 9310018
Flag: Russia
Vessel Type: Icebreaker/AHTS Ship



Possible Vessels Related to Nord Stream 1 and Nord Stream 2 Forensic Investigation

[Data from MarineTraffic.com and GoogleEarth: 04 October 2022 – 21:15 EDT (unless otherwise noted)]

[1] Name: ***HDMS SOELOEVEN***
MMSI: 219000217
Flag: Denmark
Vessel Type: Military Operations Vessel

[2] Name: ***HORIZON GEOBAY***
IMO: 7801556
Flag: Panama
Vessel Type: Research/Survey Vessel

[3] Name: ***LEOPOLD ROSENFELDT***
IMO: 8902670
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[4] Name: ***KOMMANDOR SUSAN***
IMO: 9177844
Flag: United Kingdom
Vessel Type: Research/Survey Vessel

[5] Name: ***HDMS ABSALON***
IMO: 9284441
Flag: United Kingdom
Vessel Type: Military Command Vessel

[6] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196149
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 1 RAD 5 NM"

[7] Name: ***HDMS SALTHOLM***
MMSI: 219000093
Flag: Denmark
Vessel Type: Military Operations Vessel

[8] Name: ***GUNNAR THORSON***
IMO: 7924061
Flag: Denmark
Vessel Type: Pollution Control Vessel

[9] Name: ***DANISH WARSHIP F342***
MMSI: 220191000
Flag: Denmark
Vessel Type: Military Operations Vessel

[10] Name: ***KVB 003 AMFITRITE***
IMO: 9380465
Flag: Sweden
Vessel Type: Salvage/Rescue Vessel

[11] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196151
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 3 RAD 5 NM"

[12] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196150
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 2 RAD 5 NM"

[13] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196152
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 4 RAD 5 NM"

[14] Name: ***BELOS – SWEDISH WARSHIP A214***
IMO: 8308288
Flag: Sweden
Vessel Type: Naval Salvage Vessel

[15] Name: ***SWEDISH WARSHIP M14***
MMSI: 265500790
Flag: Sweden
Vessel Type: Military Operations Vessel

[16] Name: ***KBV 502***
MMSI: 111265102
Flag: Sweden
Vessel Type: Search and Rescue

[17] Name: ***SAR 111265102***
MMSI: 111265102
Flag: Sweden
Vessel Type: Search and Rescue Aircraft

Danish Exclusive Economic Zone, Southeast of Bornholm, Denmark;

Swedish Exclusive Economic Zone, Northeast of Bornholm, Denmark

(MarineTraffic.com positions as of 04 October 2022, 21:15 EDT. Insets from MarineTraffic.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Select Vessels Near Nord Stream 1 and Nord Stream 2 Forensic Investigation Sites

[Data from MarineTraffic.com and GoogleEarth: 06 October 2022 – 20:00 EDT (unless otherwise noted)]

[1] Name: ***DNK NAVY PATROL P523***
MMSI: 220434000
Flag: Denmark
Vessel Type: Military Operations Vessel

[2] Name: ***HORIZON GEOBAY***
IMO: 7801556
Flag: Panama
Vessel Type: Research/Survey Vessel

[3] Name: ***LEOPOLD ROSENFELDT***
IMO: 8902670
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[4] Name: ***HDMS ABSALON***
IMO: 9284441
Flag: United Kingdom
Vessel Type: Military Command Vessel

[5] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196149
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 1 RAD 5 NM"

[6] Name: ***USNS WILLIAM MCLEAN***
IMO: 9552006 [*Approx. location as of 16:00 EDT*]
Flag: United States
Vessel Type: Navy Replenishment Vessel

[7] Name: ***NIVENSKOYE***
IMO: 8843018 [*Approx. location as of 16:00 EDT*]
Flag: Russian Federation
Vessel Type: Fishing Vessel

[8] Name: ***GUNNAR THORSON***
IMO: 7924061
Flag: Denmark
Vessel Type: Pollution Control Vessel

[9] Name: ***RIB KRST 850 001 16***
MMSI: 219021615
Flag: Denmark
Vessel Type: Search and Rescue Vessel

[10] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196150
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 2 RAD 5 NM"

[11] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196151
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 3 RAD 5 NM"

[12] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196152
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 4 RAD 5 NM"

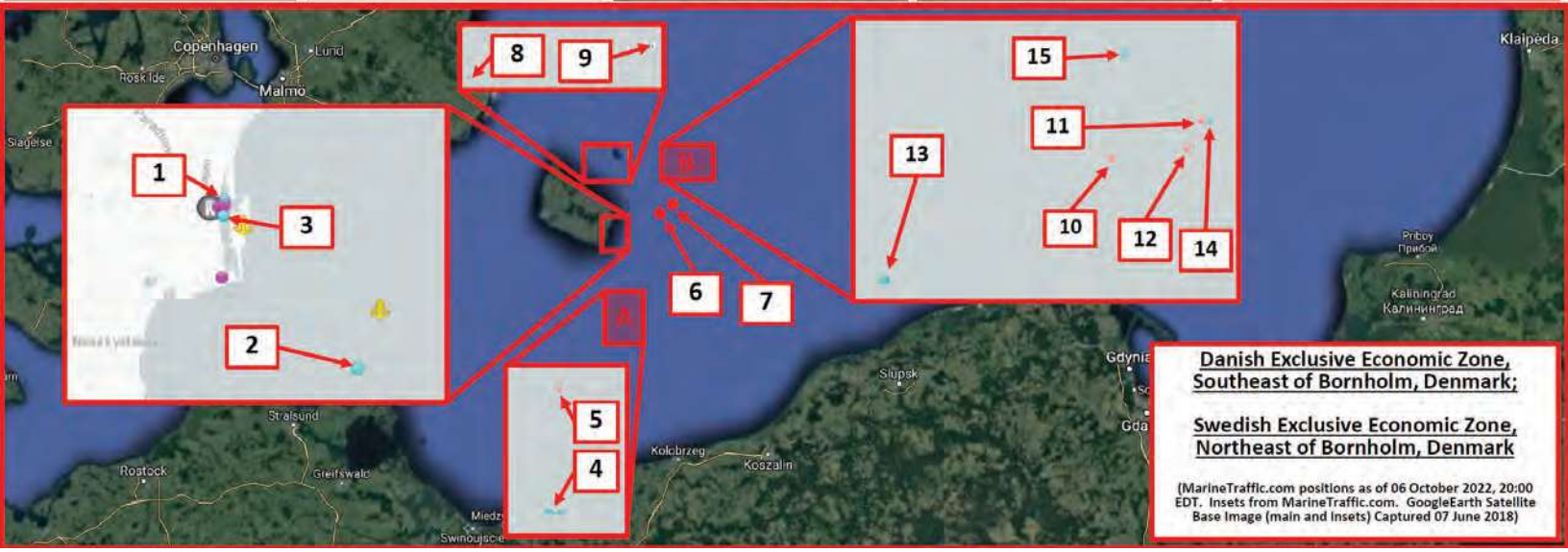
[13] Name: ***DANISH WARSHIP F342***
MMSI: 220191000
Flag: Denmark
Vessel Type: Military Operations Vessel

[14] Name: ***BELOS – SWEDISH WARSHIP A214***
IMO: 8308288
Flag: Sweden
Vessel Type: Naval Salvage Vessel

[15] Name: ***KVB 002 TRITON***
IMO: 9380453
Flag: Sweden
Vessel Type: Coast Guard Tug

DANGER ZONE A:
Nord Stream 2 (One Trunkline)
Danish EEZ Leak Site

DANGER ZONE B:
Nord Stream 1 (Both Trunklines) and
Nord Stream 2 (One Trunkline)
Swedish EEZ Leak Sites



Danish Exclusive Economic Zone, Southeast of Bornholm, Denmark;

Swedish Exclusive Economic Zone, Northeast of Bornholm, Denmark

(MarineTraffic.com positions as of 06 October 2022, 20:00 EDT. Insets from MarineTraffic.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Select Vessels Near Nord Stream 1 and Nord Stream 2 Forensic Investigation Sites

[Data from MarineTraffic.com and GoogleEarth: 07 October 2022 – 17:00 EDT (unless otherwise noted)]

[1] Name: ***HORIZON GEOBAY***
IMO: 7801556
Flag: Panama
Vessel Type: Research/Survey Vessel

[2] Name: ***LEOPOLD ROSENFELDT***
IMO: 8902670
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[3] Name: ***DNK NAVY PATROL P524***
MMSI: 220435000
Flag: Denmark
Vessel Type: Military Operations Vessel

[4] Name: ***MHV 903 HJORTOE***
MMSI: 219000167
Flag: Denmark
Vessel Type: Military Operations Vessel

[5] Name: ***KYST FRB19***
MMSI: 219019015
Flag: Denmark
Vessel Type: Search and Rescue Vessel

[6] Name: ***MADS JAKOBSEN***
IMO: 9256080
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[7] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196149
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 1 RAD 5 NM"

[8] Name: ***HDMS ABSALON***
IMO: 9284441
Flag: Denmark
Vessel Type: Military Command Vessel

[9] Name: ***SERGEY BALK***
IMO: 9803182
Flag: Russian Federation
Vessel Type: Tug
Note: "Vessel Departed SEVASTOPOL, UA, on 2022-01-21"

[10] Name: ***GUNNAR THORSON***
IMO: 7924061
Flag: Denmark
Vessel Type: Pollution Control Vessel

[11] Name: ***RIB KRST 850 001 16***
MMSI: 219021615
Flag: Denmark
Vessel Type: Search and Rescue Vessel

[12] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196150
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 2 RAD 5 NM"

