European Initiative *for* Energy Security

ENERGY SECURITY LEADERSHIP COUNCIL EUROPE

BUILDING ENERGY RESILIENCE FROM THE SEABED UP

Amb. Andris Piebalgs, Dr. Benjamin L. Schmitt, and Dr. Frank Umbach

July 2024

Introduction

For over a century, Russian strategists have understood the critical role of energy, especially electricity, in national cohesion and resiliency. Lenin famously identified national electrification, together with Soviet power, as the critical element in building Communism. The corollary, that in conflict or war energy infrastructure is a critical target in breaking an enemy's capacity or will to resist, is center stage today at a time when modern technology and the increasing role of electricity in everyday life have magnified the opportunity and challenges posed by the energy weapon.

Putin's use of energy so far is a logical extension of Lenin's insight into modern conflict.

1. First, by gradually ensnaring Europe in deep dependency on Russian energy to sustain its industry and warm its homes, giving the Kremlin political leverage on the West.
2. Then by targeting Ukrainian energy infrastructure to disrupt defence and industrial capacity and civilian life and weaken morale.
3. And in suspected hybrid attacks from the Baltic to the United Kingdom – some relatively low-level, others more impactful – that so far appear to be a shot across the bow and warning of things to come to forestall more forceful actions from NATO and the European Union to support Ukraine.

In this publication, three experts on energy and infrastructure security – from Latvia, Germany and the United States – examine Russian strategies to date, analyze recent Russian actions in Europe, confirmed and suspected, and discuss ways Europe and the U.S., as nations and in multinational organizations like NATO and the EU, can harden their energy infrastructure, build in resilience, and devalue, dissuade and if necessary, defeat the Russian threat. As we build out clean offshore energy infrastructure to reduce dangerous dependencies, meet growing electricity demands, and improve net energy security, addressing vulnerabilities of both old and new systems is critical.

Their key recommendations, as the EU enters a new policy cycle and NATO's Washington Summit kicks off, are listed below.

1. Our interconnected energy infrastructure is vulnerable not just to cyber but also physical threats, particularly as we invest in the necessary expansion of our offshore wind and grid capacity. While cyber protection must remain a priority and evolve to match the threat, we need policies and technical solutions that can help protect critical infrastructure from physical attacks and sabotage.
2. Resilience must be integral to the design of the energy sector, with all stakeholders involved, and will cost money and change investment and ROI assumptions. When deploying or upgrading critical infrastructure, resilience capabilities should be adequately financed, installed and integrated "by design" by public and private actors.
3. Russia's targeting of Ukraine's energy system underlines the importance of diversified energy infrastructure, interconnectivity, flexibility resources, distributed generation, and a secure and steady supply of replacement parts and repair materials such as power cables, transformers, and generators.
4. NATO and the EU should increase their support for the protection of Ukraine's energy infrastructure through further investments in both active air defense, counter-drone, and passive defense systems. The West must learn from Ukraine's example that the protection of energy infrastructure is a high priority to deter the Kremlin and defeat Russia's strategy.
5. Infrastructure resilience challenges existing institutional boundaries. Progress has been made, but even greater communication and cooperation between the EU, NATO and industry is essential to create synergies through collective action and must be increased, building on the 2023 launch of the EU-NATO Task Force on Resilience of Critical Infrastructure and other recent NATO and EU initiatives.
6. EU and NATO members need holistic national security concepts that include effective crisis mechanisms, with clearly defined responsibilities for operators of critical infrastructure and national and regional administrations, and effective points of contact for NATO and EU institutions.
7. NATO must take action to ensure the expansion and enhanced physical monitoring and protection of its own energy network. The Alliance should work to push forward vital investments, such as increasing the involvement of the commercial geospatial industry in critical infrastructure.
8. Antimonopoly policy frameworks deployed as part of the EU's Third Energy Package have been effective at undermining Russia's ability to use energy as a geopolitical tool. Energy market liberalization must be sustained to support economic security.
9. Sanctions and technology export controls enforcement aimed at Russia's energy sector must be sustained, as they can have a direct impact in supporting Ukraine on the battlefield. Transatlantic leaders must remain firm that there can be no return to "energy business as usual" with Putin's Kremlin.

