DIIS REPORT 2024: 06

Invisible frontlines

SAFEGUARDING THE EUROPEAN ENERGY INFRASTRUCTURE

Veronika Slakaityte and Izabela Surwillo

The report is written by Veronika Slakaityte, Analyst and Izabela Surwillo, Senior Researcher, DIIS, and is published by DIIS.

DIIS · Danish Institute for International Studies
Gl. Kalkbrænderi Vej 51A
DK-2100 Copenhagen, Denmark
Tel: +45 32 69 87 87
E-mail: diis@diis.dk
www.diis.dk

Layout and figures: Lone Ravnkilde.
Cover illustration: Cecilie Castor von Spreckelsen
Printed in Denmark by Johansen Grafisk
All DIIS Reports are printed on Ecolabel and FSC certified paper

ISBN 978-87-7236-136-9 print
ISBN 978-87-7236-137-6 pdf

DIIS publications can be downloaded free of charge or ordered from www.diis.dk.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

PT	Advanced persistent threat
BVs	Biomimetic vehicles
CEE	Central and Eastern Europe
EC	European Commission
EEZ	Exclusive economic zone
EU	European Union
EUCO	European Council
EUMSS	EU Maritime Security Strategy
EP	European Parliament
FSRU	Floating storage and regasification unit
GUGI	Glavnoye Upravleniye Glubokovodnykh Issledovaniy (Main Directorate of Deep-Sea Research)
HVs	Hybrid vehicles
LNG	Liquefied natural gas
MARCOM	NATO Maritime Command
NATO	North Atlantic Treaty Organization
NORSAR	Norwegian Seismic Array
NPP	Nuclear power plant
NS1	Nord Stream 1
NS2	Nord Stream 2
RES	Renewable energy sources
ROVs	Remotely operated vehicles
SCADA	Supervisory control and data acquisition
UAVs	Unmanned aerial vehicles
UGVs	Unmanned ground vehicles
UMVs	Unmanned maritime vehicles
UN	United Nations
UNCLOS	UN Convention on the Law of the Sea
USVs	Unmanned surface vehicles
UUVs	Unmanned underwater vehicles
WBIED	Water borne improvised explosive device

PREFIXES AND UNITS OF POWER AND ENERGY USED IN THE REPORT

Symbol	Name	Value	
W(h)	Watt (hour)	10^0 W	1 W
kW(h)	Kilowatt (hour)	10^3 W	1,000 W
MW(h)	Megawatt (hour)	10^6 W	1,000,000 W
GW(h)	Gigawatt (hour)	10^9 W	1,000,000,000 W
TW(h)	Terawatt (hour)	10^{12} W	1,000,000,000,000 W
Area			
m^2	Square meters	10^0 m^2	1 m^2
Natural gas/LNG			
m^3	Cubic meters	10^0 m^3	1 m^3
mcm (/y)	Million cubic meters (/per year)	10^6 m^3	1,000,000 m^3
bcm(/y)	Billion cubic meters (/per year)	10^9 m^3	1,000,000,000 m^3
Expression and comparison of different sources			
toe	Tonne of oil equivalent	10^0 toe	1 toe
Ktoe	Kilo-tonne of oil equivalent	10^3 toe	1,000 toe
Mtoe	Mega-tonne of oil equivalent	10^6 toe	1,000,000 toe

EXECUTIVE SUMMARY

The Russian invasion of Ukraine in February 2022 has significantly altered the geopolitical landscape, underscoring critical vulnerabilities in energy infrastructure to both physical and cyber threats. As Europe transitions towards a greener, more interconnected and digitalised energy system, the emergence of hybrid threats poses a substantial risk to its critical infrastructure. Recent cyberattacks on European energy firms and physical incidents, such as the Nord Stream pipeline explosions and Balticconnector damage, underscore the urgent need to bolster security measures against potential attacks and sabotage, especially in maritime zones where new energy projects are increasingly located.

This report examines the evolution of threats to the critical European energy infrastructure amidst shifting geopolitical dynamics and technological advances. It highlights the multifaceted nature of these vulnerabilities, influenced by political tensions, economic dependencies, technological weaknesses and environmental challenges. The strategic use of energy dependencies and sophisticated hybrid attacks necessitate adaptive strategies that address both overt and covert dimensions of security.

The European Union (EU) and North Atlantic Treaty Organization (NATO) have actively engaged in developing reactive measures to enhance infrastructure resilience. These efforts encompass enhanced international cooperation, security measures and technological innovation, aiming for a balanced approach that integrates immediate defensive capacities with long-term strategic planning. However, the effectiveness of these initiatives is challenged by fragmented governance, the high costs of surveillance and protection technologies, and the dual-use nature of modern technology, which can be employed both to defend and exploit existing vulnerabilities.

Addressing these challenges requires a nuanced policy approach that acknowledges the complex role of infrastructure in geopolitical and security contexts. Recommendations for future action include enhanced backup and repair capacities, conducting regular risk assessments, improving surveillance and monitoring, strengthening physical and cyber security measures, fostering collaboration among stakeholders, establishing clear governance structures and considering legal protections. The segmentation of maritime zones based on threat levels and strategic importance is also suggested to optimise resource allocation.

INTRODUCTION

The Russian invasion of Ukraine in February 2022 radically altered continental geopolitics and highlighted some of the key contemporary physical and cyber threats to critical energy infrastructure. During the conflict, the shelling of Ukrainian nuclear power plants (NPPs) by Russian forces not only raised nuclear safety concerns across the region but also marked a deliberate strategy to inflict substantial harm on the Ukrainian population by targeting the energy infrastructure. Various aggressive tactics included missile and drone strikes that damaged heating and power facilities and disrupted the energy supply, as well as cyberattacks targeting Ukrainian power grid (Vatman and Hart 2024). The intentional damage inflicted on the Ukrainian energy system highlighted that infrastructures are not just physical assets but significant elements in global politics, playing a pivotal role in shaping international relations (see Bueger, Liebetrau and Stockbruegger 2023).

While the European energy system is unlikely to experience threats of the same magnitude and intensity, the rise in hybrid threats targeting Europe's critical infrastructure is of a growing concern. The current energy-climate crisis necessitates an expedited shift away from fossil fuels and a mass scale-up of renewable energy technologies accompanied by increased interconnectedness and the digitalisation of the European energy system. This amplifies emerging security risks in relation to both potential cyber and physical attacks. The recent surge in cyberattacks targeting European energy companies – along with significant incidents like the 2022 Nord Stream pipeline explosions, the 2023 damages to Balticconnector and underwater cables – emphasise the urgent need to bolster security measures to shield Europe's critical energy infrastructure. This need becomes even more pressing considering the location of many new projects in the maritime zones. Given the

inherent difficulties in monitoring and securing maritime areas, the increasing European dependence on offshore and subsea infrastructure (e.g. wind farms, pipelines, power cables) significantly heightens its susceptibility to sabotage and espionage.

In the face of these multifaceted threats, the EU and NATO have been developing an array of reactive measures. These efforts are aimed at enhancing the resilience and security of Europe's critical energy infrastructure through enhanced international cooperation, more effective policymaking on national and regional levels, and technological innovation. Multiple challenges remain, however, as fragmented governance, unclear legal provisions and high costs of physical and cyber protective measures hinder this process.

This report examines the vulnerabilities of the critical European energy infrastructure by tracing their evolution against the backdrop of evolving geopolitical tensions, existing economic dependencies and technological innovation. The study highlights how this complexity renders the development of a nuanced approach for effective identification, evaluation and mitigation of potential threats challenging. The analysis starts by examining the historical backdrop of European energy vulnerabilities, exploring how varying threat perceptions have influenced diverse energy policies and approaches to safeguarding energy infrastructure. It then proceeds to an in-depth analysis of the evolving security threats confronting the European energy sector in both physical and cyber realms, paying special attention to energy projects sited in the maritime zones. In conclusion, the report addresses some of the pressing contemporary dilemmas in critical energy infrastructure protection and provides a series of policy recommendations for future action.

The analysis broadly covers the countries of the Energy Community.[1] The overall approach to energy security in Europe is discussed along the classic East–West divide. The empirical focus is kept mostly on Eastern and Northern Europe, which stems from the prevalence of security incidents in these regions coupled with the anticipation of substantial challenges ahead. Foremost among these challenges is the planned strategic scale-up of offshore energy projects in the Baltic and North Seas that necessitates closer scrutiny and a more proactive policy approach.

HISTORICAL CONTEXT OF THE GEOPOLITICAL TENSIONS IN EUROPE

The Russian invasion of Ukraine in February 2022 marked a critical juncture, prompting the EU to adopt a more robust stance on both its security and energy security policy. This shift did not take place in a vacuum, however, as many of the current challenges have been developing in the region for decades. This section delves into the historical context shaping the current European security dilemmas, ultimately informing different national approaches to energy security and energy infrastructure protection.

Increasing Russian activities – signalling escalating tensions – were observed well before the Russian invasion of Ukraine in February 2022, especially in Eastern Europe and the EU's neighbours to the East.

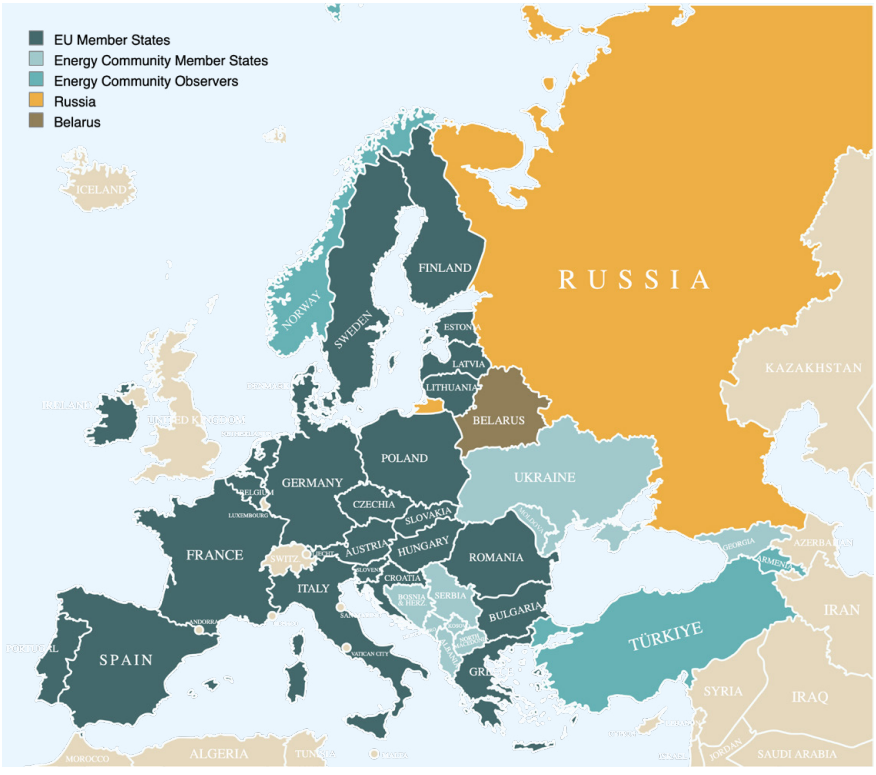
Following the 2008 war between Russia (alongside the self-proclaimed republics of South Ossetia and Abkhazia, backed by Moscow) and Georgia, the Russian military contingent was permanently deployed to both breakaway statelets (Ponomarev 2023). The diplomatic relations between Georgia and Russia have not been restored since. Six years later, Ukrainian pro-Western aspirations gave rise to conflict with Moscow, with Russia annexing the Crimean Peninsula and supporting pro-Russian separatists in Ukraine's Donbas region – a conflict that ultimately culminated in a full-scale Russian invasion in 2022.

Although less dramatic, the security situation has also been deteriorating in the region more broadly. Mainland Russia directly neighbours three EU Member States: Estonia, Finland and Latvia. Additionally, an exclave known as Kaliningrad Oblast is squeezed between Lithuania and Poland. Isolated incidents have increased in the

region in recent years, including breaches of territorial waters and national airspace, ghost ships etc. This trend has escalated further since 2022. In 2023, NATO air patrols were most active over the Baltic Sea region, where they conducted over 300 interception missions to counter Russian aircraft approaching Alliance airspace (NATO 2023c). Such incursions have been most frequent in the vicinity of the Baltic States (DW News 2021).

Moreover, the increasingly pro-Russian regime in Belarus has prompted security measures to be implemented alongside the Latvian–, Lithuanian– and Polish–Belarusian borders. Currently, the border security on the EU's eastern flank offers among the most advanced physical and virtual barriers, including unmanned aerial vehicles, drones, radars and detection cables. Two events in 2021 induced the securitisation of the border: joint Russian–Belarusian military exercises, 'West' (org. Запад/Zapad), which involved 200,000 troops simulating a hypothetical NATO

Figure 1. Geopolitical energy dynamics in Europe



Source: Based on data from the Energy Community

invasion of Belarus (Rumer 2021); and especially, the coordinated influx of immigrants from Middle Eastern and North African countries (see Surwillo and Slakaityte 2022). While these developments preceded the February 2022 Russian invasion of Ukraine, the situation has further deteriorated since that time. The presence of the Wagner Group in Belarus in 2023 (Humphries and Macfie 2023) triggered discussions regarding the full closure of the EU–Belarusian border.

The security situation has been escalating in both the physical and cyber realms. Notably, Russia regards cyberattacks as a wider military and foreign policy instrument in times of peace – and especially in times of war. The cyber capacities are used for two primary objectives aimed at information warfare and technical operations, both of which have been increasingly prominent in Europe. For instance, the 2007 cyberattacks on Estonia, following a dispute over a Soviet war memorial, targeted key Estonian digital infrastructure including government, financial and media websites, significantly disrupting the country's digital operations (Herzog 2011). This incident is widely regarded as one of the first major state-sponsored cyberattacks and underscores the Russian approach to using cyber capabilities as a tool for strategic influence in international relations. Although the rest of Europe also registered multiple interceptions in the cyber realm, cybersecurity first topped the EU political agenda in 2020, culminating with cyber sanctions against several Russian, Chinese and North Korean hackers (European Commission 2023b).

Unsurprisingly, responding to this geopolitical context, a number of strategic security centres were established in the region, including the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, Strategic Communications Centre of Excellence in Latvia, the Energy Security Centre of Excellence in Lithuania, Military Police and Counter Intelligence centres of excellence in Poland, as well as the European Centre of Excellence for Countering Hybrid Threats in Finland.