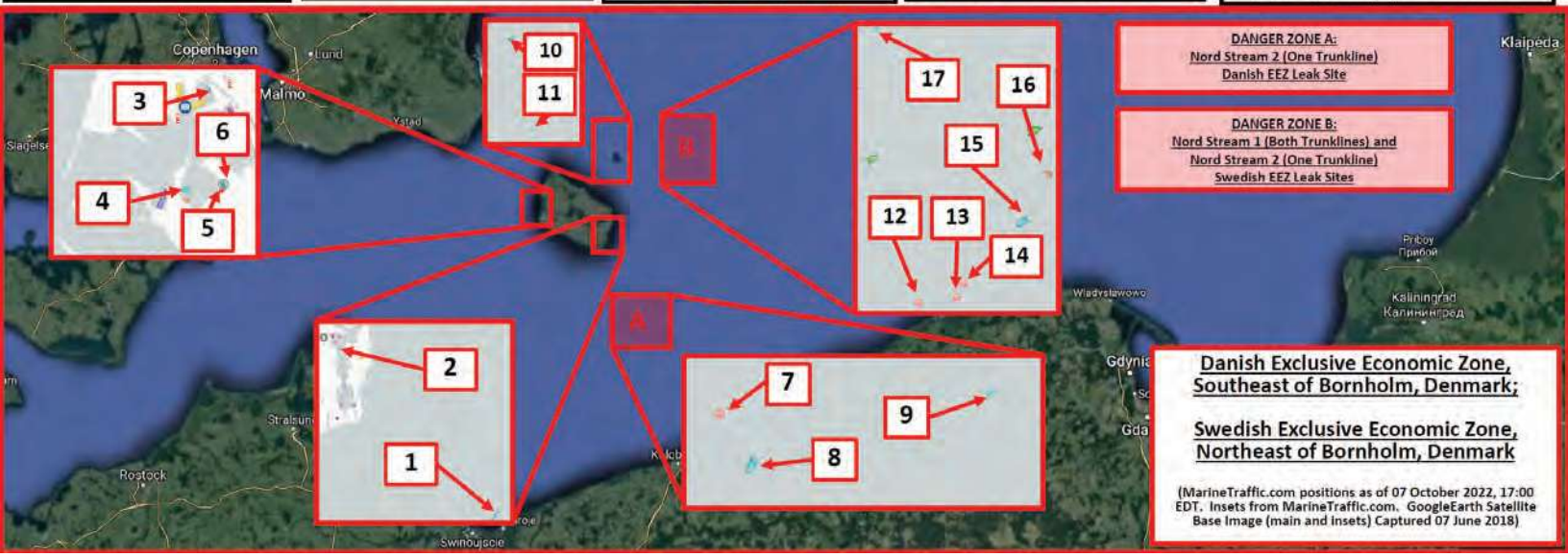
[13] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196152
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 4 RAD 5 NM"

[14] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196151
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 3 RAD 5 NM"

[15] Name: ***DANISH WARSHIP F342***
MMSI: 220191000
Flag: Denmark
Vessel Type: Military Operations Vessel

[16] Name: ***ATLANTNIRO***
IMO: 8607050
Flag: Russian Federation
Vessel Type: Fishing Vessel

[17] Name: ***SWEDISH WARSHIP***
MMSI: 265500350
Flag: Sweden
Vessel Type: Military Operations Vessel



Select Vessels Near Nord Stream 1 and Nord Stream 2 Forensic Investigation Sites

[Data from MarineTraffic.com and GoogleEarth: 08 October 2022 – 20:00 EDT (unless otherwise noted)]

[1] Name: ***HORIZON GEOBAY***
IMO: 7801556
Flag: Panama
Vessel Type: Research/Survey Vessel

[2] Name: ***LEOPOLD ROSENFELDT***
IMO: 8902670
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[3] Name: ***DNK NAVY PATROL P524***
MMSI: 220435000
Flag: Denmark
Vessel Type: Military Operations Vessel

[4] Name: ***MHV 903 HJORTOE***
MMSI: 219000167
Flag: Denmark
Vessel Type: Military Operations Vessel

[5] Name: ***MADS JAKOBSEN***
IMO: 9256080
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[6] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196149
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 1 RAD 5 NM"

[7] Name: ***ASSISTER***
IMO: 9193783
Flag: Denmark
Vessel Type: Tug/Supply Vessel

[8] Name: ***HDMS ABSALON***
IMO: 9284441
Flag: Denmark
Vessel Type: Military Command Vessel

[9] Name: ***RIB KRST 850 001 16***
MMSI: 219021615
Flag: Denmark
Vessel Type: Search and Rescue Vessel

[10] Name: ***GUNNAR THORSON***
IMO: 7924061
Flag: Denmark
Vessel Type: Pollution Control Vessel

[11] Name: ***SKOVEN***
IMO: 8621408
Flag: Denmark
Vessel Type: Standby Safety Vessel

[12] Name: ***SORMOVSKIY 53***
IMO: 8628133 [*Position as of 10:30 EDT*]
Flag: Russian Federation
Vessel Type: General Cargo Vessel

[13] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196150
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 2 RAD 5 NM"

[14] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196152
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 4 RAD 5 NM"

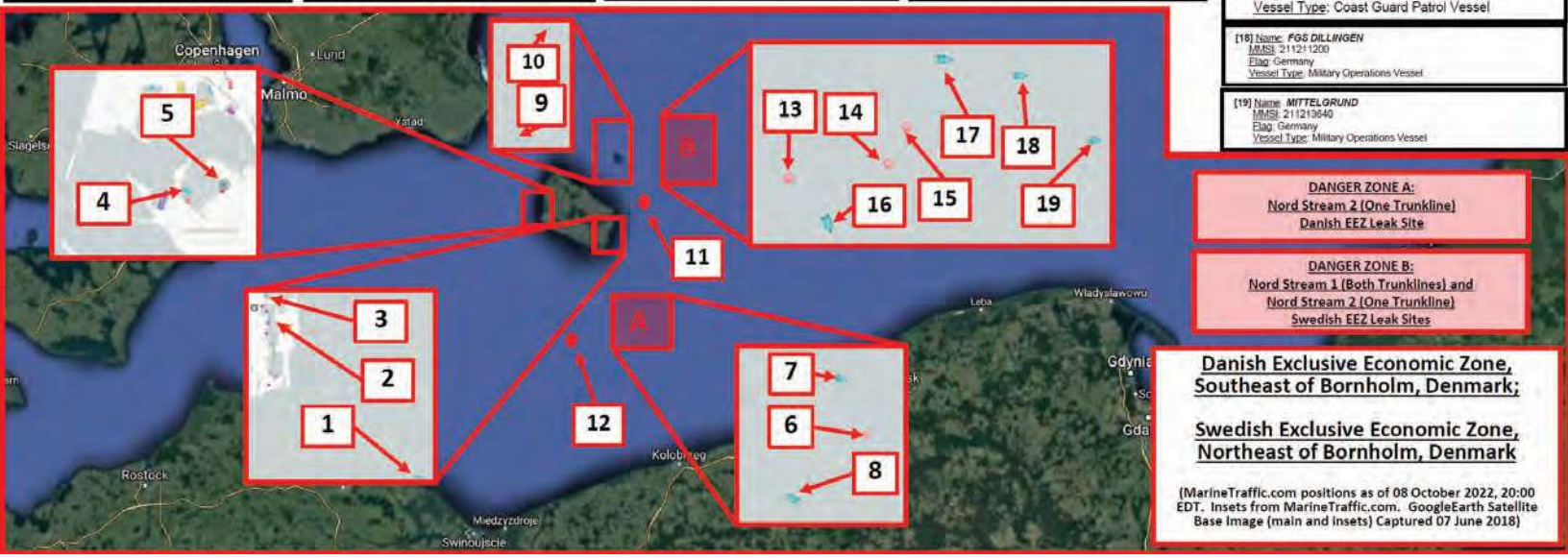
[15] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196151
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 3 RAD 5 NM"

[16] Name: ***DANISH WARSHIP F342***
MMSI: 220191000
Flag: Denmark
Vessel Type: Military Operations Vessel

[17] Name: ***POTSDAM***
IMO: 9830018
Flag: Germany
Vessel Type: Coast Guard Patrol Vessel

[18] Name: ***FGS DILLINGEN***
MMSI: 211211200
Flag: Germany
Vessel Type: Military Operations Vessel

[19] Name: ***MITTELGRUND***
MMSI: 211213640
Flag: Germany
Vessel Type: Military Operations Vessel



Select Vessels Near Nord Stream 1 and Nord Stream 2 Forensic Investigation Sites

[Data from MarineTraffic.com and GoogleEarth: 09 October 2022 – 10:30 EDT (unless otherwise noted)]

[1] Name: ***LEOPOLD ROSENFELDT***
IMO: 8902670
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[2] Name: ***DNK NAVY PATROL P524***
MMSI: 220435000
Flag: Denmark
Vessel Type: Military Operations Vessel

[3] Name: ***GUNNAR THORSON***
IMO: 7924061
Flag: Denmark
Vessel Type: Pollution Control Vessel

[4] Name: ***MHV 903 HJORTOE***
MMSI: 219000167
Flag: Denmark
Vessel Type: Military Operations Vessel

[5] Name: ***MADS JAKOBSEN***
IMO: 9256080
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[6] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196149
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 1 RAD 5 NM"

[7] Name: ***ASSISTER***
IMO: 9193783
Flag: Denmark
Vessel Type: Tug/Supply Vessel

[8] Name: ***DANISH WARSHIP F342***
MMSI: 220191000
Flag: Denmark
Vessel Type: Military Operations Vessel

[9] Name: ***HORIZON GEOBAY***
IMO: 7801556
Flag: Panama
Vessel Type: Research/Survey Vessel

[10] Name: ***AKADEMIK B.PETROV***
IMO: 8211150 [*Position as of 03:15 EDT*]
Flag: Russian Federation
Vessel Type: Research/Survey Vessel

[11] Name: ***SKOVEN***
IMO: 8621408
Flag: Denmark
Vessel Type: Standby Safety Vessel

[12] Name: ***RIB KRST 850 001 16***
MMSI: 219021615
Flag: Denmark
Vessel Type: Search and Rescue Vessel

[13] Name: ***HDMS ABSALON***
IMO: 9284441
Flag: Denmark
Vessel Type: Military Command Vessel

[14] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196150
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 2 RAD 5 NM"

[15] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196152
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 4 RAD 5 NM"

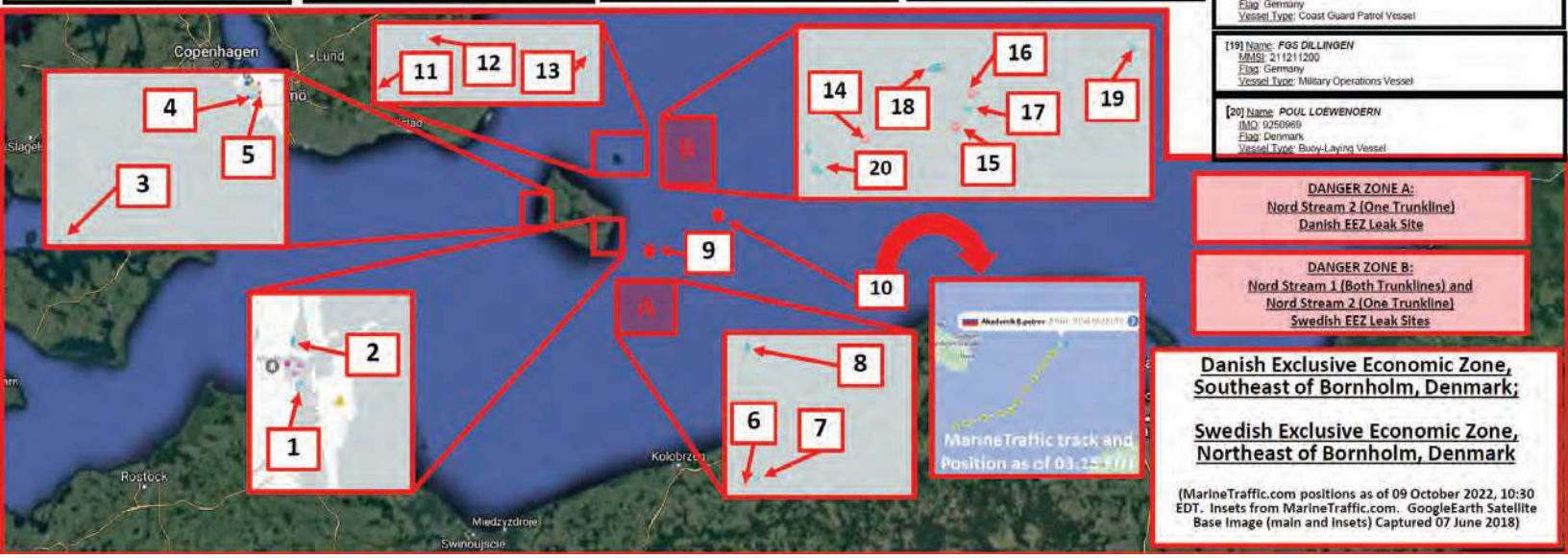
[16] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196151
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 3 RAD 5 NM"