ABOUT EIES

European Initiative *for* Energy Security

The European Initiative for Energy Security (EIES) advocates for secure pan-European and national energy policies, dedicated to fostering collaboration between government and industry leaders. EIES seeks to address critical energy challenges and champion comprehensive solutions for the benefit of Europe's energy security, transition, and industrial competitiveness. EIES works with the Energy Security Leadership Council-Europe (ESLC-Europe), composed of retired and active military, political and business figures, to achieve these goals. While launched through SAFE, EIES maintains independence from SAFE in its research and policy positions. Learn more at SecureEnergyEurope.org

LEARNING FROM RUSSIA'S TARGETING OF UKRAINIAN AND EUROPEAN ENERGY INFRASTRUCTURE

By Amb. Andris Piebalgs

Andris Piebalgs is a Professor at the European University Institute and a member of EIES' Energy Security Leadership Council-Europe. He is the Chairman of the Implementation Committee of the International Methane Emissions Observatory. He is a former EU Commissioner for Energy and EU Commissioner for Development, a key figure in the formation of the EU's renewable energy and energy efficiency policies, and was instrumental in the creation of the European energy market. Piebalgs has a distinguished carrier as a Latvian politician and diplomat. As Latvia's Ambassador to the EU, he played an important role in Latvia's EU accession.

Destroying Ukraine's energy infrastructure: a comprehensive and evolving strategy

The full-scale invasion of Ukraine, which began on February 24, 2022, has imparted several crucial lessons about the vulnerabilities and resilience of critical infrastructure in the face of targeted military aggression. From the outset, Ukraine's energy infrastructure has been a primary target of Russian forces. The most significant blackout occurred on November 23, 2022, symbolizing the extensive damage inflicted throughout the winter of 2022-2023. From October 10 to the end of December 2022, Ukrainian households endured an average of five cumulative weeks without electricity.

From the beginning, Russia's strategy prioritized attacking Ukraine's energy infrastructure to disrupt daily life and weaken morale, first targeting power plants, the grid, and electricity substations. Since early 2024, gas storage sites have also been increasingly targeted, as these facilities are also used by other European countries to store gas reserves. A report by the Yale Humanitarian Research Lab, released on February 29, 2024, documented 223 verified attacks on Ukraine's power-generation-and-transmission infrastructure between October 1, 2022, and April 30, 2023. This equates to over seven attacks per week, with peak impact during the winter months. The sustained focus on energy infrastructure highlights its strategic importance in modern warfare.

The attacks were comprehensive and meticulously planned. With over 1,200 missiles and drones used by 2023, and hundreds of cyberattacks per month, the destruction was both extensive and systematic. On May 8, 2024, for example, 12 power facilities were struck in a single day. Thermal and hydropower facilities, along with power transmission systems, bore the brunt of these attacks, resulting in the loss of about 80% on Ukraine's thermal power generation capacity. This level of destruction underscores the effectiveness of well-prepared strikes aimed at crippling essential services.

Repercussions on the well-being of the Ukrainian population have been severe, compromising water supply, hindering humanitarian assistance, and causing prolonged blackouts that adversely affected millions of households. Children's education was disrupted, older persons and individuals with disabilities faced mobility challenges, and many were left without essential services for heating, cooking, and hygiene. The targeting of combined heat and power facilities in urban centers will prove especially challenging as we approach the coming winter. In Kharkiv, all such facilities have now been destroyed.

The lack of access to energy has serious implications for a country's defense capacity and economy. Energy shortages cripple industrial activities, hinder economic growth, and weaken national defense capabilities, and the extensive damage inflicted upon Ukraine's energy infrastructure underscores the importance of a resilient energy system and the necessity for Europe of **identifying and protecting critical infrastructure** – including, in Ukraine's urgent case, with air defense systems. Ukraine's efforts to strengthen passive protection, such as safeguarding autotransformers from drones and key substations from missiles, were crucial steps. However, the scale of the attacks revealed vulnerabilities that need to be addressed more robustly to withstand such targeted destruction.