Over time, European states also became increasingly concerned with how growing Russian military capacities and expertise can be used for targeted attacks on critical infrastructure in the maritime zones. This expertise was developed over the years with the help of a deep-sea research agency under the command of the Armed Forces of the Russian Federation – the so-called GUGI (Glavnoye Upravleniye Glubokovodnykh Issledovaniy[2]) – based in Olenya Bay, Kola Peninsula and elsewhere. With a fleet consisting of highly specialised nuclear-powered submarines, ships for oceanographic research and undersea drones (commonly known as UUVs). GUGI is considered to operate the world's largest fleet of manned deep-sea vessels. Together with the naval special forces from the Baltic Fleet, GUGI has

enough power not only to disrupt but also to destroy critical infrastructure. GUGI focuses primarily on reconnaissance activities, such as tapping or cutting communication cables, installing movement sensors and collecting ship, plane and satellite wreckage – both Russian and foreign – to obtain intelligence. It also specialises in so-called 'grey operations' that are generally subdivided into three categories, although no details are disclosed: 1. Ensuring the operation of the Poseidon vehicles (an autonomous nuclear-powered unmanned underwater vehicle capable of delivering both conventional and nuclear warheads) and their carriers; 2. Deployment and maintenance of the Skif autonomous underwater launch system for intercontinental missiles; and 3. Development of the Harmony hydroacoustic tracking system, which can detect and classify surface and underwater targets (Ramm 2016; Гавриленко 2019). With 'eyes and ears in the ocean', GUGI carries out operations of national importance on a daily basis and 'all the more priceless is their contribution to the country's security and defence of its national interests' (Гавриленко 2019).

Being among the most classified operations, GUGI was a highly secretive organisation prior to 2014, when the annexation of Crimea and subsequent geopolitical turmoil increased the presence of GUGI's vessels, attracting Western attention (Giles and Hartmann 2021).

Figure 2. The Russian naval ensign atop the K-18 Karelia, a formidable nuclear-powered ballistic missile submarine, anchored in the Murmansk Region of Russia

Photo: Lev Fedoseyev/TASS, April 2018. Available in the public domain via the Official United States Air Force Website. Accessed on February 22, 2024, https://www.960cyber.afrc.af.mil/News/Photos/igphoto/2002879315/

The increasing Russian military capacities and expertise, capable of targeting critical infrastructure in maritime zones, were recognised in Europe before 2022. For instance, at the 2016 Warsaw Summit, NATO established seven Baseline Requirements for national resilience in alignment with Article 3 of the North Atlantic Treaty. These requirements, including 'resilient energy supplies', were designed to enhance the Alliance's foresight. NATO prioritised the robustness of critical energy infrastructure against unpredictable security challenges (NATO 2019). The commitment reflected a collective acknowledgment of the evolution of the strategic environment and the indispensable role of resilience in civil preparedness, particularly within the energy sector, which is fundamental to national security and societal stability. Despite such measures, however, the energy crisis following the war in Ukraine revealed that many European countries were still not fully prepared for the unprecedented challenges it posed. This proved to be the case especially in Western Europe, as the growing regional tensions and historical energy dependencies in the Central and Eastern Europe (CEE) region had prompted many Eastern European states to securitise their approaches to energy policy early on.

ENERGY POLITICS AND DEPENDENCIES

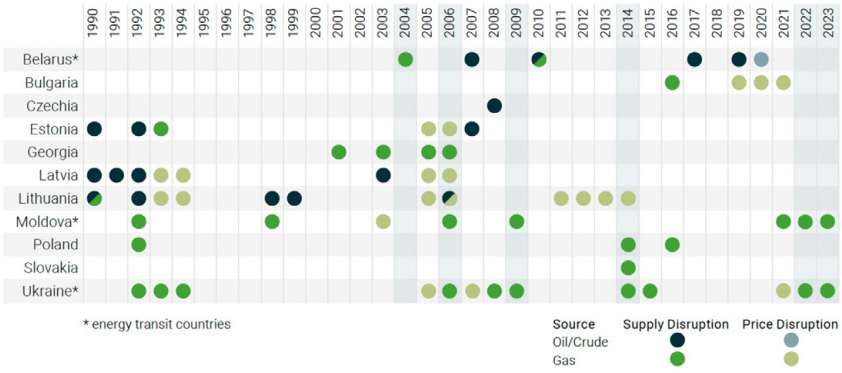
The increasingly tense geopolitical situation in the CEE contributed to the ever-growing perception of the Russian threat to the region over the last three decades. This perception affected the general foreign policy and security approaches of many states, and it was particularly visible in the energy sector, where many Soviet-era dependencies continued to play out.

Moscow has been weaponizing energy resources and key energy infrastructure for economic and political gains since the early 1990s. This tactic was enabled by the concentration of strategic fossil fuel resources in mainland Russia and a complex network of dependencies created by the oil and gas pipelines connecting former Soviet/satellite states with Russia as well as with each other. The remaining Soviet era infrastructure locked-in the newly independent states in a continuous dependency on Russian energy resources. The period following the collapse of the Soviet Union marked a significant political transition in CEE, as countries aimed to establish market economies despite their institutional weaknesses. This left them particularly vulnerable to Moscow's use of energy exports as a foreign policy tool, as the Kremlin's direct political and military control over their 'near abroad' was masterfully being replaced with non-military means.

Following the collapse of the Soviet Union, the physical disruptions of the oil and gas supply – of varying scale and scope – were regularly taking place in the Russian 'near abroad', frequently preceded or accompanied by disputes over Russian pricing policy (see Figure 3).

These incidents would typically correlate with political developments in the energy-importing states that contradicted Russian interests, although Moscow would habitually deny any connection. Among the more prominent examples were the tactics employed in 1992-93, when the newly restored Baltic States requested that Russian military forces leave their territory, and Moscow responded by periodically shutting off the oil supply and limiting gas flows. Later incidents include a gas cut-off in 2006, when Russia and Ukraine clashed over prices in a new political context with pro-Western President Viktor Yushchenko in office; 2006 gas blackmail against Georgia, when Gazprom more than doubled the prices not long after the country expressed its interest in joining the NATO alliance; gas price spikes for Lithuania leading up to 2014 in response to the Lithuanian state buying out Gazprom's shares in the domestic gas company and constructing the national liquefied natural gas (LNG) terminal; or Gazprom limiting the gas supply to Moldova in 2021 and causing a domestic energy crisis that coincided with the election of pro-EU Maia Sandu as president of Moldova. These are but a few instances.

Figure 3. Known and/or likely instances of political motivations influencing Russian energy supply and pricing



Source: Slakaityte and Surwillo 2024. Figure from DIIS Policy Brief: Energy as a weapon, January 2024. Illustration by Studio Jakob Glad.

The vulnerability of many European countries resulted from overdependence on Russian energy imports together with the entrenched Russian presence in the European energy sector. Gazprom, for example, held stakes in several national

gas companies across Europe, including EuRoPol Gaz in Poland, Vemex in Czechia and Slovakia, Overgas Inc. in Bulgaria, Panrusgas in Hungary, Gasum Oy in Finland, Eesti Gaas in Estonia, Wingas GmbH in Germany, Amber Grid and Lietuvos Dujos in Lithuania, and (UK) Limited in the UK (European Parliament 2018, 21; Schubert, Pollak and Brutschin 2014). In the post-Soviet region, Gazprom's ownership of transmission networks (through stakes in integrated national gas companies) solidified its market dominance by encompassing supply, operations and transportation of natural gas through the pipelines. While countries have reduced their dependencies over the years – for instance, by enacting new legislation following the Third Energy Package (e.g. Lithuania's full ownership unbundling, challenging Gazprom's vertical control of gas operations) – the increased security concerns after 2022 further motivated them to seize control over strategic assets in the national energy sectors. Nevertheless, Gazprom continues to be a significant stakeholder in Latvian Latvijas Gāze and Hungarian PanRusGaz. Additionally, Gazprom subsidiaries like Centrex hold stakes in several European firms. Notable examples include the aforementioned Hungarian PanRusGaz as well as the Serbian Yugorosgaz (Elliot 2023b). Through these indirect investments, Gazprom consequently maintains a substantial presence in the European gas sector. Gazprom also co-owns vital energy infrastructure, including key import pipelines (e.g. Nord Stream, Yamal-Europe, Blue Stream, TurkStream).

SECURITY-CENTRIC ENERGY POLICIES

Past experience with energy blackmail influenced the regional perception of energy security in the former Soviet space, which was starkly different from most of Western Europe (see Slakaityte, Surwillo, and Berling 2023). In the latter, efforts were centred on balancing the energy trilemma of sustainability, affordability and security of supply. As such, energy policy in Western Europe increasingly pivoted towards the green transition, emphasising investments in low-carbon technologies. Simultaneously, expanding cooperation with Russia in sectors like gas (notably in Germany and Austria) and nuclear energy (as in Finland) has primarily been viewed through an economic lens. Meanwhile, many CEE states emphasised the geopolitical dimension of security of supply and sought to diversify away from Russia through investments in alternative supply routes such as new gas pipelines, oil and liquefied natural gas terminals and electricity grid interconnections. In the CEE region – with some notable exceptions, such as Hungary – energy policy has been increasingly treated as a security issue since the 1990s. In other words, many CEE states have 'securitised' their energy policy over the years.

COMMON INDICATORS OF THE SECURITISATION OF ENERGY POLICY IN CEE

Energy policy and national security: Energy security equated with 'energy sovereignty' and 'energy independence'. Diversification of energy supply away from Russia becomes a matter of national security, with diversification projects having a strong political rationale that trumps purely economic considerations.

Energy infrastructure projects: Emphasis on large-scale power generation units that the state can control and protect (e.g. LNG terminals, NPPs).

Political and security oversight of energy policy: Energy predominantly governed by high-level political and security authorities. This underscores the elevation of energy policy to the security realm.

High-security risks in energy infrastructure: Protection strategies for critical energy infrastructure now actively encompass measures against significant security threats, including espionage, sabotage and terrorist attacks.

The divergent geopolitical threat perceptions throughout Europe have been closely aligned with distinct approaches to energy policy and protection of critical energy infrastructure more specifically. CEE states (e.g. Poland, the Baltic States) have frequently contemplated dystopian scenarios that would extend well beyond unintentional hazards (e.g. technical failures, natural disasters) and encompass potential incidents of espionage, sabotage or terrorist attacks. Consequently, these states have often incorporated vigorous security measures both in their scenario planning and the protection of infrastructure projects. For instance, the Lithuanian LNG Independence project was a matter of national security, developed by a handful of experts and politicians under the close supervision of the prime minister at the time (2011–14), eventually docked near a naval base. Besides strategic precautions, the infrastructure (i.e. the floating storage and regasification unit (FSRU) and the terminal itself) has been under the protection of armed forces since operations started in 2014 (Pryšmantas 2023). Following the war in Ukraine, the LNG terminal in Lithuania has been under protection of a special 24/7 rapid response team, a soon-to-be-installed anti-drone system (Ibid.) and a re-established Coast Guard Frontier District (BNS 2023a). Responding to the latest escalation with the Balticconnector pipeline in October 2023, Lithuanian authorities announced that underwater surveillance systems will be installed to increase the underwater monitoring capability, allowing the detection of unmanned objects and management of risks (BNS 2023b). Similarly, energy policy was securitised in Poland, with security considerations being the primary driver behind construction of the LNG terminal in

Świnoujście and Baltic Pipe connector with Norway via Denmark. The Polish Internal Security Agency has also overseen the development of the first NPP in Poland, ensuring non-interference of foreign actors and interests, while the LNG terminal has been guarded 24/7 by the Polish Border Guard and police since Russian invaded Ukraine in 2022 (Lesman 2023).

Prior to 2022, energy infrastructure protective measures in most Northern and Western European countries revolved around mitigating non-intentional hazards, such as technical errors, accidents and disasters trigged by natural events. The Nordic states have become known for their 'resilience over protection' model, which views infrastructure not as critical individual units but as integral parts of vital societal functions (Pursiainen 2018); the approach focuses less on the 'neutralization of threats, risks, and vulnerabilities' (2008/114/EC 2008) and more on the 'mitigative and preparedness activities' (Pursiainen 2018: 634). The notion of resilience provides answers to emerging and unforeseen threats. It also shifts the focus of security away from extensive planning, instead placing reliance on individuals' abilities to engage in self-governance. In essence, security solutions predominantly originate at the individual and organisational levels as opposed to government and political initiatives (Berling and Lund Petersen 2020). However, this emphasis on micro-level planning may lead to difficulties in seamlessly integrating resilience management into pragmatic operational structures (Pursiainen 2018).

In Europe (with the notable exception of CEE countries), more dystopian scenarios have traditionally been confined to military simulations and trials. However, the integration of these simulations into civilian emergency response protocols has been notably slow. This delay is attributed to a myriad of factors: the stark differences between military and civilian planning frameworks, bureaucratic inertia and the significant challenges of adapting highly specialised military scenarios to fit broader civilian emergency preparedness measures (Bollen and Kalkman 2022; Lillywhite and Wakefield 2021; Moore et al. 2010). Effective integration necessitates cross-sector collaboration and a thorough re-evaluation of existing protocols to ensure they are both comprehensive and adaptable to the dynamic nature of threats. Historically, the potential consequences of intentional physical destruction to critical energy infrastructure projects were often overlooked. The events of 2022 have impacted this perspective, leading to a gradual realignment of views on energy security across Europe. This realignment now places greater emphasis on the geopolitical dimensions, highlighting the increasingly hard security threats to critical energy infrastructure, although outliers in perception and policy preparedness remain.