[17] Name: ***MITTELGRUND***
MMSI: 211213640
Flag: Germany
Vessel Type: Military Operations Vessel

[18] Name: ***POTSDAM***
IMO: 9830018
Flag: Germany
Vessel Type: Coast Guard Patrol Vessel

[19] Name: ***FGS DILLINGEN***
MMSI: 211211200
Flag: Germany
Vessel Type: Military Operations Vessel

[20] Name: ***POUL LOEWENOERN***
IMO: 9250969
Flag: Denmark
Vessel Type: Buoy-Laying Vessel



DANGER ZONE A:
Nord Stream 2 (One Trunkline)
Danish EEZ Leak Site

DANGER ZONE B:
Nord Stream 1 (Both Trunklines) and
Nord Stream 2 (One Trunkline)
Swedish EEZ Leak Sites

Danish Exclusive Economic Zone, Southeast of Bornholm, Denmark;

Swedish Exclusive Economic Zone, Northeast of Bornholm, Denmark

(MarineTraffic.com positions as of 09 October 2022, 10:30 EDT. Insets from MarineTraffic.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

Select Vessels Near Nord Stream 1 and Nord Stream 2 Forensic Investigation Sites

[Data from MarineTraffic.com and GoogleEarth: 16 October 2022 – 13:30 EDT (unless otherwise noted)]

[1] Name: ***LEOPOLD ROSENFELDT***
IMO: 8902670
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[2] Name: ***MADS JAKOBSEN***
IMO: 9256080
Flag: Denmark
Vessel Type: Salvage/Rescue Vessel

[3] Name: ***HDMS FREJA***
MMSI: 220432000
Flag: Denmark
Vessel Type: Military Operations Vessel

[4] Name: ***GUNNAR THORSON***
IMO: 7924061
Flag: Denmark
Vessel Type: Pollution Control Vessel

[5] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196149
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 1 RAD 5 NM"

[6] Name: ***POUL LOEWENOERN***
IMO: 9250969
Flag: Denmark
Vessel Type: Buoy-Laying Vessel

[7] Name: ***AKADEMIK TRYOSHNIKOV***
IMO: 9548536
Flag: Russian Federation
Vessel Type: Icebreaking Vessel

[8] Name: ***CABLE ONE***
IMO: 7409281
Flag: Denmark
Vessel Type: Cable Laying Vessel

[9] Name: ***PLEIJEL***
IMO: 7229502
Flag: Sweden
Vessel Type: Cable Laying Vessel

[10] Name: ***RIB KRST 850 001 16***
MMSI: 219021615
Flag: Denmark
Vessel Type: Search and Rescue Vessel

[11] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196150
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 2 RAD 5 NM"

[12] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196152
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 4 RAD 5 NM"

[13] Name: ***ISOLATED DANGER BUOY***
MMSI: 992196151
Flag: Denmark
Vessel Type: Aid to Navigation
Message: "DANGER AREA 3 RAD 5 NM"

[14] Name: ***ASSISTER***
IMO: 9193783
Flag: Denmark
Vessel Type: Tug/Supply Vessel

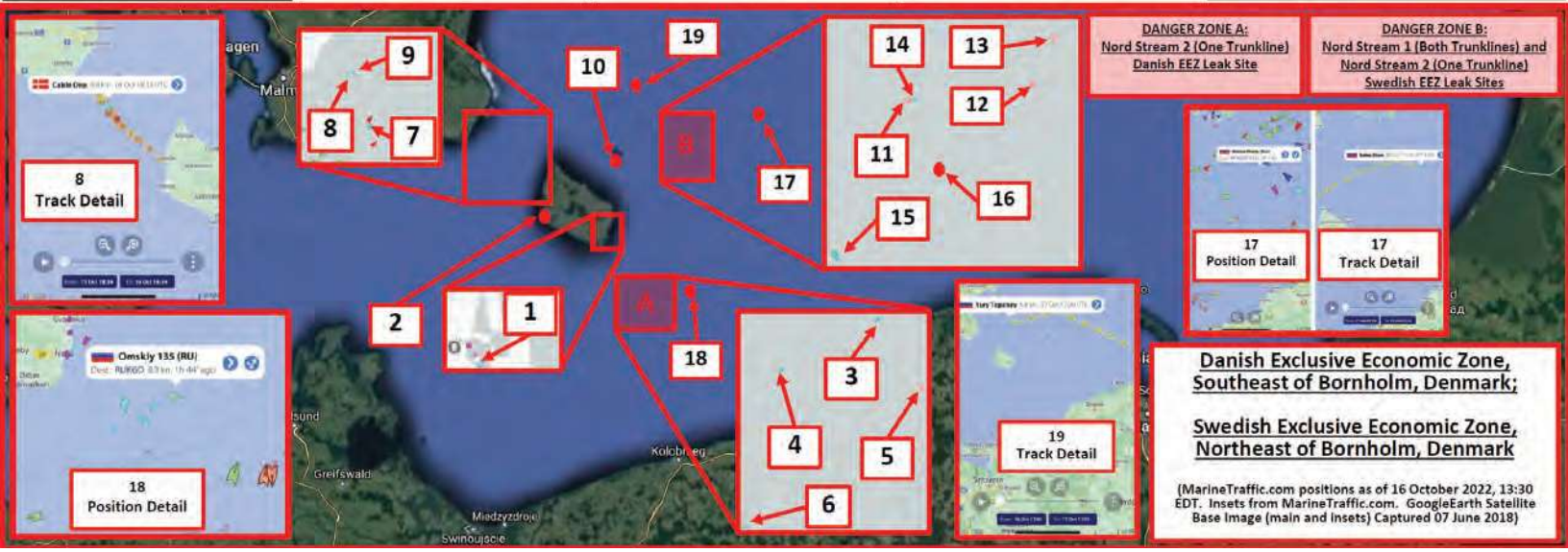
[15] Name: ***DANISH WARSHIP F342***
MMSI: 220191000
Flag: Denmark
Vessel Type: Military Operations Vessel

[16] Name: ***OCEANIA***
IMO: 8304854 [*Approx. Position as of 12:00 EDT, 15 Oct 22*]
Flag: Poland
Vessel Type: Research/Survey Vessel

[17] Name: ***BELOE MORE***
IMO: 9775696 [*Approx. Position as of 21:15 EDT, 11 Oct 22*]
Flag: Russian Federation
Vessel Type: Dredging Vessel

[18] Name: ***OMSKIY 135***
IMO: 8881723 [*Approx. Position as of 08:45 EDT, 12 Oct 22*]
Flag: Russian Federation
Vessel Type: General Cargo Vessel

[19] Name: ***YURY TOPCHEV*** [US OFAC SDN: PEESA-EO]
IMO: 8881723 [*Approx. Position as of 13:00 EDT, 17 Oct 22*]
Flag: Russian Federation
Vessel Type: Icebreaking/AHTS Vessel



DANGER ZONE A:
Nord Stream 2 (One Trunkline)
Danish EEZ Leak Site

DANGER ZONE B:
Nord Stream 1 (Both Trunklines) and
Nord Stream 2 (One Trunkline)
Swedish EEZ Leak Sites

Danish Exclusive Economic Zone, Southeast of Bornholm, Denmark;

Swedish Exclusive Economic Zone, Northeast of Bornholm, Denmark

(MarineTraffic.com positions as of 16 October 2022, 13:30 EDT. Insets from MarineTraffic.com. GoogleEarth Satellite Base Image (main and insets) Captured 07 June 2018)

"Ich bin ein Bornholmer." Gutemensch storefront window in Rønne on the island of Bornholm, Denmark. (September 2024) / CREDIT: B. L. Schmitt

ENDNOTES

1. Danish Defence Command. 2022. "Gas Leak in the Baltic Sea." Danish Defense (Forsvaret) News. September 27, 2022. https://www.forsvaret.dk/en/news/2022/gas-leak-in-the-baltic-sea/

2. European Space Agency. 2022. "Nord Stream as Captured by Planet Dove." The European Space Agency. October 10, 2022. https://www.esa.int/ESA_Multimedia/Images/2022/10/Nord_Stream_as_captured_by_Planet_Dove

3. Poursanidis, K., Sharanik, J., Hadjistassou, C. 2024. "World's Largest Natural Gas Leak from Nord Stream Pipeline Estimated at 478,000 Tonnes." iScience Cell Press Open Access. January 19, 2024. https://www.sciencedirect.com/science/article/pii/S2589004223028493

4. Lehto, E., Ringstrom, A. 2022. "Nord Stream Investigation Finds Evidence of Detonations, Swedish Police Say." Reuters. October 6, 2022. https://www.reuters.com/world/europe/kremlin-says-russia-not-invited-nord-stream-investigation-2022-10-06/

5. Kirby, P. 2014. "Russia's Gas Fight with Ukraine." BBC. October 31, 2014. https://www.bbc.com/news/world-europe-29521564

6. Schmitt, B. L. 2019. "The Neue Ostpolitik Approach to Nord Stream 2: A Legal Fiction Carried a Little Too Far." Atlantic Council EnergySource. December 6, 2019. https://www.atlanticcouncil.org/blogs/energysource/the-neue-ostpolitik-approach-to-nord-stream-2-a-legal-fiction-carried-a-little-too-far/

7. Jewkes, S., Vukmanovik, O. 2017. "Suspected Russia-backed Hackers Target Baltic Energy Networks." Reuters. May 11, 2017. https://www.reuters.com/article/world/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W8/

8. Borger. J. 2018. “U.S. Accuses Russia of Cyber-Attack on Energy Sector and Imposes New Sanctions.” The Guardian. March 15, 2018. https://www.theguardian.com/us-news/2018/mar/15/russia-sanctions-energy-sector-cyber-attack-us-election-interference

9. Åslund, A., Schmitt, B. L. 2021. “Biden Must Persuade Germany and Austria to Stop the “Schroederization” of Europe.” Atlantic Council UkraineAlert. March 11, 2021. https://www.atlanticcouncil.org/blogs/ukrainealert/biden-must-persuade-germany-and-austria-to-stop-the-schroederization-of-europe/