One critical aspect of Russia's attacks is the focus on **flexibility resources**. By targeting facilities essential for balancing the power grid, Russian forces made it challenging for Ukraine to manage its energy supply. This strategic targeting created widespread and prolonged blackouts, severely disrupting civilian life and economic activities. The emphasis on flexibility resources highlights the importance of protecting these assets to maintain supply stability during conflicts.

Another vital lesson from the conflict is the need for well-prepared **supply chains for backup equipment**. Ukraine's power system faced significant electricity shortages, with the available capacity of transmission system transformers in February 2024 being 32% lower than at the beginning of 2022. The urgent need for flexible capacities, such as gas turbine generators, and backup components like power cables and transformers, became evident. Ensuring a steady supply of replacement parts and repair materials is essential for quick recovery and maintaining operational integrity.

The conflict also highlighted the role of **distributed generation** in enhancing resilience. With centralized facilities being prime targets, diversifying energy sources and incorporating distributed generation can help mitigate the impact of attacks. This approach can provide localized power generation, reducing the strain on the national grid and ensuring more stable electricity supply during crises.

The international community's response has also been crucial in countering the devastation. From May 2023 to January 2024, Ukraine activated emergency support from neighboring ENTSO-E countries 33 times. On average now, emergency aid from EU countries was needed every second day, emphasizing the critical role of **international cooperation and solidarity** in addressing energy deficits. However, the growing difficulty in securing funds and equipment highlights the need for sustained and coordinated support.

The systematic destruction of Ukraine's energy infrastructure has provided several vital lessons, including the prior identification of critical infrastructure and deployment of robust defences against air, missile, and other attacks, the importance of flexibility resources and well-prepared and resilient supply chains, and the critical role of distributed generation and international support to address the severe humanitarian impact of energy shortages. By rapidly incorporating these lessons, Ukraine and other nations can develop strategies to better protect their critical infrastructure and enhance resilience against future threats.

European energy sector infrastructure resilience: the fourth dimension of energy policy

Beyond the pressing Ukrainian case, Europe as a continent is grappling with the convergence of geopolitical, cyber, and physical threats to its expansive energy infrastructure. Central to these concerns is the looming question: how real is the Russian threat to Europe's energy infrastructure? Recent events and historical patterns show this threat, particularly to gas pipelines and offshore wind projects in the North Sea and other areas, cannot be underestimated.

The sabotage of the Nord Stream gas pipelines in September 2022 starkly reminded us of the volatile security context surrounding Europe's critical infrastructure. This vulnerability is not exclusive to Europe or the seabed. In the U.S., a 2013 attack on a power substation near San Jose, and a similar incident in North Carolina which led to significant power outages nine years later highlight the reality of the dangers posed by **physical assaults** on electricity equipment.

Orchestrated **cyberattacks**, such as those in Ukraine in 2015, also demonstrate the capabilities of external actors to exploit vulnerabilities. The Ukrainian power outages, affecting 225,000 customers, were the result of sophisticated cyber intrusions, not physical tampering. Russia's longstanding targeting of Ukraine illustrates how critical infrastructure can be compromised through various methods, ranging from espionage and cyberattacks to physical strikes and acts of sabotage.

The case of the **Balticconnector** is a clear call to action for Europe. The subsea gas link between Estonia and Finland was severely damaged in October 2023, taking half a year to repair. Finnish authorities have identified a Hong Kong-flagged container ship as the prime suspect, though the investigation is ongoing. The damage to the Balticconnector occurred one year after the explosions in 2022 that destroyed the larger Nord Stream pipelines. Despite increased vigilance, the damage was done, and it took two days after a rapid reduction in pipeline pressure to discover the rupture. In the meantime the ship was able to continue its course unmolested by authorities towards Arkhangelsk, Russia. To further complicate the matter, two subsea telecommunications cables - the FEC cable between Finland and Estonia and the EE-S1 cable between Estonia and Sweden - were also damaged around the same time, seemingly by the same ship anchor that destroyed the pipeline, highlighting increasing challenges in protecting subsea infrastructure.

European energy infrastructure, spanning thousands of kilometres in pipelines, electricity lines, and cables, presents unique challenges. A single attack on a strategic location, such as a hydroelectric dam, can wreak havoc on vast areas. The **interconnected nature** of these infrastructures means disruptions in one area can cascade, impacting regions far removed from the initial incident. Their digitalisation renders them susceptible to cyberattacks and digital disruptions. With the EU's projected power demand set to soar by 80% by 2050, these vulnerabilities will likely become more pronounced, and must be addressed.