EVOLVING THREATS: ENERGY SECURITY POST-2022

As the Russian war in Ukraine progressed, the Russians began employing a new strategy. The previously dominant energy blackmail tactic, which was marked by a high degree of deniability, gave way to a more direct and forceful approach. In late 2022, Moscow started a deliberate systematic mass-scale attack on the Ukrainian energy system, which was accompanied by new rhetoric. From deputies in the Duma to political researchers under the Russian Ministry of Foreign Affairs, the narrative shifted to 'bombing Ukraine into the Stone Age' by 'knocking out all Ukrainian plants', also noting that 'nuclear power plants should not be destroyed, but their substations should be' (Жданов 2022). According to Sergey Mironov from the 'Just Russia – for Truth' party, it was 'time to smash the entire infrastructure of Ukraine' (Головатенко 2022). Threats were scaled up from manipulation, and acts of sabotage and physical destruction became a reality. During to the 2022–23 heating season, in October–November alone, there were 69 missile and drone attacks on Ukrainian critical energy infrastructure, which devastated the power grid and energy supply. Damage to heat and power plants deprived many Ukrainians of access to electricity and water (due to electricity-powered pumps) in the middle of the cold season. An assessment from April 2023 estimated the damage to Ukrainian energy infrastructure at USD 10 billion, with Ukrainian electricity production capacity reduced by 61% – 22 out of 36 power generation plants damaged, destroyed or inaccessible – and a significant part of the heating infrastructure in war-affected territories broken beyond repair (Cilliers 2023). Despite these setbacks, the Ukrainian power supply system has demonstrated remarkable resilience during the war with Russia. It has been able to quickly rebuild and restore vital functions after both cyber and kinetic attacks, ensuring that essential services continued under challenging conditions. This resilience has been critical in mitigating the impact on the population,

although the damage still deprived or limited access to energy for 12 million people (Ibid.). Furthermore, around 200 kilometres of gas pipelines were damaged during military operations, while the shelling of Ukrainian NPPs and Russian occupation of the largest NPP, Zaporizhzhia, raised international concerns regarding nuclear safety (Task Force 2023, 7-14).

In autumn 2023, Russia resumed its tactic ahead of another winter season, with the Ukrainian side better prepared to counter the attacks, albeit in a weaker position due to the damage already inflicted to its energy infrastructure (Balmforth and Richardson 2023). Notably, some recent analyses pointed out how Russia kept changing its tactics in Ukraine to maximise the damage caused, with the use of different types of air-based and sea-based long-range missiles, kamikaze drones and guided air bombs alongside its standard use of artillery and rocket launcher systems in the frontline regions (Task Force 2023, 4).

The deliberate targeting of Ukrainian critical infrastructure by Russia since the February 2022 invasion, coupled with Moscow's use of energy blackmail against Western Europe, and an increase in hybrid threats to Europe's critical infrastructure – marked notably by cyberattacks and intentional physical damage –have triggered a gradual shift in threat perceptions within the EU. This shift has resulted in a re-evaluation and reprioritisation of energy security priorities. Overall, Western states became more appreciative of the geopolitical aspect of the security of supply, while Eastern states found themselves requiring an accelerated roll-out of low-carbon energy to complement their fossil fuel diversification policies going forward. The REPowerEU Action Plan (European Commission 2022) adopted in May 2022 placed emphasis on the diversification of the energy supply (especially away from Russian fossil fuels) and accelerating the energy transition. After banning Russian coal imports in August 2022 and most oil products in 2022/23, the EU aims to phase out Russian gas by 2027 – a more challenging task for some land-locked states that opt for a longer timeline, as accessing LNG in large quantities is difficult without port access. The new EU binding target for renewable energy from November 2023 (42.5% by 2030, with the aspiration to reach 45%) also translates into an almost two-fold increase in the existing share of renewable energy by 2030 (European Commission 2023a). Moreover, the revised EU energy policy necessitates substantial investments in various energy projects, including offshore wind farms, gas and hydrogen infrastructure, as well as electricity cables. This strategy aims to foster increased regional interconnectivity and digitalisation, enhancing the collective security of the energy supply. Unique challenges accompany these advances in both

physical and cyber security, particularly in monitoring current and proposed critical energy infrastructure. Consequently, a robust 'hard security' approach is needed to address these emerging risks.

Navigating the new risks: the case of Nord Stream and Balticconnector pipelines

While the direct attacks on Ukrainian energy infrastructure highlighted the extent to which the latter can become a target, recent damage to the NS1, NS2 and Balticconnector pipelines illustrates how the attacks on critical energy infrastructure risk becoming the 'new normal' – also in the rest of Europe. In 2024, almost 18 months after the Nord Stream pipeline explosions, the speculation over who is responsible for the explosions remains ongoing. Germany, Denmark and Sweden have initiated individual investigations into the attack and continue to cooperate on the matter. Moscow, Kyiv (Инь and Чжон 2023), London and Washington (Faulconbridge and Ravikumar 2022) have all publicly denied any responsibility. Following widespread Western suspicions regarding Russian involvement, some Russian sources tried to play the reverse tactic and pointed a finger at the US as the most plausible destructor (Инь and Чжон 2023), with the Russian state media even implying that Denmark fears joint investigation with Russia of 'the terrorist attacks', as it would risk compromising its relationship with the US (Риа Новости 2023). In February 2023, Russia also requested a special United Nations commission to

Figure 4. The damaged Balticconnector gas pipeline, October 2023

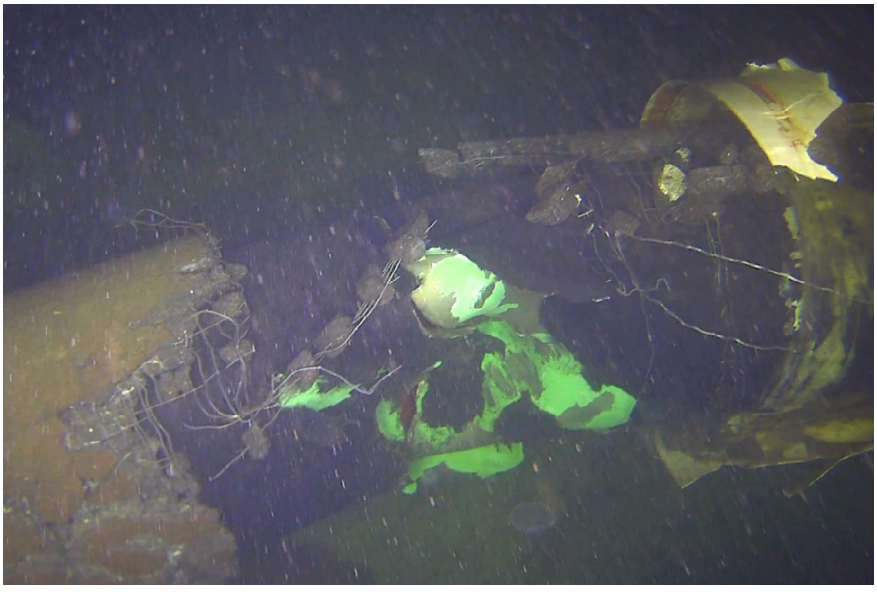
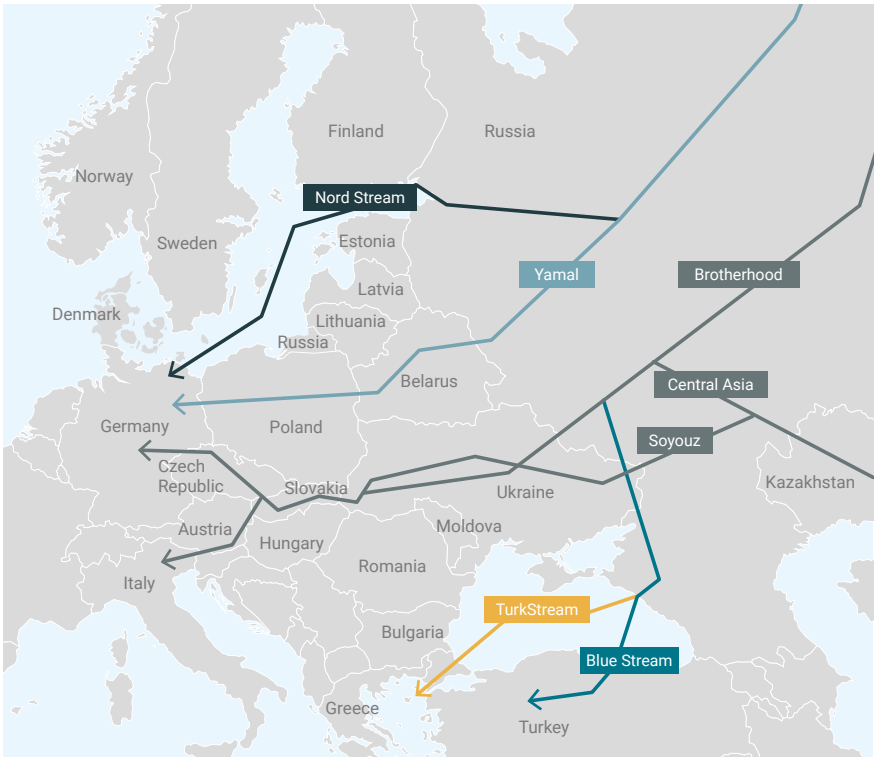


Photo and source: The Finnish Border Guard.

investigate the sabotage (DeYoung 2023). While the international community has concluded that the explosions were intentional, the party responsible for the sabotage remains unclear. In early February 2024, Sweden dropped the investigation due to insufficient evidence, followed by Denmark later that month.

On 7 October 2023, the Finnish authorities confirmed that the Balticconnector pipeline connecting Finland with the European gas market was leaking alongside damaged telecommunications cables in the Estonian exclusive economic zone connecting the Baltic State with Finland and Sweden. The Finnish side believes the damage was intentional. As noted by the Finnish Prime Minister Petteri Orpo, the damage 'could not have been caused by normal pipeline use or pressure fluctuations' (Armstrong and Sri-Pathma 2023). An investigation by Finnish authorities identified a Chinese container ship, which is believed to have dragged its anchor across more than 180 kilometres of the Baltic seabed, causing damage to the pipeline and surrounding cables (Chiappa and Ngendakumana 2023). Finnish

Figure 5. Key west-bound natural gas pipelines carrying Russian fossil fuels



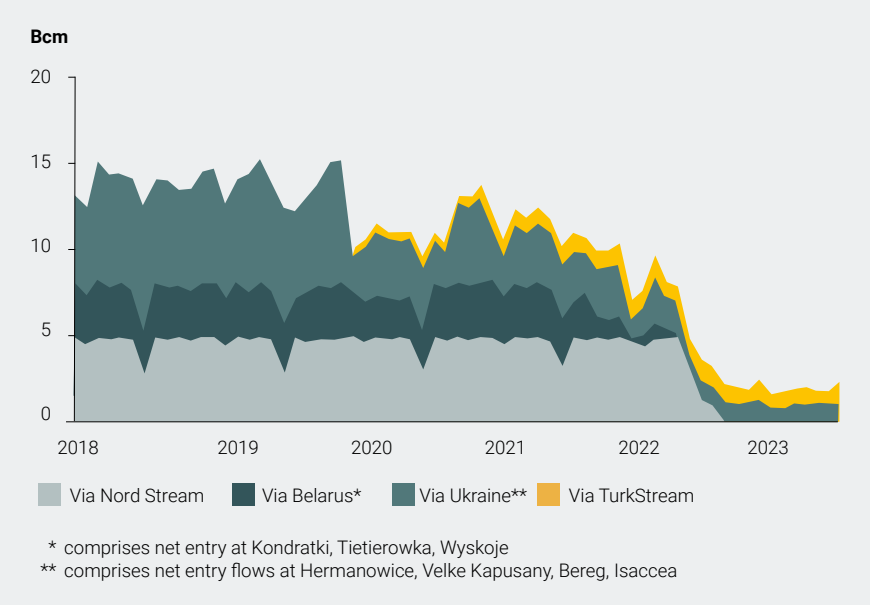
Source: Euranet Plus (2022).
https://euranetplus-inside.eu/europe-braces-for-a-new-phase-in-the-war-in-ukraine/

Minister of European Affairs Anders Adlercreutz has expressed doubts regarding the accidental nature of the undersea gas pipeline damage, indicating potential intent. Both Finland and Estonia have contacted Chinese authorities to request their cooperation in the ongoing investigation (Ibid.).

Despite high security alerts raised across the region in relation to both incidents, security of supply was not significantly affected. The NS1 and NS2 explosions did not lead to immediate natural gas shortages, as the import volumes through NS1 had already stopped in late August 2022 (Statista 2023a), and NS2 never received its final certification, following its suspension on 22 February 2022 in response to Russian recognition of Donetsk and Luhansk as independent republics (Marsh and Chambers 2022). While the Yamal pipeline is no longer carrying volumes as of April 2023, Russian gas continues to reach Europe through the Brotherhood, Soyuz and TurkStream pipelines (see Figure 5).

In the Balticconnector case, despite several months needed to repair the damage (Ritzau 2023), Finland will have sufficient gas supply due to the new LNG infrastructure developed at an accelerated rate post-2022 (onshore LNG Hamina and an FSRU unit leased jointly with Estonia).

Figure 6. Russian gas volumes flowing to Europe



Source: Elliot (2023a).
https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/natural-gas/080223-russian-gas-flows-to-europe-hit-seven-month-high-on-turkstream-record

Although historically low, the Russian natural gas flow to Europe in 2023 was rather stable and followed seasonal patterns (Figure 6). However, the gas transit agreement between Russia and Ukraine is about to expire in December 2024, and Ukraine has no intentions of renewing it, therefore leaving only one vein open for Russian gas imports to Europe – through Turkey.

HYPERCONNECTIVITY OR HYPERSENSITIVITY?

Physical attacks are currently not the only risks facing the European critical energy infrastructure. Amidst the escalation of the war in Ukraine, the already rapid pace of technological advancement, coupled with the shift towards decarbonising industries, has further accelerated the new era of hyperconnectivity. This evolution means that modern energy systems (e.g. solar, wind) are increasingly interconnected through a network of devices, communication cables, satellites and other technologies. This heightened interconnectivity exposes these systems to unprecedented vulnerabilities.

In the Thales Data Threat Report published in March 2023, the global share of cyberattacks targeting the EU increased from 10% to 47% following the war in Ukraine; furthermore, 61% of the global cyberattacks have been of Russian origin (Vincent and Pietralunga 2023). In Ukraine alone, Microsoft captured 237 Russian cyber operations just weeks before the full-scale invasion (Willett 2022). While so-called information warfare is often thought to be a modern phenomenon, in fact, all that has changed over centuries are the means and scope of it. Historians have registered a continuous tradition of Russian military and intelligence using information operations. While in the earlier days, such tactics required the destruction of broadcast facilities or interruption of telegraph exchanges (e.g. the attempted communist coup d'état in Estonia in 1924), today's hyperconnectivity of infrastructure introduces vulnerabilities that could trigger a domino effect, causing multiple socio-technological ecosystems to collapse (Giles and Hartmann 2021). Such ecosystems encompass digital networks, public services, economic functions and social structures, leaving them particularly susceptible to cascading failures.