10. Michel, C., Schmitt, B. L. “How to Stop Former Western Leaders From Becoming Paid Shills for Autocrats.” Foreign Policy. February 15, 2022. https://foreignpolicy.com/2022/02/15/gerhard-schroder-gazprom-russia-tony-blair/

11. Barnes, J. E. 2024. “Russia Steps Up a Covert Sabotage Campaign Aimed at Europe.” The New York Times. May 26, 2024. https://www.nytimes.com/2024/05/26/us/politics/russia-sabotage-campaign-ukraine.html

12. Agence France-Presse (Vilnius). 2025. “Russia Behind Arson Attack on IKEA Store in Lithuanian Capital, Says Prosecutor.” The Guardian. March 17, 2025. https://www.theguardian.com/world/2025/mar/17/russia-behind-arson-attack-on-ikea-store-in-lithuania-capital-says-prosecutor

13. Staalesen, A. 2022. “’Human Activity’ Behind Svalbard Cable Disruption.” The Barents Observer. February 11, 2022. https://www.thebarentsobserver.com/security/human-activity-behind-svalbard-cable-disruption/160886

14. Carrel, P., Jacobsen, S. 2022. “EU Vows to Protect Energy Network After ‘Sabotage’ of Russian Gas Pipeline.” Reuters. September 28, 2022. https://www.reuters.com/business/energy/mystery-gas-leaks-hit-major-russian-undersea-gas-pipelines-europe-2022-09-27/

15. Wu, H., Lai, J. 2023. “Taiwan Suspects Chinese Ship Cut Islands’ Internet Cables.” Associated Press. April 18, 2023. https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70

16. Sky News. 2023. “Chinese Ship’s Anchor Caused Damage to Baltic Gas Pipeline, Finland suggests.” Sky News. October 25, 2023. https://news.sky.com/story/chinese-ships-anchor-caused-damage-to-baltic-gas-pipeline-finland-suggests-12992004

17. Pancevski, B. 2024. “Chinese Ship’s Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables.” The Wall Street Journal. November 29, 2024. https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1

18. McHugh, D. 2024. “Finland Stops Russia-linked Vessel Over Damaged Undersea Power Cable in Baltic Sea.” Associated Press. December 26, 2024. https://apnews.com/article/eu-finland-estonia-baltic-sea-power-cable-6741ef1ce9130602abac6214d7297717

19. The Canadian Press. 2025. “Bell Says Subsea Cable from Cape Breton to Newfoundland was Deliberately Cut – Twice.” CTV News. February 19, 2025. https://www.ctvnews.ca/canada/newfoundland-and-labrador/article/bell-says-subsea-cable-from-cape-breton-to-newfoundland-was-deliberately-cut-twice/

20. Tobin, M., Xiao, M., Chang Chien, A. 2025. “Taiwan Says it Suspects a Chinese-linked Ship Damaged an Undersea Internet Cable.” The New York Times. January 7, 2025. https://www.nytimes.com/2025/01/07/world/asia/taiwan-internet-cable-china.html

21. Lee, Y. 2025. “Taiwan Detains China-linked Cargo Ship After Undersea Cable Disconnected.” Reuters. February 25, 2025. https://www.reuters.com/world/asia-pacific/taiwan-detains-china-linked-cargo-ship-after-undersea-cable-disconnected-2025-02-25/

22. MarineTraffic. 2025. “MarineTraffic Web Platform.” MarineTraffic. Accessed 2025. https://www.marinetraffic.com

23. Planet. 2025. “Planet Web Platform.” Planet. Accessed 2025. https://www.planet.com/

24. National Intelligence Council (U.S.). 2021. “Foreign Threats to the 2020 U.S. Federal Elections.” National Intelligence Council Intelligence Community Assessment. March 10, 2021. https://www.intelligence.gov/assets/documents/702%20Documents/declassified/ICA-declass-16MAR21.pdf

25. Fischhoff, B. 2012. “Communicating Uncertainty: Fulfilling the Duty to Inform.” Issues in Science and Technology, The National Academies Press. 2012. https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_070995.pdf

26. Flintoff, C. 2007. “Breaking Down the National Intelligence Estimate.” National Public Radio. December 6, 2007. https://www.npr.org/2007/12/06/16989979/breaking-down-the-national-intelligence-estimate

27. Rojcik, Ondra. 2023. “Communicating Uncertainties: A Guide to Estimative Language and Confidence Levels in CTI Reporting.” Medium. December 12, 2023. https://medium.com/@orojcik/the-shades-of-doubt-a-guide-to-estimative-language-and-confidence-levels-in-cti-reporting-1545233f7470

28. Kent, S. 1964. (Declassified and Approved for Release, 2012). “Words of Estimative Probability.” Central Intelligence Agency (U.S.). Declassified and Approved for Release May, 4, 2012. https://www.cia.gov/readingroom/docs/CIA-RDP93T01132R000100020036-3.pdf

29. Berkowitz, B. (2003). “The Big Difference Between Intelligence and Evidence.” RAND. February 2, 2003. https://www.rand.org/pubs/commentary/2003/02/the-big-difference-between-intelligence-and-evidence.html

30. MarineTraffic, 2025. “<MELKART-5> IMO: 9130183.” MarineTraffic. Accessed 2025. https://www.marinetraffic.com/en/ais/details/ships/shipid:313507/mmsi:273418680/imo:9130183/vessel:MELKART_5

31. MarineTraffic, 2025. “<LEOPOLD ROSENFELDT> IMO: 8902670.” MarineTraffic. Accessed 2025. https://www.marinetraffic.com/en/ais/details/ships/shipid:153850/mmsi:219002761/imo:8902670/vessel:LEOPOLD_ROSENFELDT

32. Submarine Cable Map. 2025. “Svalbard Undersea Cable System.” TeleGeography Submarine Cable Map. Accessed 2025. https://www.submarinecablemap.com/submarine-cable/svalbard-undersea-cable-system

33. Frederiksen, M. 2024. “A Conversation with Prime Minister Mette Frederiksen of Denmark.” Council on Foreign Relations. July 9, 2024. https://www.cfr.org/event/conversation-prime-minister-mette-frederiksen-denmark

34. Hodges, B. 2025. “General Ben Hodges Commentary at Delphi Economic Forum, Greece 2025. Panel: Europe Under Attack, Russia’s Hybrid Activities & the Continent’s Muted Response.” Delphi Economic Forum. April 11, 2025. https://www.youtube.com/watch?v=-haXhA2j7K4

35. Landsbergis, G. 2024. “Why do we call it “Hybrid Warfare”?” Twitter. October 19, 2024. https://x.com/GLandsbergis/status/1847586513229377681?mx=2

36. Energy Union. 2025. “Energy Union.” European Council. 31 January 2025. https://www.consilium.europa.eu/en/policies/energy-union/

37. EU Third Energy Package. 2025. “Third Energy Package.” Thomson Reuters Practial Law. Accessed 2025. https://uk.practicallaw.thomsonreuters.com/w-001-8222?transitionType=Default&contextData=(sc.Default)&firstPage=true

38. Central Europe Pipeline System. 2021. “Central Europe Pipeline System (CEPS).” NATO. August 30, 2021. https://www.nato.int/cps/en/natohq/topics_49151.htm

39. Michel, C., Schmitt, B. L. 2022. “How to Stop Former Western Leaders from Becoming Paid Shills for Autocrats.” Foreign Policy. February 15, 2022. https://foreignpolicy.com/2022/02/15/gerhard-schroder-gazprom-russia-tony-blair/

40. Larsson, R. L. 2006. “Russia’s Energy Policy: Security Dimensions and Russia’s Reliability as an Energy Supplier.” FOI. March 2006. https://www.foi.se/rest-api/report/foi-r--1934--se

41. Associated Press. 2009. “Europeans Shiver as Russia Cuts Gas Shipments.” NBC News. January 6, 2009. https://www.nbcnews.com/id/wbna28515983

42. MacFarquhar, N. 2014. “Gazprom Cuts Russia’s Natural Gas Supply to Ukraine.” The New York Times. June 16, 2014. https://www.nytimes.com/2014/06/17/world/europe/russia-gazprom-increases-pressure-on-ukraine-in-gas-dispute.html

43. Talant, B. 2018. “Russia Retaliates Against Ukraine’s Court Win, Shuts Off Natural Gas Supplies Indefinitely.” Kyiv Post. March 2, 2018. https://www.kyivpost.com/post/10954

44. Schmitt, B. L. 2020. “Mr. Putin’s Not Quite 2020 Energy Vision.” CEPA. April 13, 2020. https://cepa.org/article/mr-putins-not-quite-2020-energy-vision/

45. Plucinska, J., Strzelecki, M. 2022. “Russia Warns Poland, Bulgaria of Gas Supply Cuts Wednesday.” Reuters. April 26, 2022. https://www.reuters.com/world/europe/russian-gas-supplies-poland-halted-polish-media-reports-2022-04-26/

46. Deutsche Welle. 2022. “Russia to Cut Nord Stream Gas Flows By Half.” Deutsche Welle. July 25, 2022. https://www.dw.com/en/russia-to-further-slash-gas-deliveries-to-germany-via-nord-stream-pipeline/a-62588620

47. Lawson, A. 2022. “Nord Stream 1: Gazprom Announces Indefinite Shutdown of Pipeline.” The Guardian. September 2, 2022. https://www.dw.com/en/russia-to-further-slash-gas-deliveries-to-germany-via-nord-stream-pipeline/a-62588620

48. BBC. 2022. “Russian Operator to Suspend Electricity Supply to Finland.” BBC. May 13, 2022. https://www.bbc.com/news/business-61442432

49. NRK TV. 2023. “Skyggekrigen: Brennpunkt.” NRK TV. Spring 2023. https://tv.nrk.no/serie/brennpunkt-skyggekrigen

50. Huppertz, C., et. al. 2024. “‘Make a Molotov Cocktail:’ How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder.” OCCRP. September 26 2024. https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder

51. University of Pennsylvania. 2025. “University of Pennsylvania Website.” University of Pennsylvania. Accessed 2025. https://www.upenn.edu/

52. Kleinman Center for Energy Policy. 2025. “Kleinman Center for Energy Policy.” Kleinman Center for Energy Policy. Accessed 2025. https://kleinmanenergy.upenn.edu/

53. Perry World House. 2025. “Perry World House.” Perry World House. Accessed 2025. https://perryworldhouse.upenn.edu/

54. Burke, L. E. 2025. “ Subsea fibre optic cable deliberately cut for the 2nd time between

N.S. and N.L." CBC. February 19, 2025. https://www.cbc.ca/news/canada/nova-scotia/bell-subsea-fibre-optic-cable-newfoundland-1.7461963

55. Antarctic Treaty System. 2025. "Antarctic Treaty System Website." Secretariat of the Antarctic Treaty. Accessed 2025. https://www.ats.aq/index_e.html