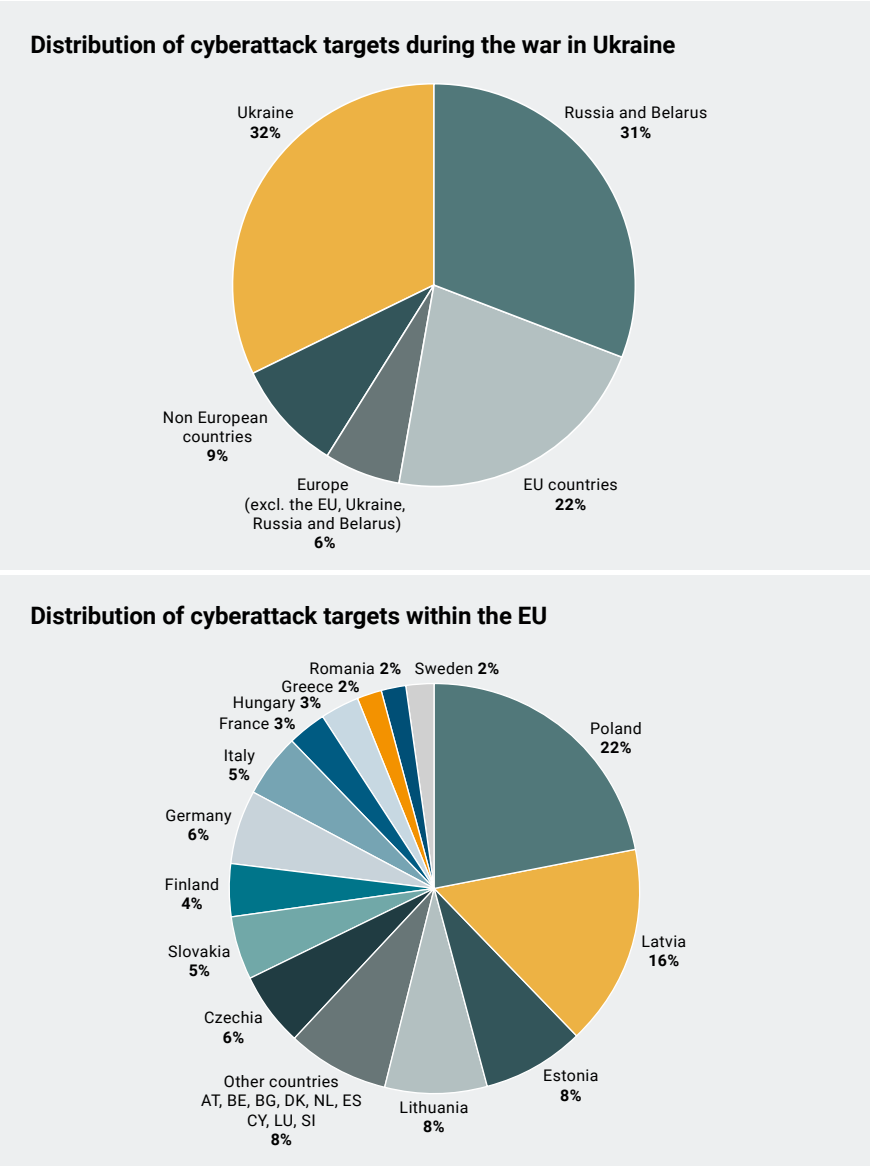
Strategic Russian advances have traditionally focused on the post-Soviet states; following the 2022 invasion, however, the blacklist has been extended to all pro-Ukrainian states – a strategy that is visibly reflected in cyber-incident distribution statistics (see Figure 7). In 2022, approximately 4% of all ransomware attacks

targeted the energy sector, averaging a breach cost of EUR 4.43 million per incident (IBM Security 2022). Power grid security has therefore become an increasingly pressing issue.

The hyper-connectedness and digitalisation of the energy system that are blurring the line between cyber and physical realms means that many potential attacks constitute a genuine risk of mass shutdown. This dynamic is particularly visible with respect to power grids.

Power grids connect diverse power generation sources, facilitating the transmission of electricity to households and businesses. The switch from analogue to digital grid infrastructure made the simultaneous multi-station manipulation of high-voltage grids a reality; something that was not physically possible before digitalisation (Rajkumar et al. 2019). With power grids being the 'connective tissue' of energy infrastructure and transmitting electricity generated from nuclear, geothermal, hydro, combustion, wind turbines, solar panels and massive fossil-powered generation units, they are pivotal to the energy ecosystem (Plėta et al. 2020). Such extremely complex and extended networks tend to be centralised, as power grid security has become national security (Ibid.). As power grids link multiple sources of power generation, a cyberattack on the grid or control centre may thus trigger a domino effect with serious physical consequences, including damage to power generation units and other critical infrastructure, such as water supply systems, transport networks and communication infrastructure (Badihi et al. 2021). Beyond causing blackouts, disruptions in these systems can lead to interruptions in electricity generation, increasing the risk of explosions (Kshetri and Voas 2017); for instance, in facilities such as natural gas power plants, chemical plants relying on precise electrical controls, and other industrial operations where electrical malfunctions can ignite volatile substances. Consequently, cyberattacks have an impact extending well beyond the digital realm and infiltrate the physical infrastructure (Badihi et al. 2021). Even though energy infrastructure is protected by cyber-defence technologies, the communication channels, as well as the control, optimisation and monitoring systems, remain particularly susceptible to attacks. Highly skilled cyber adversaries can circumvent security measures, disrupting, e.g., the operations of an entire wind farm, which, in turn, can have a cascading effect, disrupting energy flows across the entire region (Ibid.).

Figure 7. Distribution of cyberattacks following the war in Ukraine



Source: Cordes et al. (2023).
https://warsawsecurityforum.org/wp-content/uploads/2023/09/WSF2023_raport_20-09_WEB.pdf

CYBERATTACKS ON THE DANISH ENERGY SYSTEM

In May 2023, the Danish energy sector faced a critical threat when 22 of its energy companies were targeted in a significant cyberattack. This incident compromised their control systems, forcing several to operate in 'island mode' to maintain functionality. Detected by SektorCERT's sensor network, which identified recurring patterns across the affected companies, the attack unfolded in two waves. The initial assault on 11 May exploited vulnerability CVE-2023-28771, with a subsequent, possibly more sophisticated attack following on 22 May. An alert two days later revealed the involvement of an Advanced Persistent Threat (APT) group, known for its associations with actors like Sandworm, responsible for the cyberattacks on Ukraine in 2015, 2016 and several incidents in 2022 (Proska et al. 2023). This attack served as a stark warning, highlighting the systemic vulnerabilities inherent in Denmark's decentralised energy-sector governance. It underscored the critical importance of cross-company data monitoring, the implementation of rigorous security updates, and the development of comprehensive emergency plans. The incident was a very close call, almost triggering a catastrophic energy-infrastructure failure. The effective collaboration among industry stakeholders, including SektorCERT, the targeted companies, their suppliers and law enforcement, proved instrumental in minimising the impact of the attack and bolstering the defence against such formidable threats (SektorCERT 2023).

HARD SECURITY RISKS IN THE EXCLUSIVE ECONOMIC ZONES

In the wake of the war in Ukraine, the spotlight has turned to the security of energy infrastructure in the exclusive economic zones (EEZs), a topic that has only recently started making newspaper headlines frequently. This section explores the intricate challenges of safeguarding maritime energy infrastructure, which are additionally heightened by current geopolitical tensions, existing infrastructural dependencies and the overlay of diverse jurisdictions.

Since the construction of the NS 1 pipeline, any deep-sea operations (research, intelligence or sabotage) in the Baltic Sea have enjoyed a deniability cover under 'repair and maintenance work' by the Russian side on the gas pipeline(s) (Ryzhenko 2022). This tactic is nothing new and has been exploited by different parties under different pretences ever since World War I. However, given the current density of critical energy infrastructure in the maritime zones, the risks are magnified. For instance, the recently opened Baltic Pipe (2022) – connecting the Norwegian, Danish and Polish gas markets – crosses the Nord Stream pipelines and around 25 data

cables, thereby exposing this infrastructure to potential third-party activities under the cover of 'repair and maintenance work' in the area. Similarly, the Balticconnector (2019) adjoining Finnish and Estonian gas markets crosses the Nord Stream pipelines.

A variety of actors can easily access critical energy infrastructure sited in the maritime zones even without such cover. The recent findings of Putin's Shadow War docuseries produced by the Nordic broadcasting companies (DR, NRK, YLE and SVT) showcased Russian vessels conducting intelligence operations and mapping vital offshore infrastructure (including wind farms, gas pipelines and even electricity and data cables) in the Baltic and North Seas (DRTV – Skyggekrigen 2023). Often disguised as standard fishing and research units, such boats can carry out underwater surveillance operations and map offshore energy infrastructure with heavily armed 'research personnel' on board. For instance, the Admiral Vladimirsky was observed monitoring wind farms in Belgian and Dutch waters. Nearly 50 other vessels have stirred similar suspicions in the past decade in different locations (Radowitz 2023). In late December 2022, Italian authorities reported suspicious activity in the Otranto Canal, a location where multiple infrastructures (e.g. gas pipelines, electricity and internet cables) are concentrated. The Russian replenishment oiler Akademik Pashin was observed sailing along the Trans Adriatic Pipeline for hours (Grant 2022). While such activities raise alarms across Europe, these vessels claim to operate within the boundaries of international law, as the Russian ambassador to Norway asserted in April 2023 (James 2023).

Within the realm of the international law of the sea, the EEZ represents a unique and distinctive zone combining elements from both territorial waters and the high seas, creating a *sui generis* legal framework. Coastal states hold two types of rights within their EEZs: sovereign rights to manage and exploit both living and non-living resources, and jurisdictional rights. In terms of living resources, coastal states have the exclusive authority to explore, exploit, conserve and manage fish stocks found in the water column, seabed and subsoil of their EEZs (Liu and Tronchetti 2019). The exploration and exploitation of non-living resources in the EEZs (e.g. hydrocarbons, minerals) are unrestricted for coastal states, with no specific obligations pertaining to conservation or responsible utilisation. These rights are genuinely exclusive, as coastal states are not obliged to provide access to other nations. Article 56 of the UNCLOS Convention also mentions 'energy from the water, currents, and winds'. The Article states that the coastal states are further granted three jurisdictional rights related to the establishment and use of artificial islands, installations and structures; marine scientific research; and the protection and preservation of the marine

environment. The first right in particular grants the coastal state exclusive jurisdiction to construct and operate artificial islands, installations and structures for economic purposes, with provisions for safety zones and the enactment of various laws and regulations. It is important to note, however, that an EEZ is not considered a part of the coastal state's territory, despite the state enjoying extensive rights to utilise and govern it. While these rights appear 'exclusive' in name, they are therefore not without limitations, as other states also possess certain rights and freedoms within the EEZ.

The distance of energy infrastructure from the coastal state's shores inversely correlates with the legislative power that the country can exert over the area (Figure 8).

Despite the observable movement of commercial vessels, yachts, scientific expeditions and warships, international conventions complicate the further monitoring of sea activities. According to the United Nations Convention on the Law of the Sea (UNCLOS), the conduct of military activities in other nations' EEZs is deemed lawful, whereas the coastal country holds full jurisdiction over territorial waters (United Nations 1982).

Figure 8. Maritime zones under the UNCLOS Convention and the dispersion of jurisdictional rights

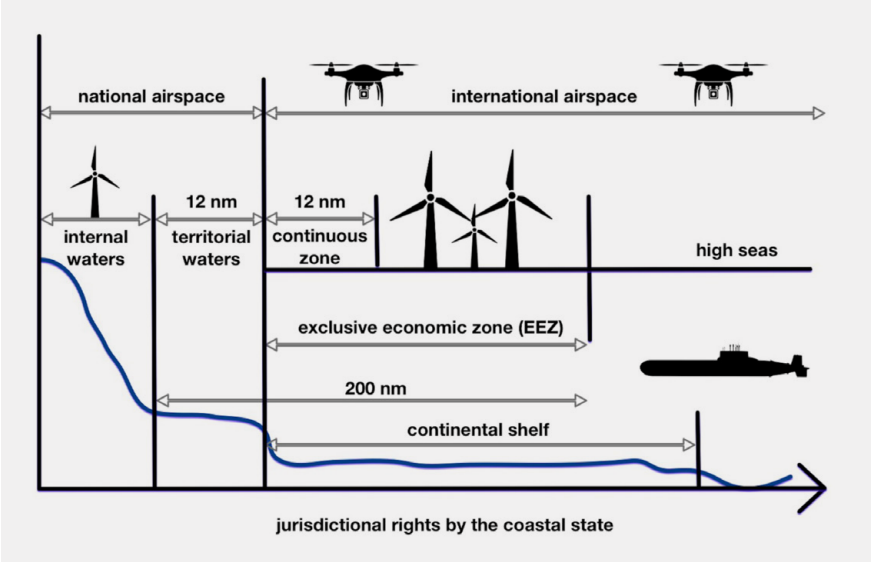


Illustration by Veronika Slakaityte, published in the DIIS Working Paper: Nærområdet, 2023.

While UNCLOS forms the fundamental legal framework, additional international conventions play a pivotal role in regulating the security of offshore energy infrastructure. Among these, conventions established by the International Maritime Organization (IMO) take centre stage, overseeing shipping operations near offshore installations. These conventions encompass the International Convention for the Prevention of Pollution from Ships (MARPOL), the Convention for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (SUA PROT), the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA), the Safety of Life at Sea Convention (SOLAS), and its related amendment, the International Ship and Port Facility Security Code (ISPS). Notably, MARPOL governs the circumstances under which coastal states can designate safety zones and special protection zones around offshore structures, affecting navigation. While ISPS and SUA conventions hold paramount significance in maritime security, their detailed application to wind farms remains limited. Complementary legal frameworks encompass international environmental law and international criminal law (see Bueger and Edmunds 2023).

Article 58 of the Law of the Sea Convention also introduces elements from the high seas' regime into the EEZ framework, such as the freedom of navigation and overflight. Coastal states are entitled to take measures to enforce foreign vessel compliance, although the boundaries of such enforcement measures remain somewhat ambiguous, creating the potential for undue interference with other states' rights. Furthermore, even in the areas where critical infrastructure is sited, achieving comprehensive surveillance is an insurmountable challenge, as it extends across the seabed, featuring multiple overlapping layers and constant maritime traffic. Such zones therefore represent an ideal theatre for hybrid attacks, allowing malicious actors with intentions to disrupt the infrastructure to operate with minimal risk of apprehension.

Here, it is crucial to note how recent incidents of sabotage on both the Nord Stream and Balticconnector pipelines occurred in the EEZs. The Nord Stream sabotage incidents occurred just outside the Danish territorial waters surrounding the island of Bornholm. As it is lawful to conduct military activities in the high waters (i.e. EEZs), the sabotage incidents along the NS1 and NS2 pipelines in September 2022 became a matter of international diplomacy rather than an act of open hostility towards a specific country. This would not have been the likely outcome had the explosions instead occurred in Danish territorial waters. In fact, the NS 1 pipeline runs through the territorial waters of Denmark south of Bornholm. This stretch of pipeline could just as easily have been the target. Similarly, the damage to the Balticconnector

pipeline occurred in the Finnish EEZ. And even though NATO Secretary General Jens Stoltenberg noted at the time that 'a united and determined response from NATO' would follow if the pipeline damage proves to be an attack on NATO critical infrastructure, there is no clear legal basis for such a response (just like with the NS1 and NS2 explosions). Simultaneously, the fact that both incidents took place in the proximity of territorial waters – but not in them – points therefore to an important spatial factor that must be considered when constructing new infrastructure; namely, that future attacks may be strategically aimed at exploiting the gaps in security protocols just beyond the territorial waters, in the EEZs. Hence, judiciary boundaries should be considered in future energy project plans.

> In response to escalating threats to undersea and maritime critical infrastructure, NATO has significantly stepped up its strategic efforts. In February 2023, the Alliance established the Critical Undersea Infrastructure Coordination Cell at its headquarters, aiming to enhance collaborative efforts, intelligence sharing and response coordination against threats to vital undersea assets. This move underscores NATO recognition of the growing vulnerabilities within its members' maritime domains. Bolstering its maritime defence further, the NATO Maritime Command (MARCOM) in the UK has seen its role expanded as of June 2023, following a statement by Secretary General Jens Stoltenberg. This enhancement bears witness to the NATO commitment to not only address the direct threats but also to safeguard the maritime critical infrastructure proactively against both traditional and non-conventional threats, ensuring Alliance resilience in the face of evolving maritime challenges (NATO 2023a).

Those incidents also highlight the need for legal interpretation of how to respond to activities perpetrated by different actors in EEZs; especially that the EEZs encompass a multitude of offshore energy infrastructures that frequently traverse multiple jurisdictions, in the European context extending beyond EU boundaries and encompassing countries such as Norway and the UK. This infrastructure includes subsea pipelines, power cables, mining and mineral extraction platforms, as well as offshore windfarms, wave and tidal energy systems, and floating production systems typically used for the extraction and processing of oil and gas in deeper waters. Such complexity further complicates the development of comprehensive regulatory, legal and technical solutions for safeguarding critical infrastructure.

While national and international legal frameworks can e.g., impose penalties for any actions disrupting or damaging underwater cables, additional comprehensive policies and procedures must be developed to address the unique challenges posed by large-scale offshore and undersea projects, which often reside in the EEZs and face distinct security considerations.

TIME, PLACE AND SABOTAGE

If recent incidents in the EEZs point to an important spatial dimension to consider while preparing for future attack scenarios in the region, it is also worth noting when attacks occur. Russia frequently adheres to historical narratives, typically timing strategic political/military moves around key historical dates. The very invasion of Ukraine on 24 February 2022 was preceded by the festivities of the Russian 'Defender of the Fatherland Day' on 23 February – a holiday devoted to soldiers, patriotism and masculinity. Although still pending investigation, it might also be worth noting that the news of the Nord Stream pipeline sabotage in 2022 broke in international media on the very day Poland and Denmark celebrated the opening of the Baltic Pipe – a project that drastically reduced decades-long Polish dependence on Russian natural gas. Would the next attacks similarly happen in EEZs at the crucial timing (e.g. the re-installation of the Danish Tyra natural gas field platform in spring 2024 or the opening of the prestigious Bornholm energy island in five-year's time)? The temporal and spatial dimensions should be considered.

REINFORCING THE ENERGY BACKBONE: DEFENCE AND THREATS

In the current geopolitical landscape, marked by an urgent need to diversify energy supply, the security of gas infrastructure, encompassing both existing pipelines and new LNG terminals, has become critically important. The urgency to diversify energy sources away from Russian gas, previously a transitional fuel in the EU shift to green energy, has accelerated the development of new gas infrastructures. While natural gas (or oil) pipeline projects often take years to complete, the current crisis has shown how – if needed – LNG terminals can be built in under a year (e.g. the new LNG in Inkoo, Finland or the three FSRUs docked in the German ports of Wilhelmshaven, Brunsbuettel and Lubmin). Expanding LNG infrastructure, while enhancing regional energy security, introduces new vulnerabilities, especially in coastal areas. Likewise, the rapidly expanding renewable energy infrastructure in maritime zones faces similar threats.

The following section delves into the complex array of threats and protective measures for these critical assets. Additionally, we explore the burgeoning field of offshore renewable energy infrastructure. In light of the ambitious EU plans to increase renewable energy capacity significantly (particularly through offshore wind farms), understanding and mitigating the array of risks facing these installations is imperative. From physical security concerns to the intricacies of cyber threats, this section provides a comprehensive overview of the current state and future challenges in safeguarding vital European energy infrastructure.

From gas pipelines to LNG terminals

LNG infrastructure can be categorised into two primary types: onshore and offshore floating facilities. It is essential to underscore how national boundaries delineate the jurisdiction of LNG infrastructure in both cases, which significantly influences the design and implementation of protective measures. While the resilience of the onshore energy infrastructure against physical attacks relies on standard physical protection and surveillance techniques, the safeguarding of floating terminals presents a more complex challenge due to the additional maritime dimension; the inherent nature of such infrastructure dictates that it resides within territorial waters. Consequently, the coastal state exercises authority over its territorial sea, the airspace above, and the seabed and subsoil below. This distinction plays a pivotal role in ensuring the security and resilience of these critical energy assets.

Nonetheless, there are multiple potential threats to LNG infrastructure. As identified by Miętkiewicz (2021), such threats include surface vessel attacks, submarines, sea mines, autonomous systems, activist actions, firearm and explosive threats, ship-to-ship missiles, submarine warfare, suicide attacks, dense maritime traffic, indirect and dynamic threats, media influence, the instability of oil and LNG shipments, vessel seizures during international tensions, blockades and the potential for diverse attack methods. The threat landscape is complex, characterised by terrorist creativity and the interplay of state terrorism, piracy and hybrid conflicts (Figure 9).

The highly flammable content in the storage tanks magnifies the risks to the LNG infrastructure. Therefore, weaponry that is typically utilised in terrorist operations (e.g. grenade launchers, suicide attacks, armed assaults) is also simulated in the LNG threat scenario assessments.

Moreover, autonomous systems – which can be used for both protection and sabotage of different types of critical energy infrastructure – comprise a diverse category of vehicles operating in various domains, including unmanned aerial vehicles in the skies (UAVs), unmanned ground vehicles on the ground (UGVs) and unmanned maritime vehicles on (and in) the sea (UMVs). Of these three sectors, the effective implementation of protective measures in the maritime domain seems to pose the greatest challenges.

Figure 9. Security and operational risks for LNG terminals and tankers

THREATS TO THE OPERATION OF LNG TERMINALS AND TANKERS FROM THE SEA DIRECTION			
Means to conduct the assault	Availability	Assault target	
		Terminal	LNG carrier
From the sea			
Hijacking	Low	–	•
High-speed unit	High	•	•
Fire from the sea	Low	•	•
Unmanned systems	High	•	•
Disguised unit	Medium	•	•
Surface mine/WBIEDs	High	•	•
From the air			
Airliner	Low	•	•
Light aircraft	Low	•	•
Powered hang glider	Medium	•	•
UAV	High	•	•
Ship-to-ship missile	Low	•	•
Ballistic missiles	Low	•	–
Balloons	High	•	–
From underwater			
Sea mines	Medium	•	•
Underwater WBIEDs	High	•	•
Diver/saboteur	High	•	•
Miniature submarine	Low	–	•
Combined attacks	Hard to predict	•	•

Source: Miętkiewicz (2021).https://www.sciencedirect.com/science/article/abs/pii/S0925753521002411

Given the diverse locations of floating storage and regasification units – all situated within national jurisdictions – the most effective means of safeguarding this infrastructure necessitate context-specific approaches. For instance, the Lithuanian FSRU Independence stands as a resilient bulwark against potential threats, primarily due to its proximity to Kaliningrad and the longstanding complex relations with Russia, which led to the heavy fortification of the facility. Conversely, offshore LNG terminals in Southern Europe may contend with distinct threat scenarios (e.g. potential piracy incidents in the Mediterranean region), which demand bespoke security measures.

Nonetheless, the fact that these facilities are positioned within territorial waters grants the host country complete jurisdiction, facilitating effective security solutions. However, offshore energy infrastructure located further out to sea presents a distinct set of challenges, which we will delve into in the following section.

The offshore renewable energy infrastructure

The maritime critical infrastructure – gas and oil pipelines, power and communication cables – has been deployed for decades. While recent years have witnessed a significant increase in offshore wind farms, new regulations aimed at almost doubling renewable energy generation in the EU by 2030 will also translate into the further scaling up of wind energy (European Commission 2024). If the cumulative installed wind capacity in the EU stood at approximately 255.5 GW in 2022 (Statista 2023b), the EU aims to house 451 GW of wind power capacity by 2030. This highlights the need for a significant expansion, which will mostly be achieved by developing large-scale offshore wind farms in the Baltic and North Seas.

> The primary offshore wind energy hubs are planned in the North and Baltic Seas, solidified by two key declarations: the Esbjerg Declaration (May 2022) commits Denmark, Belgium, the Netherlands and Germany to reach 65 GW by 2030 and 150 GW by 2050. The Marienborg Declaration (August 2022) involves eight Baltic Sea states, targeting a capacity increase from 2.8 GW to 19.6 GW by 2030.

The necessary protective measures in the maritime areas are much more complex than onshore. The maritime-residing infrastructure is exposed to two additional types of threats: surface and underwater. The former can be enacted by a wide range of means, including commercial and research vessels as well as warships (see our chapter on EEZs). The latter includes automated underwater vehicles, submarines and divers. A simultaneous multi-site disruption of underwater critical infrastructure would have significant impact on a major scale.

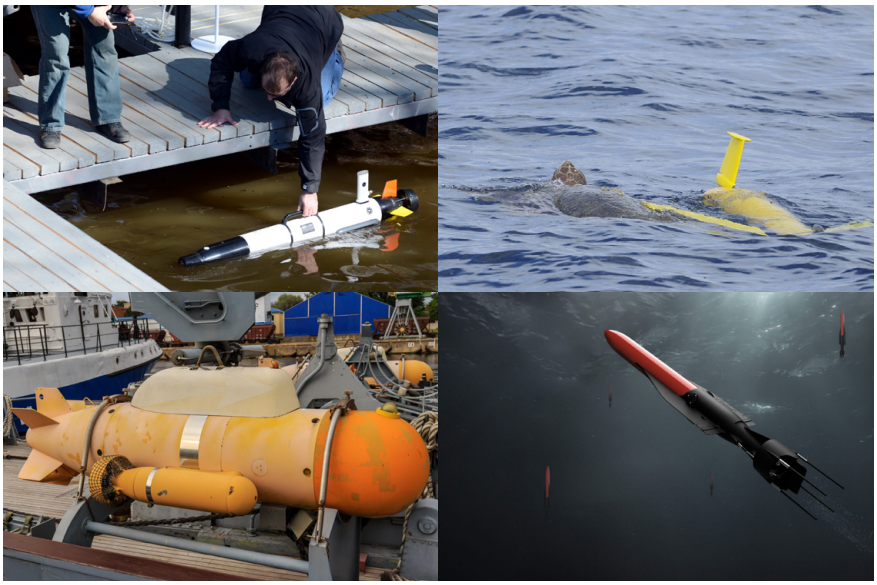
Although often said to be subject to 'sea blindness', maritime infrastructure is increasingly being protected by technologies ranging from satellites to detection cables. Surveillance and monitoring of the energy infrastructure sited in the maritime zones typically involves visual inspections conducted by patrols, deployment of underwater cameras as well as acoustic sensors to detect, e.g., cable movement or damage. Depending on the most prominent risk factors, various technological solutions are employed to counter the threats. As regards the surface level, for instance, the most common protective measures are the so-called above-water heterogeneous systems and sensors, which include technologies ranging from satellite sensors (automatic identification systems that large ships must use to broadcast their position) to terrestrial radars, which allow high accuracy real time monitoring of dynamic structures.

PATROLLING THE MARITIME ZONES

The Nord Stream and Balticconnector incidents demonstrated the insufficiency of current security measures. In the aftermath of the NS1 and NS2 explosions in September 2022, Germany and other countries increased the patrolling of the maritime zones. Since the Balticconnector incident in October 2023, NATO has also intensified its surveillance and reconnaissance activities in the Baltic Sea region. This includes the deployment of maritime patrol aircraft, NATO AWACS aircraft and drones for ongoing patrols. Four NATO minehunters were also dispatched to the area (NATO 2023a). Moreover, numerous reported drone sightings near offshore oil and gas platforms and other Norwegian infrastructure (Euronews and AFP 2022) prompted improvements to North Sea aerial surveillance. Additional security measures are needed, however, in terms of enhancements to the typical access control, security and video surveillance systems and the underwater surveillance.