56. Perkins. R., Griffin, R. 2020. "Russia Stokes Political Tensions with Hunt for Antarctic Oil." S&P Global. February 21, 2020. https://www.spglobal.com/commodity-insights/en/news-research/latest-news/crude-oil/022120-russia-stokes-political-tensions-with-hunt-for-antarctic-oil

57. Schmitt, B. L. 2024. "TESTIMONY: Russia's Shadow War on NATO." U.S. Senate and House CSCE (U.S. Helsinki Commission). September 24, 2024. https://www.csce.gov/wp-content/uploads/2024/09/Schmitt-Testimony.pdf

58. U.S. Helsinki Commission. 2025. "HEARING:Russia's Shadow War on NATO." U.S. Senate and House CSCE (U.S. Helsinki Commission). September 24, 2024. https://www.csce.gov/hearings/russias-shadow-war-on-nato/

59. Starr, B. 2015. "U.S. Sensors Detect Russian Submarines Near Underwater Cables." CNN. October 28, 2015. https://www.cnn.com/2015/10/28/politics/russian-submarine-expansion-atlantic/index.html

60. Sutton, H. I. 2021. "Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables." Naval News. August 19, 2021. https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/

61. Zetter. K. 2016. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired. March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

62. Polityuk, P. 2016. "Ukraine investigates suspected cyber attack on Kiev power grid" Reuters. December 20, 2016. https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF/

63. Condliffe J. 2016. "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks" MIT Technology Review. December 22, 2016. https://www.technologyreview.com/2016/12/22/5969/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

64. Polityuk, P. 2016. "Ukraine investigates suspected cyber attack on Kiev power grid" Reuters. December 20, 2016. https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF/

65. CISA. 2021. "Cyber-Attack Against Ukrainian Critical Infrastructure." CISA. July 20, 2021. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

66. EURACTIV. 2015. "Russia accused of disrupting new energy link between Sweden and Lithuania." EURACTIV. May 4, 2015. https://www.euractiv.com/section/global-europe/news/russia-accused-of-disrupting-new-energy-link-between-sweden-and-lithuania/

67. Braw, E. 2015. "Balts Say Russian Navy Bullying Undersea Cable Crews." RFE/RL. May 5, 2015. https://www.rferl.org/a/russia-bullying-undersea-baltic-cable/26996165.html

68. Schmitt, B. L. 2024. "Wake Up NATO: It's Sabotage." CEPA. June 12, 2024. https://cepa.org/article/wake-up-nato-its-sabotage/

69. Bewarder, M. et. al. 2024. ""Der Ukrainekrieg ist hier längst angekommen."" Sueddeutsche Zeitung. May 21, 2024. https://www.sueddeutsche.de/politik/sabotage-russland-nato-pipeline-geheimdienst-1.7253897?reduced=true

70. Central Europe Pipeline System. 2021. “Central Europe Pipeline System (CEPS).” NATO. August 30, 2021. https://www.nato.int/cps/en/natohq/topics_49151.htm

71. YLE News. 2024. “Police suspect vandalism behind cell tower collapse in Häme.” YLE News. July 29, 2024. https://yle.fi/a/74-20101909

72. DPA. 2024. “German police say arson causes damage on Hamburg-Bremen train line.” DPA. July 29, 2024. https://www.yahoo.com/news/german-police-arson-causes-damage-152727728.html

73. Der Spiegel. 2024. “Drohnen über Industriepark – Behörden gehen von Spionageangriff aus” Der Spiegel. August 22, 2024. https://www.spiegel.de/panorama/drohnen-ueber-chemcoast-park-brunsbuettel-behoerden-gehen-von-spionageangriff-aus-a-45de7019-b74e-456c-807c-6a72b021363b

74. Quecke, F. 2024. “Suspected sabotage at regional German LNG pipeline might cause million-euro-damage – report.” Clean Energy Wire. January 9, 2024. https://www.cleanenergywire.org/news/suspected-sabotage-regional-german-lng-pipeline-might-cause-million-euro-damage-report

75. Staalesen. A. 2024. “Military experts suspect sabotage at Andøya.” The Barents Observer. September 13, 2024. https://www.thebarentsobserver.com/security/military-experts-suspect-sabotage-at-andoya/166701

76. Dobrokhotov, R. Weiss, M., Grozev, C. 2024. “Michelin Red Star: The Insider reveals identity of arrested Russian chef-agent who planned “destabilizing” acts at Paris Olympic Games” The Insider. July 25, 2024. https://theins.ru/en/politics/273350

77. Springe, I., Roonemaa, H. Weiss, M. 2024. “Exclusive: Inside Russia’s Latvian Sabotage Squad.” The Insider. July 10, 2024.

78. Jeznach, K., Grove, T. Pancevski, B. 2024. “The Misfits Russia Is Recruiting to Spy on the West” The Wall Street Journal. May 15, 2024. https://www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5?mod=hp_lead_pos9

79. Keate, N. 2024. “Brits charged with helping Russia after suspected arson attack on Ukraine-linked firm.” Politico. April, 26, 2024. https://www.politico.eu/article/britons-dylan-earl-jake-reeves-charged-help-russia-suspected-arson-attack-ukraine-national-security-cps/

80. Deutsche Welle. 2024. “Germany charges 3 over alleged Russia spying plot.” Deutsche Welle. December 30, 2024. https://www.dw.com/en/germany-charges-3-over-alleged-russia-spying-plot/a-71187987

81. Financial Times. 2024. https://www.ft.com/content/c88509f9-c9bd-46f4-8a5c-9b2bdd3c3dd3

82. Sheppard, L. R. et. al. 2019. “By Other Means Part II: Adapting to Compete in the Gray Zone.” CSIS. August 13, 2019. https://www.csis.org/analysis/other-means-part-ii-adapting-compete-gray-zone

83. NTV. 2024. “Oberleitung manipuliert - Vandalismus bremst Fernverkehr aus.” NTV. February 2, 2024. https://www.n-tv.de/wirtschaft/Vandalismus-bei-der-Bahn-Fernverkehr-zwischen-Koeln-und-Frankfurt-beeintraechtigt-article24707540.html

84. Reuters. 2024. “German union Verdi calls public transport strike for Friday” Reuters. January 29, 2024. https://www.reuters.com/business/autos-transportation/german-union-verdi-calls-public-transport-strike-friday-2024-01-29/

85. Marsh, S., Rinke, A. 2022. “‘Malicious and targeted’ sabotage halts rail traffic in northern

Germany." Reuters. October 8, 2022. https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/

86. Pancevski, B. 2024. "Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin" The Wall Street Journal. May 20, 2024. https://www.wsj.com/world/europe/europe-sees-signs-of-russian-sabotage-but-hesitates-to-blame-kremlin-72598d4b

87. RFE/RL. 2022. "German Rail Operator DB Blames 'Sabotage' After Stoppage Paralyzes North." RFE/RL. October 8, 2022. https://www.rferl.org/a/german-rail-operator-blames-sabotage-train-stoppage/32071278.html

88. Marsh, S., Rinke, A. 2022. "'Malicious and targeted' sabotage halts rail traffic in northern Germany." Reuters. October 8, 2022. https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/

89. Reuters. 2022. "No sign that foreign state was behind German rail sabotage, police say" Reuters. October 9, 2022. https://www.reuters.com/world/europe/no-sign-that-foreign-state-was-behind-german-rail-sabotage-police-2022-10-09/

90. Fokuhl, J. 2022. "Germany Won't Rule Out Foreign Country Role in Rail Sabotage." Bloomberg. October 10, 2022. https://www.bloomberg.com/news/articles/2022-10-10/germany-won-t-rule-out-foreign-country-role-in-rail-sabotage

91. Pearson, W. R., Schmitt, B. L. 2022. "2022 Is the Year for a Space Summit" Foreign Policy. January 1, 2022. https://foreignpolicy.com/2022/01/01/space-russia-anti-satellite-test-debris/

92. NATO. 2023. "The consultation process and Article 4" NATO. July 18, 2023. https://www.nato.int/cps/en/natohq/topics_49187.htm

93. NATO. 2023. "NATO stands up undersea infrastructure coordination cell." NATO. February 13, 2023. https://www.nato.int/cps/en/natohq/news_211919.htm

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

95. Schmitt, B. L., 2024. "An Energy Transition without National Security Won't Be "Just." Kleinman Center for Energy Policy. May 16, 2024. https://kleinmanenergy.upenn.edu/commentary/blog/an-energy-transition-without-national-security-wont-be-just/

96. United Nations Digital Library System. 2023. "Letter dated 10 July 2023 from the representatives of Denmark, Germany and Sweden to the United Nations addressed to the President of the Security Council." United Nations Security Council. July 10, 2023. S_2023_517-EN

97. Adomaitis, N. et. al. 2024. "Nord Stream: What's known about the mystery pipeline explosions?" Reuters. February 7, 2024. https://www.reuters.com/world/europe/qa-what-is-known-about-nord-stream-gas-pipeline-explosions-2023-09-26/

98. GEM Wiki. 2025. "Nord Stream Gas Pipeline." GEM Wiki. Accessed 2025. https://www.gem.wiki/Nord_Stream_Gas_Pipeline#:~:text=Nord%20Stream%20is%20an%20offshore,further%20connections%20in%20Western%20Europe

99. Wettengel, J. 2025. "Nord Stream 2 – Symbol of failed German bet on Russian gas." Clean Energy Wire. March 18, 2025. https://www.cleanenergywire.org/factsheets/gas-pipeline-nord-stream-2-links-germany-russia-splits-europe

100. GEM Wiki. 2025. "Nord Stream Gas Pipeline." GEM Wiki. Accessed 2025. https://www.gem.wiki/Nord_Stream_Gas_Pipeline#:~:text=Nord%20Stream%20is%20an%20offshore,further%20connections%20in%20Western%20Europe

101. Yaakoubi, A. E., Kahn, S. 2022. “Exclusive: Nord Stream 2 owner considers insolvency after sanctions” Reuters. March 1, 2022. https://www.reuters.com/markets/europe/exclusive-nord-stream-2-owner-considers-insolvency-after-pipeline-halt-sanctions-2022-03-01/

102. Chambers, M., Steitz, C. 2022. “Nord Stream 1 gas supply cut aimed at sowing uncertainty, Germany warns.” Reuters. June 15, 2022. https://www.reuters.com/business/energy/german-minister-accuses-russia-finding-excuse-cut-nord-stream-1-gas-2022-06-15/

103. Deutsche Welle. 2022. “Russia to cut Nord Stream gas flow by half.” Deutsche Welle. July 25, 2022. https://www.dw.com/en/russia-to-further-slash-gas-deliveries-to-germany-via-nord-stream-pipeline/a-62588620

104. Lawson, A. 2022. “Nord Stream 1: Gazprom Announces Indefinite Shutdown of Pipeline.” The Guardian. September 2, 2022. https://www.dw.com/en/russia-to-further-slash-gas-deliveries-to-germany-via-nord-stream-pipeline/a-62588620