As with other maritime activities (e.g. military operations, transport of goods or marine and climate research), the security and surveillance of critical infrastructure (including ports, naval bases and offshore installations) takes advantage of the rapid progress of autonomous technologies in the maritime domain (Miętkiewicz 2021). The maritime domain encompasses systems capable of functioning on the sea's surface as unmanned surface vehicles (USVs) and underwater as unmanned underwater vehicles (UUVs) (see Figure 10). Another intriguing subset of vehicles includes biomimetic vehicles (BVs), which are designed to emulate the movement and appearance of living organisms (e.g. fish, birds) (see Figure 11). Consequently, BVs tend to be less noticeable, making such technologies more effective for a variety of uses, including potential covert surveillance operations. Modern technological

Figure 10. Exploring the Depths: various underwater autonomous vehicles

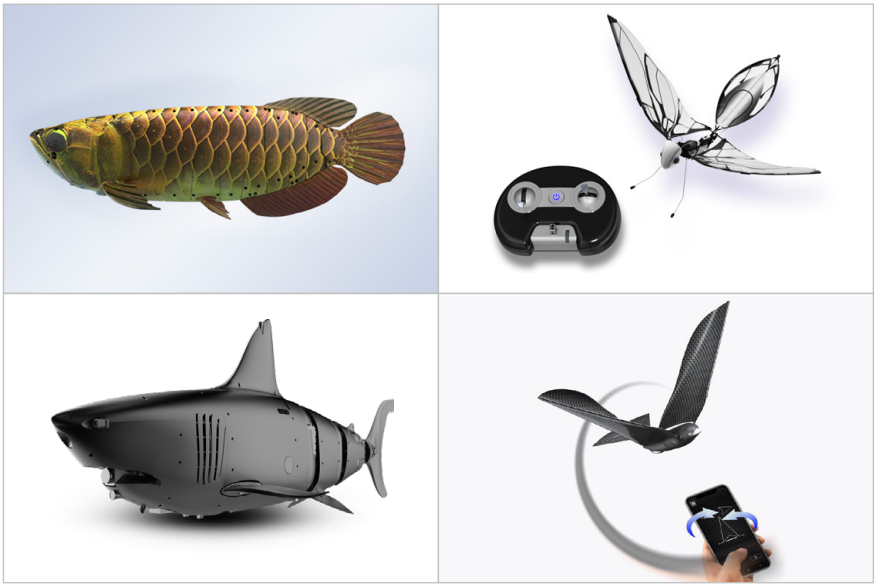


Photos and descriptions:
Upper left corner: Stock Photo ID: 422858695, Free Wind 2014, Shutterstock.com.The marine scientists launch an autonomous underwater unmanned vehicles. Moscow, Russia, 2014.
Lower left corner: Stock Photo ID: 496337446, Venot, Shutterstock.com. Underwater drones.
Upper right corner: Photo: Eric Bowles (Bowles Images). A glider - designed to operate in coastal waters up to a depth of 200 metres where high manoeuvrability is needed near the shelf break off Long Bay, South Carolina.
Lower right corner: Photo: Jaia Robotics, as featured on Rhode Island Current. The micro-sized, low-cost, aquatic drones known as JaiaBots, designed to collect data for academic, industry, government, and U.S. Department of Defense applications. This photograph is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. For more information, visit https://rhodeislandcurrent.com/briefs/r-i-commerce-authorizes-225k-in-research-grants-for-three-companies/

advances have resulted in the development of hybrid vehicles (HV), which are platforms designed to adapt or modify the environment to enhance task execution during missions.

UUVs (underwater drones), are frequently used in underwater-level surveillance. The oil and gas industry has been employing autonomous underwater systems for tasks such as monitoring submarine infrastructure, particularly transmission systems (González-García et al. 2020). The remotely operated vehicles (ROVs) also find significant utility in a broad spectrum of missions, including the monitoring of underwater environments for example around offshore wind farms. Unlike UUV systems, ROVs maintain continuous communication with their parent unit, providing the benefit of real-time data transmission, including sonar and camera images, for immediate analysis at the control station. ROVs are versatile and can perform various underwater tasks, such as carrying loads, additional lighting sources, and extending working booms when required (Miętkiewicz 2021).

Figure 11. Mimicking nature: innovations in biomimetic vehicle design



Photos and descriptions:
Upper left corner: Photo: ROBOSEA. The ROBOLAB-GL—designed and manufactured by ROBOSEA— equipped with infrared obstacle avoidance sensors, can therefore avoid surrounding obstacles.
Lower left corner: Photo: ROBOSEA. The ROBO-SHARK (also known as BS-100)—designed and manufactured by ROBOSEA—has a high underwater speed and large payload capacity for its size.
Upper right corner: Photo: Bionic Bird. App controlled Drone METAFLY for Indoor/Outdoor use.
Lower right corner: Photo: Bionic Bird. App controlled Drone METABIRD for Indoor/Outdoor use.

Underwater surveillance also includes various sensors (e.g. sonars, cameras) typically installed on the critical infrastructure itself. Other contextual data is also used to feed supplementary information. For instance, the Swedish National Seismic Network and the Geological Survey of Denmark and Greenland both detected powerful under-water explosions coinciding with the Nord Stream pipeline sabotage, and the NORSAR station registered seismic waves near the coast of Finland when the Balticconnector started leaking (The Maritime Exclusive 2023). Various contextual information (e.g. bathymetry, weather, human and open-source intelligence) is paramount. Given the massive amount of data, it is processed using artificial intelligence and information fusion techniques (Soldi et al. 2021). Such data-processing methods allow the detection of anomalies and tracking of targets to monitor daily activities by utilising various data sources. The processed data is then transmitted to authorities that – depending on the assessment – can respond by alerting the coastguard, defence forces, police or others to investigate further.

Figure 12. The Saab MuMNS system - a new generation of mine neutralisation and immunisation

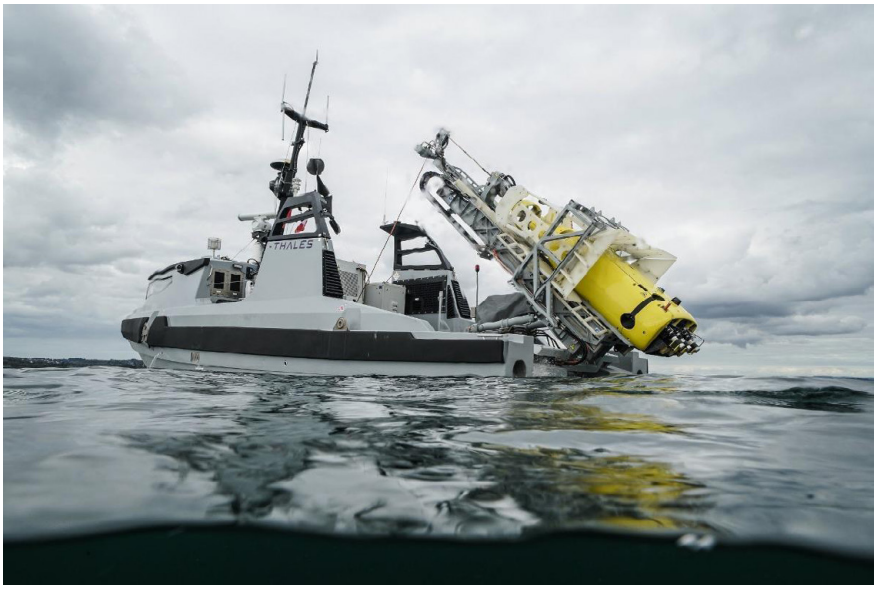


Photo and source: Thales/OCCAR.
Available via the Organisation Conjointe de Coopération en matière d'Armement (OCCAR) Website. Accessed on February 27, 2024. https://www.occar.int/news/maritime-mine-counter-measures-mmcm-france-receives-next-capability-step

Figure 13. Beluga whale 'Hvaldimir' in northern Norway

Photo and source: Stock Photo ID: 2331521549, Anton Berking, Shutterstock.com.

While the concept of biomimetic vehicles, ingeniously engineered to replicate the movements of living organisms, may strike as a futuristic innovation, the strategic deployment of actual animals in surveillance operations has a rich history. A compelling illustration is 'Hvaldimir', the Beluga whale adorned with a mysterious harness. Discovered off Norway's coast in 2019 (see Figure 13), 'Hvaldimir' ignited widespread conjecture about having been trained as a Russian navy spy. The whale's subsequent appearance near Sweden further fuelled the intrigue surrounding the use of marine mammals in espionage (AFP 2023).

Notably, the Soviet Navy at Kazachya Bukhta once spearheaded a ground-breaking programme dedicated to the military utilisation of dolphins. Such endeavours were not exclusive to the Soviets; a myriad of nations, including the United States and Iran, have ventured into similar domains, employing animals for tactical operations. These historical episodes underscore a persistent fascination with harnessing the innate abilities of animals for defence and intelligence purposes. They also serve as a stark reminder of the diverse and unexpected nature of security threats in the modern world (Walker 2014).

Safeguarding offshore energy infrastructure often requires additional considerations, such as burying cables deeper in the seabed, applying protective coatings, installing physical covers, using concrete mats to enhance physical security, and establishing safety zones around subsea infrastructure to offer protection to/from fishing activities (typically 500 metres measured from the centre of its location) (FishSAFE 2024).

Underwater cables – being flexible and fragile – represent the most vulnerable maritime infrastructure. Spanning over 1.3 million kilometres globally, underwater optical fibre and electricity cables are a vital part of modern infrastructure. The most significant risk to underwater cables is in areas with dense maritime traffic bottlenecks. One such critical passage is in the Strait of Gibraltar, through which seven intercontinental cables pass. Another passage concerns the transit through the Red Sea, connecting the Mediterranean Sea to the Indian Ocean, where 16 underwater cables traverse the Egyptian mainland.

Moreover, projects such as offshore wind parks, which primarily operate in an automated mode as intricate cyber-physical systems, are continuously exposed to a multitude of interconnected threats, ranging from physical to cyber, often striking simultaneously (Torres et al. 2020).

Wind farms are susceptible to attacks due to their geographical scale, the remoteness of their turbines and substations, the flat logical configurations of their control networks, and the use of insecure supervisory control and data acquisition (SCADA) protocols (Staggs, Ferlemann and Shenoi 2017, 3). On the most basic level, attackers might focus on gaining physical access to wind turbines and substations. While typically located in remote areas, wind farms often have rudimentary physical security mechanisms. Even with more advanced security solutions (e.g. unauthorised entry alerts), the remote location makes rapid response to physical security challenging (Staggs, Ferlemann and Shenoi 2017, 7), especially for offshore wind farms. Therefore, the planned expansion of offshore wind in Europe poses additional challenges. While the physical monitoring of compact facilities in proximity to the shore is somewhat more manageable in the Baltic Sea, the planned North Sea wind projects will be located further from the coast and therefore harder to protect.

The European Wind Action Plan, published in late October 2023, places significant emphasis on cybersecurity measures. The Commission will assess cybersecurity risks in wind energy installations and related infrastructure, including data protection, to determine their potential threat to EU economic and electricity supply security. This evaluation is part of the broader risk assessment led by the Commission, High Representative and the NIS Cooperation Group, as outlined in the Council Recommendation of 8 December 2022. To facilitate this analysis, the Commission will engage expert groups, such as the Smart Energy Expert Group, and draw from the experience gained in the field of 5G technology (COM (2023) 669 final).

Once physical security is breached, the wind farm's control network can be compromised, possibly using malicious devices, resulting in damage that can affect other connected turbines and substations (Ibid.). Cyberattacks can also target the control systems of wind farms and information technology, disrupting wind farm operations or even damaging physical components, such as wind turbines (Staggs, Ferlemann and Shenoi 2017, 5–8). Other potential physical threats include collisions between ships and wind farm infrastructure, which have been documented in the past. Although the likelihood of a terrorist attack on such facilities remains remote, it is also a possibility.

To mitigate potential attacks on wind farms, essential security measures against both physical and cyber threats are needed. The former involve implementing strong locking mechanisms with multi-factor authentication, deploying motion sensors and security cameras, and establishing remote alarm notification systems. Network segmentation and system hardening, such as adjusting default configurations to

more customised settings, are also critical components of the defence strategy (Staggs, Ferlemann and Shenoi 2017). Additionally, comprehensive policies and procedures must be developed to address the unique challenges posed by large-scale offshore wind projects, which often reside in the EEZs and face distinct security considerations.

Despite significant technological advances, the detailed monitoring of energy infrastructure sited across vast maritime areas is often unfeasible due to the limited technical and financial capacities of different actors, with governance structures for this task remaining in the formative stages. With hard-security threats in the maritime zones on the rise, the technologies typically employed (e.g. autonomous underwater vehicles and remotely operated vehicles) no longer prove sufficient to ensure thorough monitoring in the increasingly tense geopolitical context (Soldi et al. 2023). A key impediment to the protection of critical maritime infrastructure also derives from the challenge of determining equipment ownership and fostering cooperation between public and private sectors for security, maintenance and regulatory frameworks. Exacerbating this challenge is the fact that more than 80% of all European critical infrastructure is controlled and operated by private companies (Umbach 2023). In addition to the private-ownership issue, the sheer expanse of the geographic area covered by this equipment (connecting multiple countries) further complicates the governance of these indispensable networks for communication, energy and finance (Fridbertsson 2023).

Considering these challenges, increased co-operation between national and supranational actors across different sectors is needed to boost the resilience of critical energy infrastructure. The effective management of future threats in the region will necessitate cooperative efforts and the establishment of regulatory frameworks for monitoring and intercepting both physical and cyber threats. Many of these initiatives should be implemented on a regional scale, encompassing both territorial and EEZ zones.

Increasing regional cooperation

The EU commitment to protecting critical infrastructure, initiated with Directive 2008/114/EC, overlooked the pivotal role of maritime zones (European Council 2008). Acknowledging this oversight, the EU has now advanced security measures to bolster the resilience of maritime infrastructure alongside other critical sectors (Belyi and Piebalgs 2024).

In response to various security threats, including unauthorised intrusions and cyberattacks on maritime assets, the EU also updated its Maritime Security Strategy and Action Plan (Council of the European Union 2023). This revision aims to bolster the protection of critical maritime infrastructure amidst the sector's digitalisation, which presents new complexities and vulnerabilities. The revamped strategy supports a rules-based maritime governance system in line with international law and outlines specific measures for EU and Member State cooperation. These measures focus on reinforcing EU leadership, addressing maritime risks and threats, and enhancing partnerships, including capacity building, research and education aligned with the European Green Deal targets.

The EU Maritime Security Strategy (EUMSS) emphasises the protection of offshore energy infrastructure, advocating for the coexistence of renewable energy and defence activities (European Council 2023). A comprehensive set of actions beginning in 2023 is designed to enhance the resilience of vital infrastructure across all EU sea basins. These actions include risk assessments, contingency plans, stakeholder engagement and regular maritime exercises to address various security challenges. Enhanced collaboration between Member States, EU agencies (e.g., Frontex – the European Border and Coast Guard Agency, the European Defence Agency and the EU Agency for Cybersecurity), and partners like NATO will lead to improved surveillance, the deployment of specialised vessels, and strengthened national competences in ship and port security, with ongoing initiatives over the next few years.

The EU Strategic Compass complements the EUMSS by emphasising the readiness and interoperability Member States' naval forces, advocating for live exercises across all domains to enhance joint response capabilities. With the commencement of integrated civil–military exercises to improve response capabilities, annual naval drills involving Member States are scheduled to start in 2024. Furthermore, a comprehensive mapping of the sea basins (foreseen to be carried out in all European basins) will inform the removal of hazardous munitions. The Strategy accords special consideration to the unique features of Europe's diverse maritime regions, from the Mediterranean to the Arctic, ensuring tailored security and environmental strategies.