105. Mason, J. 2022. “U.S. slaps sanctions on company building Russia’s Nord Stream 2 pipeline” Reuters. February 23, 2022. https://www.reuters.com/business/energy/us-plans-sanctions-company-building-russias-nord-stream-2-pipeline-cnn-2022-02-23/

106. Marsh, S., Chambers, M. 2022. “Germany freezes Nord Stream 2 gas project as Ukraine crisis deepens” Reuters. February 22, 2022. https://www.reuters.com/business/energy/germanys-scholz-halts-nord-stream-2-certification-2022-02-22/

107. Yaakoubi, A. E., Kahn, S. 2022. “Exclusive: Nord Stream 2 owner considers insolvency after sanctions” Reuters. March 1, 2022. https://www.reuters.com/markets/europe/exclusive-nord-stream-2-owner-considers-insolvency-after-pipeline-halt-sanctions-2022-03-01/

108. Escritt., T., Jacobsen, S. 2022. “Gas from Russia’s Nord Stream 2 pipeline leaks into Baltic Sea.” Reuters. September 26, 2022. https://www.reuters.com/business/energy/pressure-defunct-nord-stream-2-pipeline-plunged-overnight-operator-2022-09-26/

109. GEUS (Denmark). 2022. “GEUS har registreret rystelser i Østersøen” GEUS (Denmark). September 27, 2022. https://www.geus.dk/om-geus/nyheder/nyhedsarkiv/2022/sep/seismologi

110. Bryant, M. 2023. “Key details behind Nord Stream pipeline blasts revealed by scientists.” The Guardian. September 26, 2023. https://www.theguardian.com/business/2023/sep/26/nord-stream-pipeline-blasts-key-details-revealed-by-scientists

111. Jyllands-Posten. 2022. “Rystelser i undergrunden overvåges døgnet rundt efter gaslæk” Jyllands-Posten. September 28, 2022. https://jyllands-posten.dk/indland/ECE14446472/rystelser-i-undergrunden-overvaages-doegnet-rundt-efter-gaslaek/

112. Danish Defence. 2022. “Gas Leak in the Baltic Sea.” Danish Defence. September 27, 2022. https://www.forsvaret.dk/en/news/2022/gas-leak-in-the-baltic-sea/

113. Associated Press. 2022. “Denmark says Nord Stream 1 pipelines stop leaking.” Associated Press. October 2, 2022. https://apnews.com/article/russia-ukraine-business-baltic-sea-government-and-politics-1de252c6b188f3dccad82633ae156c7c

114. Newsbase. 2024. “The Nord Stream mystery: a timeline.” BNE Intellinews. August 27, 2024. https://www.intellinews.com/the-nord-stream-mystery-a-timeline-340361/

115. Harris, S. et. al. 2023. “Investigators skeptical of yacht’s role in Nord Stream bombing.” The Washington Post. April 3, 2023. https://www.washingtonpost.com/national-security/2023/04/03/nord-stream-bombing-yacht-andromeda/

116. Struckmeier, L. 2024. “How did divers manage to blow up the Nord Stream pipeline? We went down to the spot to find out.” CBC. August 18, 2024. https://www.cbc.ca/news/

investigates/nord-stream-pipeline-explosion-ukraine-diver-1.7296527

117. Harris, S. et. al. 2023. “Investigators skeptical of yacht’s role in Nord Stream bombing.” The Washington Post. April 3, 2023. https://www.washingtonpost.com/national-security/2023/04/03/nord-stream-bombing-yacht-andromeda/

118. Hersh, S. 2023. “How America Took Out the Nord Stream Pipeline.” Substack. February 8, 2023. https://seymourhersh.substack.com/p/how-america-took-out-the-nord-stream

119. Diehl, J. et al. 2024. “Wie ein ukrainisches Geheimkommando Nord Stream sprengte.” Der Spiegel. November 20, 2024. https://www.spiegel.de/politik/deutschland/nord-stream-wie-ein-ukrainisches-geheimkommando-pipelines-sprengte-a-7aceb6f8-060f-4d29-9ddd-582dfdaf4ac6

120. Pancevski, B. 2024. “A Drunken Evening, a Rented Yacht: The Real Story of the Nord Stream Pipeline Sabotage” The Wall Street Journal. August 14, 2024. https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c

121. Corera, G. 2023. “Nord Stream: Report puts Russian navy ships near pipeline blast site.” BBC. May 3, 2023. https://www.bbc.com/news/world-europe-65461401

122. NRK TV. 2023. “Skyggekrigen: Brennpunkt.” NRK TV. Spring 2023. https://tv.nrk.no/serie/brennpunkt-skyggekrigen

123. AFP. 2023. “Russian navy ship photographed near Nord Stream pipelines before blasts.” The Guardian. April 28, 2023. https://www.theguardian.com/world/2023/apr/28/russian-navy-vessel-seen-near-nord-stream-pipelines-days-before-blasts

124. Lehto, E., Ringstom, A. 2022 “Nord Stream investigation finds evidence of detonations, Swedish police say.” Reuters. October 6, 2022. https://www.reuters.com/world/europe/kremlin-says-russia-not-invited-nord-stream-investigation-2022-10-06/

125. Barchart. 2025. “Dutch TTF Gas Historical Prices.” Barchart. Accessed 2025. https://www.barchart.com/futures/quotes/TG*0/historical-prices?orderBy=contractExpirationDate&orderDir=asc

126. Balmaced, M. et. al. 2022. “Europe’s Gas Crisis and Russian Energy Politics: Experts Respond.” Harvard-Ukrainian Research Institute. Fall 2022. https://www.huri.harvard.edu/tcup-commentary/europes-gas-crisis-russian-energy-politics

127. Barchart. 2025. “Dutch TTF Gas Jun 25.” Barchart. Accessed 2025. https://www.barchart.com/futures/quotes/TG*1

128. Stanford Sanctions Group. 2022. “Statement on European Energy Security and Siemens Turbines.” International Working Group on Russia Sanctions (Stanford University). July 2022. https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2023-04/russia_sanctions_working_group_european_energy_security_and_siemens_turbines_statement.pdf

129. Reed, S. 2022. “Russia Halts Natural Gas Flows to Germany Again.” The New York Times. August 30, 2022. https://www.nytimes.com/2022/08/31/business/russia-natural-gas-germany.html

130. EURACTIV. 2022. “EU lacking Russian gas? It should then launch Nord Stream 2, Putin says.” EURACTIV. July 20, 2022. https://www.euractiv.com/section/eet/news/eu-lacking-russian-gas-it-should-then-launch-nord-stream-2-putin-says/

131. Sauer, P. 2022. “Russia will not resume gas supplies to Europe until sanctions lifted, says Moscow.” The Guardian. September 5, 2022. https://www.theguardian.com/world/2022/sep/05/russia-will-not-resume-gas-supplies-to-europe-until-sanctions-lifted-says-moscow

132. U.S. Department of State. 2022. “The United States Supports Canada’s Decision to Reutrn Turbine to Germany.” U.S. Department of State. July 2022. https://www.state.gov/the-united-states-supports-canadas-decision-to-return-turbine-to-germany/

133. Reuters. 2022. “Technical problem with Nord Stream 1 a Russian pretext - German EconMin” Reuters. June 30, 2022. https://www.reuters.com/markets/europe/technical-problem-with-nord-stream-1-russian-pretext-german-econmin-2022-06-30/

134. Schmitt, B. L. 2022. “Don’t Stop Now — Tech Sanctions Can Wreck Putin’s War Machine.” CEPA. July 28, 2022. https://cepa.org/article/dont-stop-now-tech-sanctions-can-wreck-putins-war-machine/

135. Platt, B. 2022. “Canada Will Return Sanctioned Nord Stream Turbine to Germany.” Bloomberg. July 9, 2022. https://www.bloomberg.com/news/articles/2022-07-09/canada-to-return-sanctioned-nord-stream-turbine-to-germany?leadSource=uverify%20wall

136. U.S. Department of State. 2021. “Joint Statement of the United States and Germany on Support for Ukraine, European Energy Security, and Our Climate Goals.” U.S. Department of State. July 2021. https://www.state.gov/joint-statement-of-the-united-states-and-germany-on-support-for-ukraine-european-energy-security-and-our-climate-goals/

137. Bielieskov, M. 2024. “Time to make Russia worry about the West’s red lines in Ukraine.” Atlantic Council. September 17, 2024. https://www.atlanticcouncil.org/blogs/ukrainealert/time-to-make-russia-worry-about-the-wests-red-lines-in-ukraine/

138. Bolton, E. et. al. 2022. “Bots and disinformation: how twitter users reacted to the nord stream gas leaks.” Digitalis. December 2022. https://digitalis.com/news-research/bots-disinformation-twitter-nord-stream-gas-leaks-reaction/

139. C-SPAN. 2022. “President Biden on Nord Stream 2 if Russia Invades Ukraine: “We will bring an end to it.”” C-SPAN. February 7, 2022. https://www.c-span.org/video/?c5000795/president-biden-nord-stream-2-russia-invades-ukraine-we-bring-end-it

140. Gardner, T., Cowan, R. 2022. “Cruz’s Nord Stream 2 sanctions bill fails in U.S. Senate.” Reuters. January 13, 2022. https://www.reuters.com/world/us/us-democrats-slam-cruz-nord-stream-2-sanctions-bill-ahead-vote-2022-01-13/

141. Faulconbridge, G., Ravikumar. S. 2022. “Russia says UK navy blew up Nord Stream, London denies involvement.” Reuters. October 29, 2022. https://www.reuters.com/world/europe/russia-says-british-navy-personnel-blew-up-nord-stream-gas-pipelines-2022-10-29/

142. Bowman, R. 2022. “Putin says the CIA blew up the Nord Stream pipeline but REFUSES to provide any evidence to back up his claims because it ‘very difficult to defeat the US propaganda machine’” Daily Mail. February 8, 2024. https://www.dailymail.co.uk/news/article-13063585/Putin-says-CIA-blew-Nord-Stream-pipeline-REFUSES-provide-evidence.html

143. Socor, V. 2006. “RUSSIAN ENERGY SUPPLY CUTOFF TO GEORGIA: ANOTHER WAKE-UP SIGNAL TO THE WEST” Jamestown Foundation. January 23, 2006. https://jamestown.org/program/russian-energy-supply-cutoff-to-georgia-another-wake-up-signal-to-the-west/

144. Pannier, B. 2009. “Pipeline Explosion Raises Tensions Between Turkmenistan, Russia.” RFE/RL. April 14, 2009. https://www.rferl.org/a/Pipeline_Explosion_Stokes_Tensions_Between_Turkmenistan_Russia/1608633.html

145. Friedrich, S., Neumueller, J. “North European Gas Pipeline.” CIVPRO. 2007. https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/peti20080129_northgaspipeline_/PETI20080129_NorthGasPipeline_en.pdf