The EU's Maritime Security Strategy advocates for international cooperation through the endorsement and ratification of maritime security instruments (notably UNCLOS), and it promotes compliance and the sharing of best practices within relevant forums. It aims to intensify EU–NATO staff cooperation on maritime security, building on the Joint Declarations of 2016, 2018 and 2023 to enhance operational collaboration and coherence while avoiding redundancies. The strategy also calls for stronger partnerships with third countries, focusing on information sharing and capacity building, particularly around the EU sea basins and in regions such as the Western Balkans and the Eastern and Southern neighbourhoods. It also includes joint maritime exercises to boost interoperability and expanding the EU naval presence with frequent port calls and patrols in strategic areas like the Indo-Pacific, in accordance with the Strategic Compass. The EU continues to foster relations and synergies with multilateral and regional organisations (e.g. UN, NATO, the AU, ASEAN), and it reinforces its mutually beneficial cooperation with NATO, contributing positively to global and transatlantic security. In the Indo-Pacific, the EU is increasingly experiencing exchanges on maritime security through the 'Enhancing Security Cooperation in and with Asia' (ESIWA) project and working to gain observer status in the Indian Ocean Rim Association (IORA).

NATO has also heightened emphasis on sea protection by increasingly prioritising the integration of cutting-edge maritime technologies. In autumn 2023, in collaboration with Saab, NATO conducted two 'operational experimentation exercises' REPMUS 23 and DYNAMIC MESSENGER 23. Both exercises featured substantial collaborations between the private sector and academia, offering valuable insights into technological advancements, operational concepts, doctrines and future programmes (NATO 2023b). The exercises included anti-submarine training (AUV62-AT and Seaeye Falcon ROV) and a submarine's acoustic profile simulation (AUV62-AT in partnership with Sweden's Defence Materiel Administration) enabling navies to refine their anti-submarine warfare systems (see Figure 14). The exercises also included the identification and neutralisation of underwater explosive devices on an underwater cable (SAAB 2023).

Figure 14. Remotely operated underwater vehicle

Photo and source: Saab AB. Seaeye Falcon ROV.

NAVIGATING THE COMPLEXITIES OF ENERGY INFRASTRUCTURE PROTECTION

Securing critical energy infrastructure in the face of ever-evolving cyber-physical threats and in an increasingly tense geopolitical context is a major, multifaceted challenge. Recent incidents involving suspected sabotage highlighted the necessity of additional security measures, especially regarding the maritime zones. While the as yet insufficient policy focus, high costs of development and deployment of necessary surveillance technologies, and fragmented governance have all hindered this process, several steps can be taken to improve the resilience of the European energy system against natural disasters and deliberate attacks:

Back-up and repair capacity: Ensuring energy supply back-up in case of disruption and efficient repair capacity.

Risk assessment and mitigation: Conducting regular risk assessments that account for a variety of threats and scenarios in a new geopolitical context.

Surveillance and monitoring: Offshore energy infrastructure can be monitored using various methods, including visual surveillance by patrols, underwater cameras and acoustic sensors that detect movement or damage.

Physical protection: Enhancing physical security measures (e.g. access controls, surveillance systems) that keep unauthorised parties from accessing critical infrastructure.

Cybersecurity: Enhancing cybersecurity measures (e.g. firewalls, intrusion detection systems, encryption) essential for protecting critical energy infrastructure from cyberattacks, such as denial-of-service attacks or attempts to hack into cable control systems.

Collaboration: Increasing collaboration and knowledge-sharing between government agencies, the private sector, NGOs and other stakeholders to identify and address potential threats, and to designate necessary human and financial resources according to capacities.

Governance: Establishing clear governance structures to monitor and respond to critical infrastructure projects, including designating the bodies in each country that are responsible for cross-country cooperation.

Strategic segmentation: Aligning with advanced maritime security frameworks, this approach categorises maritime areas based on threat levels and strategic importance. 'Control' zones prioritise critical infrastructures like LNG terminals for maximum security and surveillance. 'Secure' zones, crucial for transit and ports, ensure thorough monitoring. 'Deter' zones, such as EEZs, implement selective surveillance and patrols. This strategy optimises resource distribution, addressing evolving cyber-physical threats and geopolitical tensions efficiently.

Legal provisions: Current national and international laws can provide certain legal protections (e.g. penalties for damaging or interfering with underwater cables). There is a need for additional legal interpretation of which activities should be allowed in EEZs with a view to protect critical energy infrastructure, while spatial dimension should be considered while siting new projects.

However, preparing for all the possible incidents is unfeasible due to the vast geographical surveillance area, necessary capacities and costs involved. The current policy efforts are further complicated by a number of larger dilemmas that must be addressed on a wider scale:

STREAMLINING GOVERNANCE OF PROTECTION

Fragmented governance on national and regional levels currently complicates the establishment of a coherent response structure as well as sufficient response measures to threats to critical European energy infrastructure. Different states have different governing bodies responsible for protective measures, such as coast guards, police, different ministries and other government bodies overseeing national security provisions. This complicates cross-country communication, information-sharing and coordinated response systems to incidents that are of regional scope and impact. Furthermore, transregional governance is complicated by the lack of clarity regarding the involvement of different organisations (including the EU and NATO) and under what provisions it is to be undertaken and coordinated.

The dilemma here revolves around designing clear and efficient governance structures, starting bottom-up from the national level.

CAPACITY VERSUS COSTS

The decisions about which energy infrastructure requires protection and to what extent cannot be taken without considering the costs involved. The fact that around 80% of critical infrastructure in Europe is currently owned by private companies complicates this task. While ensuring energy supply while making a profit is the primary goal of energy businesses, protection of offshore projects against hard-security threats, such as incidents of sabotage, frequently extends beyond both their financial and technical capacities. Moreover, in many cases, the delineation of responsibilities between public authorities and the private sector is not well-defined or mutually established. This often leads to ambiguity in roles and duties, creating challenges in governance and business operations.

The dilemma here revolves around the question of how to efficiently share the costs for surveillance and protection of critical energy infrastructure between different state and non-state actors, at both the national and regional levels. Coordination of efforts is crucial, as whereas national governments or the EU might dedicate funds towards this goal, other entities, such as NATO, might be better equipped for tasks such as the protection of offshore projects against military threats or physical attacks.

TECHNOLOGY AS A DOUBLE-EDGE SWORD

In the realm of energy infrastructure security, modern technology serves a paradoxical role. Advanced tools and technologies designed for system safeguarding can provide robust defence but also become formidable weapons in adversarial hands to be exploited for attacks. This blurs the line between protection and vulnerability. Simultaneously, a continuous technological race advances both the existing defensive capabilities and the corresponding offensive tactics. The rapid evolution of artificial intelligence, machine learning and cyber tools exemplifies this dual-use dilemma, as these technologies can both significantly bolster defence and facilitate increasingly complex attacks. Another pertinent example is how unmanned vehicles are instrumental in protecting remote infrastructure yet capable of being used to survey and target the very same assets.

The use of technology as a double-edged sword also has another dimension; namely, increasingly advanced technological defence systems installed, e.g., in offshore infrastructure, inadvertently place a greater target on the very projects they are designed to protect.

Hence, policymakers and stakeholders must navigate this shifting landscape, where integrating cutting-edge technology demands the careful weighing of risks and benefits.

HYPERCONNECTEDNESS

The benefits of hyperconnectedness for the operational efficiency and coordination of energy systems are being continuously contrasted with its vulnerabilities, particularly in the cybersecurity sector. Here, technological advancements not only streamline operations and strengthen system security but also amplify cybersecurity risks. A single breach can have far-reaching consequences, jeopardising the entire system.

However, the hyperconnectedness of the global energy infrastructure goes beyond technological aspects and embraces complex interlinkages between existing governance structures, economic dependencies and political considerations. This complexity means that disturbances in one area can trigger wide-ranging systemic repercussions.

Navigating hyperconnectedness therefore requires the development of broad risk management strategies that would consider the diversity of scenarios and prepare cohesive, cross-sectoral responses. Technological innovation, governance structures and infrastructure investments must all be considered together with a view to increasing the long-term resilience, efficiency and adaptability of energy systems.

NOTES

1 The Energy Community is an international organization integrating EU energy policies with neighbouring countries, primarily in Southeast Europe and the Black Sea region. Established in 2005, it focuses on market liberalization, environmental standards, renewable energy and energy efficiency to promote an integrated, sustainable European energy market. In addition to the EU Member States, the Energy Community includes Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, Georgia, Moldova, Montenegro, Serbia and Ukraine. Armenia, Norway and Turkey have observer status.

2 Main Directorate of Deepwater Research/Главное Управление Глубоководных Исследований.

REFERENCES

AFP. 2023. 'Suspected Russia-Trained Spy Whale Reappears off Sweden's Coast'. The Guardian, 29 May 2023, sec. World news. https://www.theguardian.com/world/2023/may/29/suspected-russia-trained-spy-whale-reappears-off-swedens-coast

Armstrong, Kathryn, and Vishala Sri-Pathma. 2023. 'Finland Investigates Suspected Sabotage of Baltic-Connector Gas Pipeline'. BBC News, 10 October 2023, sec. Europe. https://www.bbc.com/news/world-europe-67070389

Badihi, H., Jadidi, S., Yu, Z., Zhang, Y. & Lu, N. (2021). 'Diagnosis and mitigation of smart cyber-attacks on an offshore wind farm network operator'. In 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 479–84. Victoria, BC, Canada: IEEE. https://doi.org/10.1109/ICPS49255.2021.9468268

Balmforth, T. & Richardson, A. (2023). 'Russia attacks Ukrainian energy system 60 times ahead of winter – Kyiv'. Reuters, 8 November 2023. https://www.reuters.com/world/europe/russia-attacks-ukrainian-energy-system-60-times-ahead-winter-kyiv-2023-11-08/

BBC (2019). 'Norway finds "Russian spy whale" off Arctic coast'. BBC News, 29 April 2019. https://www.bbc.com/news/world-europe-48090616

Belyi, A. & Piebalgs, A. (2024). 'Europe's energy challenges: security and infrastructure in a dangerous landscape'. EUI.

Berling, T. V. & Lund Petersen, K. (2020). 'Designing resilience for security in the Nordic region'. In Larsson, S. & Rhinard, M. (eds) Implications for Strategy. Routledge New Security Studies. London: Routledge, pp 131–53. https://www.diis.dk/node/24270

Berling, T. V., Christensen, L. W., Cordes, M., Hansen, F. S., Jakobsson, A. K., Puck-Nielsen, A., Nissen, C. et al. (2023). Nærområdet. Copenhagen: DIIS working paper 2023: 05.

BNS (2023a). 'Lithuania to re-establish coast guard unit'. Lrt.lt, 15 September 2023. https://www.lrt.lt/en/news-in-english/19/2078130/lithuania-to-re-establish-coast-guard-unit

——— (2023b). 'Lithuania to buy underwater surveillance system to shield LNG terminal'. Lrt.Lt, 20 October 2023. https://www.lrt.lt/en/news-in-english/19/2105180/lithuania-to-buy-underwater-surveillance-system-to-shield-lng-terminal

Bollen, M. & Kalkman, J. P. (2022). 'Civil–military cooperation in disaster and emergency response'. Marine Corps University. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-13-no-1/Civil-Military-Cooperation-in-Disaster-and-Emergency-Response/

Bueger, Christian, and Timothy Edmunds. 2023. 'Maritime Security and the Wind. Threats and Risks to Renewable Energy Infrastructures Offshore'. https://doi.org/10.13140/RG.2.2.23647.64167

Bueger, C., Liebetrau, T. & Stockbruegger, J. (2023). 'Theorizing infrastructures in global politics'. International Studies Quarterly 67(4): sqad101. https://doi.org/10.1093/isq/sqad101

Chiappa, C. & Ngendakumana, P. E. (2023). '"Everything indicates" Chinese ship damaged Baltic pipeline on purpose, Finland says'. Politico, 1 December 2023. https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/

Cilliers, J. (2023). 'Uncovering the reality of Ukraine's decimated energy infrastructure'. UNDP, 2023. https://www.undp.org/ukraine/blog/uncovering-reality-ukraines-decimated-energy-infrastructure

Cordes, M., Czub, S., Kot, B., Kozłowski, A., Krenczyk, S., Przybyło, P., Pszczel R. & Smura, T. (2023). Central and Eastern Europe (CEE) as a New Centre of Gravity. Recommendation on Strengthening Regional, European and Transatlantic Security, Edited by Katarzyna Pisarska and Tomasz Smura. Fundacja Im. Kazimierza Pułaskiego.

Council of the European Union (2023). Revised EU Maritime Security Strategy (EUMSS) and Its Action Plan.

DeYoung, K. (2023). 'Russia, blaming U.S. sabotage, calls for U.N. probe of Nord Stream'. The Washington Post, 22 February 2023. https://www.washingtonpost.com/national-security/2023/02/22/russia-un-nord-stream-hersh-investigation/

DRTV – Skyggekrigen (2023). https://www.dr.dk/drtv/serie/skyggekrigen_382298

DW News (2021). 'NATO scrambled jets 290 times over Russian planes in 2021 – DW – 12/28/2021'. 28 December 2021. Dw.Com. https://www.dw.com/en/nato-scrambled-jets-290-times-due-to-russian-planes-in-2021/a-60271618

Elliot, S. (2023a). 'Russian gas flows to Europe hit seven-month high on TurkStream record | S&P global commodity insights'. S&P Global, 2 August 2023. https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/natural-gas/080223-russian-gas-flows-to-europe-hit-seven-month-high-on-turkstream-record

——— (2023b). 'With much of the European market lost, Gazprom looks closer to home'. S&P Global Commodity Insights, 24 February 2023. https://www.spglobal.com/commodityinsights/en/market-insights/blogs/natural-gas/022423-russia-ukraine-gazprom-european-market

European Commission (2022). 'REPowerEU: affordable, secure and sustainable energy for Europe'. 18 May 2022. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_en

——— (2023a). 'Renewable Energy Directive'. European Commission. https://energy.ec.europa.eu/topics/renewable-energy/renewable-energy-directive-targets-and-rules/renewable-energy-directive_en

——— (2023b). 'European cybersecurity is getting its own legs to stand on'. Research and Innovation, 8 February 2023. https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine/european-cybersecurity-getting-its-own-legs-stand

——— (2024). 'Renewable energy targets'. https://energy.ec.europa.eu/topics/renewable-energy/renewable-energy-directive-targets-and-rules/renewable-energy-targets_en

European Council (2008). Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance). OJ L. Vol. 345. http://data.europa.eu/eli/dir/2008/114/oj/eng

——— (2023). 'Maritime security'. 6 December 2023. https://www.consilium.europa.eu/en/policies/maritime-security/

European Parliament (2018). 'Energy as a tool of foreign policy of authoritarian states'. In Particular Russia. Policy Department for External Relations Directorate General for External Policies of the Union.

Faulconbridge, G. & Ravikumar, S. (2022). 'Russia says UK Navy blew up Nord Stream: London denies involvement'. Reuters, 29 October 2022. https://www.reuters.com/world/europe/russia-says-british-navy-personnel-blew-up-nord-stream-gas-pipelines-2022-10-29/

FishSAFE (2024). 'Subsea safety zones'. FishSAFE, n.d. https://fishsafe.org/en/safety-zones/subsea-safety-zones/

Fridbertsson, N. T. (2023). 'Protecting critical maritime infrastructure: the role of technology'. NATO PA.

Giles, K. & Hartmann, K. (2021). 'Adversary targeting of civilian telecommunications infrastructure'. In 2021 13th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia, pp 133–50: IEEE. https://doi.org/10.23919/CyCon51939.2021.9468303

González-García, J., Gómez-Espinosa, A., Cuan-Urquizo, E., García-Valdovinos, L. G., Salgado-Jiménez, T. & Cabello, J. A. E. (2020). 'Autonomous underwater vehicles: localization, navigation, and communication for collaborative missions'. Applied Sciences 10(4): 1256. https://doi.org/10.3390/app10041256

Grant, A. (2022). 'Russian spy ship lurks above key gas pipeline'. The New York Sun, 23 December 2022. https://www.nysun.com/article/russian-spy-ship-lurks-above-key-gas-pipeline

Herzog, S. (2011). 'Revisiting the Estonian cyberattacks: digital threats and multinational responses'. Journal of Strategic Security 4(2): 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Humphries, C. & Macfie, N. (2023). 'Poland, Baltics will shut Belarus border if "critical Incident" Occurs'. Reuters, 28 August 2023. https://www.reuters.com/world/europe/poland-baltics-will-shut-belarus-border-if-critical-incident-occurs-minister-2023-08-28/

IBM Security (2022). 'Cost of a data breach. Report 2022'.

James, L. (2023). 'Russian ships "plotting sabotage in the North Sea"'. The Independent, 19 April 2023. https://www.independent.co.uk/news/world/europe/russia-ships-sabotage-north-sea-b2322747.html

Kshetri, N. & Voas, J. (2017). 'Hacking power grids: a current problem'. Computer 50(12): 91–95. https://doi.org/10.1109/MC.2017.4451203

Lesman, U. (2023). 'Wojewoda Zachodniopomorski zamknął dostęp do terminala LNG. Na wniosek ABW'. Rzeczpospolita, 12 April 2023. https://energia.rp.pl/gaz/art38301541-abw-nakazuje-mocniej-chronic-gazoport-w-swinoujsciu

Lillywhite, L. & Wakefield, B. (2021). 'New roles for military in health emergency preparedness'. Chatham House – International Affairs Think Tank. 27 August 2021. https://www.chathamhouse.org/2021/08/new-roles-military-health-emergency-preparedness

Liu, H. & Tronchetti, F. (2019). 'Regulating near-space activities: using the precedent of the exclusive economic zone as a model?' Ocean Development & International Law, July. https://www.tandfonline.com/doi/full/10.1080/00908320.2018.1548452

Marsh, S. & Chambers, M. (2022). 'Germany freezes Nord Stream 2 gas project as Ukraine crisis deepens'. Reuters, 22 February 2022. https://www.reuters.com/business/energy/germanys-scholz-halts-nord-stream-2-certification-2022-02-22/

Miętkiewicz, R. (2021). 'LNG supplies' security with autonomous maritime systems at terminals' areas'. Safety Science 142(October): 105397. https://doi.org/10.1016/j.ssci.2021.105397

Moore, M., Wermuth, M. A., Werber, L., Chandra, A., Noricks, D., Resnick, A. C., Chu, C. & Burks, J. J. (2010). 'Bridging the gap: developing a tool to support local civilian and military disaster preparedness'. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/technical_reports/TR764.html

NATO (2019). 'NATO review: resilience: the first line of defence'. NATO Review. 27 February 2019. https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

——— (2023a). 'NATO: opinion: doorstep statement by NATO Secretary General Jens Stoltenberg ahead of the meeting of NATO Ministers of Defence in Brussels, 15 June 2023'. https://www.nato.int/cps/en/natohq/opinions_215676.htm?selectedLocale=en

——— (2023b). 'NATO exercises with new maritime unmanned systems in Portugal'. NATO (blog). 18 September 2023. https://www.nato.int/cps/en/natohq/news_218545.htm

——— (2023c). 'NATO intercepted Russian military aircraft over 300 times in 2023'. 29 December 2023. https://www.nato.int/cps/en/natohq/news_221598.htm

Plėta, T., Tvaronavičienė, M., Della Casa, S., & Agafonov, K. (2020). 'Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases'. Insights into Regional Development 2(3): 703–15. https://doi.org/10.9770/IRD.2020.2.3(7)

Ponomarev, K. (2023). '15 years after Russo–Georgian War, Russian emigres confront conflict's complicated legacy'. The Moscow Times, 14 August 2023. https://www.themoscowtimes.com/2023/08/11/15-years-after-russo-georgian-war-russian-emigres-confront-conflicts-complicated-legacy-a82097

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler Mclellan, and Chris Sistrunk. 2023. 'Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology | Mandiant'. Mandiant, 2023. https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

Pryšmantas, Valdas. 2023. 'Lithuania's LNG Terminal to Boost Anti-Drone Protection'. Lrt.Lt, 22 May 2023. https://www.lrt.lt/en/news-in-english/19/1995094/lithuania-s-lng-terminal-to-boost-anti-drone-protection

Pursiainen, C. (2018). 'Critical infrastructure resilience: a Nordic model in the making?' International Journal of Disaster Risk Reduction 27(March): 632–41. https://doi.org/10.1016/j.ijdrr.2017.08.006

Radowitz, B. (2023). 'Alarm bells sound in Nordics over Russian offshore wind "sabotage planning"'. Recharge | Latest Renewable Energy News, 19 April 2023, sec. wind. https://www.rechargenews.com/wind/alarm-bells-sound-in-nordics-over-russian-offshore-wind-sabotage-planning/2-1-1437466

Rajkumar, V. S., Tealane, M., Stefanov, A. & Palensky, P. (2019). 'Cyberattacks on protective relays in digital substations and impact analysis'. In 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES). Montreal, QC, Canada: IEEE.

Ramm, A. (2016). 'Russian "harmony" for maritime surveillance'. Russia Beyond, 30 November 2016. https://www.rbth.com/economics/defence/2016/11/30/russian-harmony-for-maritime-surveillance_652217

Ritzau (2023). 'Repairing Baltic Sea pipeline will take at least five months'. Energy Watch, 12 October 2023. https://energywatch.com/EnergyNews/Oil___Gas/article16507190.ece

Rumer, E. (2021). 'Even a major military exercise like Zapad can't fix some of the biggest security challenges facing Russia'. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/09/21/even-major-military-exercise-like-zapad-can-t-fix-some-of-biggest-security-challenges-facing-russia-pub-85397

Ryzhenko, A. (2022). 'Nord Stream explosions: Russian sabotage in the Baltic?' Jamestown. https://jamestown.org/program/nord-stream-explosions-russian-sabotage-in-the-baltic/

SAAB (2023). 'Saab collaborates in NATO underwater exercises'. Start (blog). https://www.saab.com/newsroom/press-releases/2023/saab-collaborates-in-nato-underwater-exercises

Schubert, S. R., Pollak, J. & Brutschin, E. (2014). 'Two futures: EU–Russia relations in the context of Ukraine'. European Journal of Futures Research 2(1): 52. https://doi.org/10.1007/s40309-014-0052-7

SektorCERT, Om. 2023. 'Analyse Detaljeret Analyse Af Sagen'.

Slakaityte, V. & Surwillo, I. (2024). Energy as a Weapon: Decoding Blackmail Tactics in Europe. Copenhagen: DIIS.

Slakaityte, V., Surwillo, I., Berling, T. V. (2023). 'A New Cooperation Agenda for European Energy Security'. Nature Energy 8 (10): 1051–53. https://doi.org/10.1038/s41560-023-01322-8

Soldi, G., Gaglione, D., Forti, N., Di Simone, A., Daffinà, F. C., Bottini, G., Quattrociocchi, D. et al. (2021). 'Space-based global maritime surveillance: Part II: artificial intelligence and data fusion techniques'. IEEE Aerospace and Electronic Systems Magazine 36(9): 30–42. https://doi.org/10.1109/MAES.2021.3070884

Staggs, J., Ferlemann, D. & Shenoi, S. (2017). 'Wind farm security: attack surface, targets, scenarios and mitigation'. International Journal of Critical Infrastructure Protection 17(June): 3–14. https://doi.org/10.1016/j.ijcip.2017.03.001

Statista (2023a). 'Nord Stream physical flows daily 2023'. https://www.statista.com/statistics/1331710/nord-stream-physical-flows/

——— (2023b). 'U.S. and EU: installed wind power capacity 2022'. Statista. https://www.statista.com/statistics/215646/cumulative-installed-wind-power-capacity-in-the-us-and-the-eu/

Surwillo, I. & Slakaityte, V. (2022). 'Fortifying the EU's eastern border countering hybrid attacks from Belarus'. Copenhagen: DIIS Policy Brief, 4 March 2022.

Task Force (2023). 'Ukrainian energy sector evaluation and damage assessment: X (as of May 24, 2023): cooperation for restoring the Ukrainian energy infrastructure project'. International Energy Charter.

The Maritime Exclusive (2023). 'Seismic station detected possible blast during Baltic gas line breach'. The Maritime Executive, 11 October 2023. https://maritime-executive.com/article/seismic-station-detected-possible-blast-during-baltic-gas-line-breach

Torres, F. S., Kulev, N., Skobiej, B., Meyer, M., Eichhorn, O. & Schafer-Frey, J. (2020). 'Indicator-based safety and security assessment of offshore wind farms'. In 2020 Resilience Week (RWS): 26–33. Salt Lake City, UT, USA: IEEE. https://doi.org/10.1109/RWS50334.2020.9241287

Umbach, F. (2023). 'New challenges in protecting critical EU infrastructure'. GIS Reports (blog), 6 February 2023. https://www.gisreportsonline.com/r/europe-critical-infrastructure/

United Nations (1982). 'United Nations Convention on the Law of the Sea'.

Vatman, T. & Hart, C. (2024). 'Russia's attacks on Ukraine's energy sector have escalated again as winter sets in: Analysis'. IEA. 2024. https://www.iea.org/commentaries/russias-attacks-on-ukraines-energy-sector-have-escalated-again-as-winter-sets-in

Vincent, E. & Pietralunga, C. (2023). 'Cyberattacks on the rise in Europe amidst the war in Ukraine'. Le Monde, 3 April 2023. https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html

Tyranowski, Jerzy. 1972. Traktaty Sojusznicze Polski Ludowej. Warzaw.

Walker, Shaun. 2014. 'Ukraine Demanding Return of Combat Dolphins from Russia'. The Guardian, 6 July 2014, sec. World news. https://www.theguardian.com/world/short-cuts/2014/jul/06/ukraine-combat-dolphins-russia-give-back

Willett, M. (2022). 'The cyber dimension of the Russia–Ukraine War'. Survival 64(5): 7–26. https://doi.org/10.1080/00396338.2022.2126193

Гавриленко, Алексей (2019). 'ГУГИ – Подводный Спецназ Российского Генштаба – Новости РуАН'. 2019. http://xn----ctbsbazhbctieai.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/%D0%B3%D1%83%D0%B3%D0%B8-%D0%BF%D0%BE%D0%B4%D0%B2%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9-%D1%81%D0%BF%D0%B5%D1%86%D0%BD%D0%B0%D0%B7-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B3%D0%BE-%D0%B3%D0%B5%D0%BD%D1%88%D1%82%D0%B0%D0%B1%D0%B0/

Головатенко, О. (2022). 'Факты ЛРТ. Украина. Энергетический Террор: Как Путин Пытался Запугать Украинцев и Почему Это Агония? - LRT', 2022. https://www.lrt.lt/ru/novosti/17/1802540/fakty-lrt-ukraina-energeticheskii-terror-kak-putin-pytalsia-za-pugat-ukraintsev-i-pochemu-eto-agoniia

ЖДАНОВ, ВИКТОР (2022). '«Надо Вогнать Украину в Каменный Век»: Эксперт Рассказал Об Уничтоженной Инфраструктуре'. 17 October 2022. https://www.mk.ru/politics/2022/10/17/nado-vognat-ukrainu-v-kamennyy-vek-ekspert-rasskazal-ob-unichtozhennoy-infrastrukture.html

Инь, Ж. & Чжон, К. (2023). 'Взрывы «Северного Потока» и Стоящая За Ними Геополитическая Игра'. Социальная и Экономическая География.

Риа Н. (2023). 'Посол Объяснил, Почему Дания Боится Расследования По "Северным Потокам"'. РИА Новости, 2023, sec. Новости. https://ria.ru/20230925/daniya-1898403658.html

DIIS · Danish Institute for International Studies

The Danish Institute for International Studies is a leading public institute for independent research and analysis of international affairs. We conduct and communicate multidisciplinary research on globalisation, security, development and foreign policy. DIIS aims to use our research results to influence the agenda in research, policy and public debate, and we put great effort into informing policymakers and the public of our results and their possible applications.

Defence and Security Studies at DIIS

This publication is part of the Defence and Security Studies at DIIS. The aim of these studies is to provide multidisciplinary in-depth knowledge on topics that are central for Danish defence and security policy, both current and long-term. The design and the conclusions of the research under the Defence and Security Studies are entirely independent. All reports are peer-reviewed. Conclusions do not reflect the views of the ministries or any other government agency involved, nor do they constitute an official DIIS position. Additional information about DIIS and our Defence and Security Studies can be found at www.diis.dk.

Subscribe to DIIS's Newsletter

DIIS · DANISH INSTITUTE FOR INTERNATIONAL STUDIES
Gl. Kalkbrænderi Vej 51A | DK-2100 Copenhagen | Denmark | www.diis.dk