146. RFE/RL. 2018. “U.S. Warns Russian-German Gas Pipeline Risks Triggering Sanctions.” RFE/RL. May 18, 2018. https://www.rferl.org/a/us-warns-russian-german-nord-stream-2-pipeline-risks-trigger-sanctions-security-concern-oudkirk/29233548.html

147. CGS S21 Expert Group. 2021. “Report “CONCEALED ACTIVITY OF THE RUSSIAN NAVY IN THE AREA OF THE NORD STREAM 2 PIPELINE AT COMPLETION STAGE” Strategy XXI Think Tank. October 13, 2021. https://geostrategy.org.ua/en/analysis/reports-and-presentations/report-concealed-activity-of-the-russian-navy-in-the-area-of-the-nord-stream-2-pipeline-at-completion-stage

148. Gjerding, S., Elkjaer, B. 2023. “Forsvaret bekræfter: Rusland havde specialfartøj nær Nord Streams sprængningspunkt.” Information DK. April 28, 2023. https://www.information.dk/indland/2023/04/forsvaret-bekraefter-rusland-specialfartoej-naer-nord-streams-spraengningspunkt

149. Corera, G. 2023. “Nord Stream: Report puts Russian navy ships near pipeline blast site.” BBC. May 3, 2023. https://www.bbc.com/news/world-europe-65461401

150. Schmitt, B. L. 2020. “Hot Issue – They’re Gonna Need A Bigger Boat: The Curious Voyage of the Akademik Cherskiy.” The Jamestown Foundation. March 31, 2020. https://jamestown.org/program/hot-issue-theyre-gonna-need-a-bigger-boat-the-curious-voyage-of-the-akademik-cherskiy/

151. Schmitt, B. L. 2020. “REPORT - Don’t Cross the Streams: Why the Ghost of Putin’s Pipeline Continues to Haunt Transatlantic Security.” Harvard-Ukrainain Researach Institute. May 21, 2020. https://www.huri.harvard.edu/sites/g/files/omnuum4931/files/huri/files/ns2_report_21_may_2020.pdf

152. Wyrzykowsk, K. 2022. “Nord Stream 2-linked company leases warehouse in Rostock harbour in defiance of sanctions.” Poland at Sea. May 5, 2022. https://www.polandatsea.com/nord-stream-2-linked-company-leases-warehouse-in-rostock-harbour-in-defiance-of-sanctions/

153.Solbakken, C. F. 2022. “Methane leaks from Nord Stream: A serious pollution event.” NILU. September 29, 2022. https://nilu.com/2022/09/methane-leaks-from-nord-stream-a-serious-pollution-event/

154. Benshoff, L. 2022. “The Nord Stream pipelines have stopped leaking. But the methane emitted broke records.” NPR. October 4, 2022. https://www.npr.org/2022/10/04/1126562195/the-nord-stream-pipelines-have-stopped-leaking-but-the-methane-emitted-broke-rec

155. Poursanidis, K. et al. 2024. “World’s largest natural gas leak from nord stream pipeline estimated at 478,000 tonnes.” iScience ScienceDirect, Volume 27, Issue 1. January 19, 2024. https://www.sciencedirect.com/science/article/pii/S2589004223028493

156. United Nations Environmental Program. 2023. “Impact of the Nord Stream gas leak on methane emissions.” United Nations Environmental Program. February 20, 2023. https://www.unep.org/technical-highlight/impact-nord-stream-gas-leak-methane-emissions

157. Reuters. 2023. “Swedish greenhouse gases up 7% in 2022 due to Nord Stream leak.” Reuters. December 14, 2023. https://www.reuters.com/business/environment/swedish-greenhouse-gases-up-7-2022-due-nord-stream-leak-2023-12-14/

158. RFE/RL. 2022. “Danish Island Near Nord Stream Leaks Suffers Unexplained Power Outage.” RFE/RL. October 10, 2022. https://www.rferl.org/a/nord-stream-denmark-power-outage/32073269.html

159. The Sun. 2022. “After Nord Stream, Power Cut to Danish Island Bornholm.” The Sun. October 10, 2022. https://thesun.my/home-news/after-nord-stream-power-cut-to-danish-island-bornholm-IC9949479

160. Reuters. 2024. “Sweden rejects Baltic Sea wind farms, citing defence concerns.” Reuters. November 4, 2024. https://www.reuters.com/business/energy/sweden-rejects-baltic-sea-wind-farms-citing-defence-concerns-2024-11-04/

161. UNFCCC. 2025. “United Nations Climate Change.” UNFCCC. Accessed 2025. https://unfccc.int/

162. Newsbase. 2024. “The Nord Stream mystery: a timeline.” BNE Intellinews. August 27, 2024. https://www.intellinews.com/the-nord-stream-mystery-a-timeline-340361/

163. Siebold, S., Alkoussa, R. 2023. “West cautious on Nord Stream blasts, Germany confirms raiding suspect ship.” Reuters. March 8, 2023. https://www.reuters.com/world/europe/germany-says-nord-stream-attacks-may-be-false-flag-smear-ukraine-2023-03-08/

164. Frenzel, M., Maier, S. 2023. ““Russland war beteiligt” Nord-Stream-Sprengung: Die Spur führt nach Moskau.” NTV. July 11, 2023. https://www.n-tv.de/politik/Nord-Stream-Sprengung-Die-Spur-fuehrt-nach-Moskau-article24250566.html

165. Burgess, M. 2022. “‘Dark Ships’ Emerge From the Shadows of the Nord Stream Mystery.” Wired. November 11, 2022. https://www.wired.com/story/nord-stream-pipeline-explosion-dark-ships/

166. Struckmeier, L. 2024. “How did divers manage to blow up the Nord Stream pipeline? We went down to the spot to find out.” CBC. August 18, 2024. https://www.cbc.ca/news/investigates/nord-stream-pipeline-explosion-ukraine-diver-1.7296527

167. Coleman, Z., Lefebvre, B. 2022. “‘Everything is pointing to Russia’: U.S., EU officials on edge over pipeline explosions.” Politico. September 28, 2022. https://www.politico.com/news/2022/09/28/nord-stream-pipeline-explosions-eu-00059262

168. Harris, S. et. al. 2023. “U.S. had intelligence of detailed Ukrainian plan to attack Nord Stream pipeline.” The Washington Post. June 6, 2023. https://www.washingtonpost.com/national-security/2023/06/06/nord-stream-pipeline-explosion-ukraine-russia/

169. Yaffa, J. 2025. “The Adventures of a Ukrainian Intelligence Officer.” The New Yorker. February 24, 2025. https://www.newyorker.com/magazine/2025/03/03/the-adventures-of-a-ukrainian-intelligence-officer

170. Pancevski, B. 2024. “A Drunken Evening, a Rented Yacht: The Real Story of the Nord Stream Pipeline Sabotage” The Wall Street Journal. August 14, 2024. https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c

171. Jensen, S. G. 2025. “Alle troede, Putins fangarme ind i tysk politik var kappet for bestandigt. Men: »Mosvka-forbindelsen« lever stadig.” Berlinske (Denmark). March 24, 2025. https://www.berlingske.dk/internationalt/alle-troede-putins-fangarme-ind-i-tysk-politik-var-kappet-for

172. Yoke, H. 2025. “Revealed: Russia’s secret war in UK waters.” The Times (U.K.) April 5, 2025. https://www.thetimes.com/uk/defence/article/russia-secret-war-uk-waters-submarines-dpbzphfx5

173. Space Norway. 2025. “Space Norway Website.” Space Norway. Accessed 2025. https://spacenorway.com/

174. Schia, N. N., et. al. 2023. “The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?” NUPI (Norway). January 2023. https://www.nupi.no/content/pdf_preview/26372/file/NUPI_Policy_Brief_1_23_Schia_Gjesvik_R%C3%B8dningen-FERDIG.pdf

175. Gulldahl, H., Eriksen, I. 2024. “This is what the damaged Svalbard cable looked like

when it came up from the depths." NRK (Norway). May 27, 2024. https://www.nrk.no/tromsogfinnmark/this-is-what-the-damaged-svalbard-cable-looked-like-when-it-came-up-from-the-depths-1.16895904

176. Pearson, W. R., Schmitt, B. L. 2022. "2022 Is the Year for a Space Summit" Foreign Policy. January 1, 2022. https://foreignpolicy.com/2022/01/01/space-russia-anti-satellite-test-debris/

177. Fredriksen, B. 2022. "Kabelmysteriene." NRK (Norway). July 1, 2022. https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-forbrudd-1.16007084

178. Camut, N. 2023. "Russia uses civilian boats to spy in the North Sea, joint report says." Politico. April 19, 2023. https://www.politico.eu/article/russia-uses-civilian-ships-to-spy-in-the-north-sea-reports/

179. Staalesen, A. 2024. ""This is a watershed moment." Norwegian intelligence warns about mounting Russian threats." The Barents Observer. February 12, 2024. https://www.thebarentsobserver.com/security/this-is-a-watershed-moment-norwegian-intelligence-warns-about-mounting-russian-threats/102623

180. Kalstad, L. M. 2022. "Her er det russiske «spionskipet» på tokt i Nordsjøen." NRK (Norway). October 5, 2022. https://www.nrk.no/rogaland/forsvaret-folger-med-pa-russiske-fartoy-langs-norskekysten-1.16127644

181. USGS. 2025. "SvalSat." USGS. Accessed 2025. https://eros.usgs.gov/earthshots/svalsat

182. O'Niell, P. H. 2022. "Russia hacked an American satellite company one hour before the Ukraine invasion." MIT Technology Review. May 10, 2022. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

183. Knack, A., et. al. 2024. "Enhancing the Cyber Resilience of Offshore Wind." CETAS. June 15, 2024. https://cetas.turing.ac.uk/publications/enhancing-cyber-resilience-offshore-wind

184. Whitaker, B. 2023. "All at sea: Seymour Hersh and his Nord Stream sabotage story." Medium. April 6, 2023. https://brian-whit.medium.com/all-at-sea-seymour-hersh-and-his-nord-stream-sabotage-story-b467e17a1728

185. Sullivan, A. 2025. "Nord Stream: Could Germany return to Russian gas imports?" Deutsche Welle. April 25, 2025. https://www.dw.com/en/nord-stream-russia-gas-germany-energy/a-72329126

186. Datawrapper. 2025. "Datawrapper Website." Datawrapper. Accessed 2025. https://www.datawrapper.de/

187. Submarine Cable Map. 2025. "Svalbard Undersea Cable System." TeleGeography Submarine Cable Map. Accessed 2025. https://www.submarinecablemap.com/submarine-cable/svalbard-undersea-cable-system

P0. Elgar, E. 1899. "The Swimmer." Oxford International Song Festival. Accessed 2025. https://oxfordsong.org/song/the-swimmer

P1. Danish Defence. 2022. "Gas Leak in the Baltic Sea." Danish Defence. September 27, 2022. https://www.forsvaret.dk/en/news/2022/gas-leak-in-the-baltic-sea/

P2. General view of the Meeting of the North Atlantic Council at the level of Heads of State and Government at the 75th NATO Leaders Summit in Washington, D.C. (July 2024) / CREDIT: NATO Flickr, PHOTOS: Taken 10 July 2024 Album URL: https://www.flickr.com/photos/nato/albums/72177720318646862/with/53848639816

Location: Washington, DC

P3. General view of the Meeting of the North Atlantic Council at the level of Heads of State and Government at the 75th NATO Leaders Summit in Washington, D.C. (July 2024) / CREDIT: NATO Flickr, PHOTOS: Taken 10 July 2024 Album URL: https://www.flickr.com/photos/nato/albums/72177720318646862/with/53848639816
Location: Washington, DC

P4. Danish Prime Minister Mette Frederiksen (center) along with Czech President Petr Pavel (left) and Estonian Prime Minister Kaja Kallas (right) at the meeting of the North Atlantic Council at the level of Heads of State and Government at the 75th NATO Leaders Summit in Washington, D.C. (July 2024) / CREDIT: NATO Flickr PHOTOS: Taken 10 July 2024 Album URL: https://www.flickr.com/photos/nato/albums/72177720318646862/with/53848639816
Location: Washington, DC

P5. [FIGURE 01] Illustration of the Five Primary Pillars of Contemporary European Energy Security. FIGURE DESIGN: B. L. Schmitt / TEMPLATE AND ILLUSTRATION CREDIT: Petr Vaclavek, Tuna salmon, Icons-studio, SkyLine, Genestro, Dewi, AxelBlogoodf – stock.adobe.com

P6. Naval sonar equipment demonstration during NATO exercise Dynamic Monarch 24, held off the Norwegian Coast. (September 2024) / DESIGN: B. L. Schmitt / PHOTO CREDIT: NATO Flickr PHOTOS: Taken on 10 Sep 2024 Album URL: https://www.flickr.com/photos/nato/albums/72177720321785750/with/54125271865/
Location: “Off the Norwegian Coast”

P7. A Finnish Navy crew member looks through binoculars during Exercise Freezing Winds 24 in the Baltic Sea. (November 2024) PHOTOS Uploaded: 09 Dec 2024 Album URL : https://www.flickr.com/photos/nato/albums/72177720322456500/
LOCATION: Baltic Sea Region

P8 [FIGURE 03] Map and timeline of impacted nations and regions for incidents and trends that serve as the primary research case studies of the Underwater Mayhem project. Figure Design: B. L. Schmitt / Template and Illustrations: korkun, stockdevil, S_E – stock.adobe.com

P9 [FIGURE 04] a reproduction of the metric set forth in a U.S. National Intelligence Council Intelligence Community Assessment from 10 March 2021, and provides the specific estimative language for the judgements that appear in this series roughly mapped onto the percentage of likelihood that is meant to be conveyed. Figure Design: B. L. Schmitt as adapted from an Unclassified U.S. National Intelligence Council Intelligence Community Assessment document from 10 March 2021.

P10. Royal Danish Navy Frigate <HDMS TRITON> on patrol as a part of Joint Arctic Command Denmark near the coastline of Greenland. (November 2022) / DESIGN: B. L. Schmitt / PHOTO CREDIT: NATO Flickr
PHOTOS: Taken 06 Nov 2022
Album URL: https://www.flickr.com/photos/nato/albums/72177720306352604/with/52717156881
Location: Arctic Ocean off the coast of Greenland

P11. Swedish Naval CB-90 fast assault boats operating on the Norwegian coastline near Tovik, Norway before NATO Exercise Nordic Response 24. (February 2024) / PHOTO CREDIT: NATO FlickrP11 PHOTOS: Taken 29 Feb 2024
Album URL: https://www.flickr.com/photos/nato/albums/72177720315238282/
Location: North Sea near Tovik Norway

P12. The authors recommending energy policies.. (TOP) Prof. Michał Kurtyka celebrating the close of COP24 after serving as COP President in Katowice, Poland. (2018) (MIDDLE) Prof. Alan Riley lecturing on European energy law in Oslo, Norway. (2018) (BOTTOM) Dr. Benjamin L. Schmitt testifies before the joint U.S. House and Senate Commissionm on Security and

Cooperation in Europe (U.S. Helsinki Commission) on Capitol Hill, Washington, D.C. (2024) / PHOTO CREDITS: (TOP) UNFCCC Flickr, (MIDDLE) A. Riley, (BOTTOM) U.S. Helsinki Commission Website on September 2024 Hearing: "Russia's Shadow War on NATO."
PHOTO: Taken 15 December 2018
Album URL: https://www.flickr.com/photos/unfccc/with/47472826471
Location: Katowice Poland
COP24 President Michal Kurtyka jump after approval of the Paris Agreement Work Programme
https://www.csce.gov/hearings/russias-shadow-war-on-nato/

P13. NATO special forces divers participate in exercise BOLD MACHINA 24 focused on protecting critical subsea infrastructure from hybrid threats near La Spezia, Italy (November 2024) / PHOTO CREDIT: NATO Flickr
PHOTOS TAKEN: 13 Nov 2024
Album URL: https://www.flickr.com/photos/nato/albums/72177720322392691/
Location: La Spezia, Italy

P14. German Naval team deploying the unmanned underwater vehicle SEAFOX-I into the Baltic Sea during Exercise Freezing Winds 24 focused on the protection of subsea energy and critical infrastructure in the Baltic Sea. (December 2024) / PHOTO CREDIT: NATO Flickr

PHOTOS Uploaded: 09 Dec 2024 (Cite all as December 2024)
Album URL : https://www.flickr.com/photos/nato/albums/72177720322456500/
LOCATION: Baltic Sea Region

P16. [FIGURE 02] Illustration of the increasing scope and impact of Russian energy weaponization, which has over the years included threats of energy cutoffs, energy lawfare, strategic corruption and elite capture, but has increased most recently to physical sabotage of energy and critical infrastructure across NATO member state territories as well as overt kinetic military strikes against civilian energy and critical infrastructure installations across Ukraine. Figure Design: B. L. Schmitt / Template and Illustration: Petr Vaclavek, Terriana, Iconsstudio, SkyLine, Genestro, Dewi, Cetacons – stock.adobe.com / Media Headlines: New York Times, Reuters, The Guardian, The Washington Post | New York Times (https://www.nytimes.com/2022/04/23/world/europe/schroder-germany-russia-gas-ukraine-war-energy.html); Reuters "EU Unbundling" (https://www.reuters.com/business/energy/eu-court-dismisses-russias-nord-stream-2-contest-eu-unbundling-rules-2024-11-27/); CNBC (https://www.cnbc.com/2022/04/12/ukraine-says-russian-cyberattack-sought-to-shut-down-energy-grid.html); The Guardian (https://www.theguardian.com/world/2022/jul/15/gas-blackmail-how-putins-weaponised-energy-supplies-are-hurting-europe); Reuters "Sabotage" (https://www.reuters.com/world/europe/norways-spy-chief-sees-russia-more-likely-attempt-sabotage-2024-09-10/); The Washington Post (https://www.washingtonpost.com/world/2022/11/23/ukraine-infrastructure-damage-electricity-water-russia/)

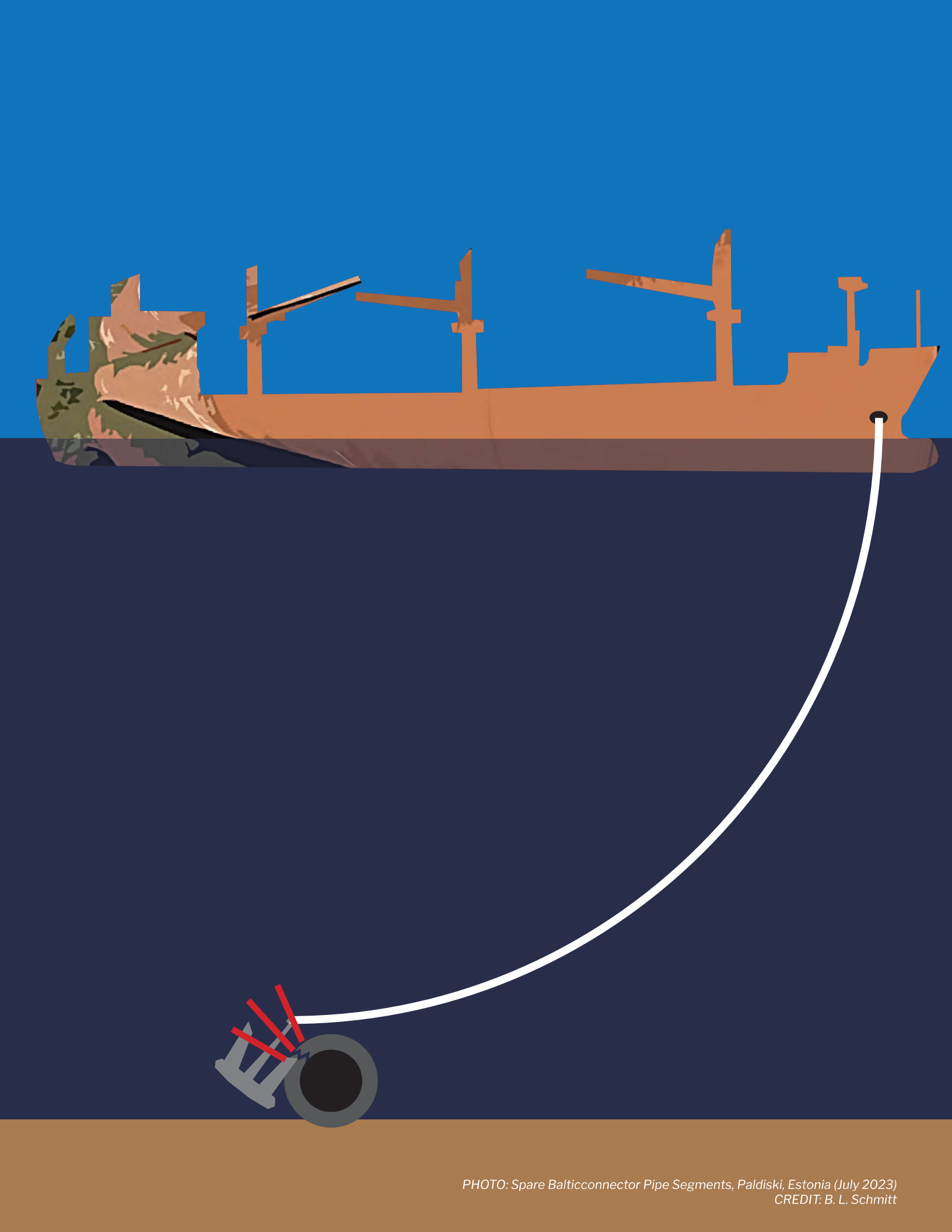


PHOTO: Spare Balticconnector Pipe Segments, Paldiski, Estonia (July 2023)
CREDIT: B. L. Schmitt

University of Pennsylvania
Philadelphia, Pennsylvania

www.upenn.edu