Europe's commitment to sustainable energy solutions, evidenced by robust investment in **offshore wind farms**, brings its own set of challenges. The scale and remoteness of these offshore installations make them vulnerable to cable theft, vandalism, ship collisions, and terrorism. The growth of wind turbines, in terms of height and rotor diameter, has increased these vulnerabilities as they entail longer and more complex cables, raising the stakes in case of failures. Various factors, both human and natural, can contribute to these damages, and the financial implications can be daunting. As wind farms expand further offshore into deeper waters, installation and repair complexities multiply.

Recognizing these challenges, the EU has fortified its **legal and policy framework** for protecting critical infrastructure. Directives like the Critical Entities Resilience (CER Directive) and the

Directive for a high common level of cybersecurity across the Union (NIS 2 Directive) emphasize the need for member states to enhance the resilience of critical entities and prepare for potential threats. Implementing cybersecurity best practices, such as procuring trusted hardware and software systems, is paramount.

The establishment of the Critical Entities Resilience Group and the adoption of the Critical Infrastructure Resilience Recommendation in December 2022 further underscore the EU's commitment to strengthening infrastructure resilience. **Collaborative efforts with NATO**, exemplified by the launch of the EU-NATO Task Force on resilience of critical infrastructure in March 2023, will create synergies through collective action.

In a world increasingly characterised by sophisticated threats to critical infrastructure, Europe faces a Herculean task. Its vast and interconnected energy infrastructure, coupled with its commitment to the expansion of sustainable solutions like offshore wind farms, presents unique vulnerabilities. The energy trilemma of security, sustainability, and affordability now demands a new layer: resilience. **Resilience** should be integral to the design of the energy sector, with all stakeholders involved.

The comprehensive destruction of Ukraine's energy infrastructure reveals Russia's evolving strategy. Europe must learn from these events, the damage already inflicted on its own energy infrastructure, and the political mistakes that led to the major energy crisis of the last two years. With concerted efforts, robust policy frameworks, and collaborative initiatives, Europe can navigate these challenges and ensure a secure energy future for its citizens.

RESPONDING TO RUSSIA'S LONGSTANDING WEAPONISATION OF ENERGY

By Dr. Benjamin L. Schmitt

Dr. Schmitt is a Senior Fellow at the Department of Physics and Astronomy and the Kleinman Center for Energy Policy at the University of Pennsylvania, a Senior Fellow for Democratic Resilience at the Center for European Policy Analysis (CEPA), an associate of the Harvard-Ukrainian Research Institute, a fellow of the Duke University "Rethinking Diplomacy" Program, and a Term Member of the Council on Foreign Relations. (X: @BLSchmitt).

Russia's historical weaponization of energy: evolving and intensifying

As the previous piece has demonstrated, Russia's large-scale campaign of kinetic strikes against Ukraine's energy infrastructure has laid bare how the Russian Federation under Vladimir Putin has **evolved its decades-long strategy of weaponizing energy against the European continent from a broad geopolitical instrument, into an acute military one**. Indeed, for many years, Putin's Kremlin has advanced a strategy, especially via pipeline gas exports, of pursuing monopolistic positions for Kremlin-controlled Gazprom along its energy export pipelines to Europe. Russia has then parlayed those positions to be utilized as instruments of political coercion, either via the threat of or overt gas cutoffs to European nations in exchange for explicitly stated or implicit political concessions.

Via these cutoffs, the Putin regime was able to use its traditional energy position across the continent as a means of **political blackmail** against European democracies. This not only includes the myriad of politically-motivated cutoffs by Russia of the Ukrainian gas transmission system over the past two decades, including notable events in 2009, 2014, 2015, and 2018, but high-profile events in the months before Russia's large-scale invasion of Ukraine in February 2022. These included Russia overtly linking political demands in exchange for gas supplies, including reports that in October 2021, the Kremlin attempted to coerce Moldova into dropping its EU aspirations in exchange for a new Gazprom contract.

Likewise, Russia weaponized gas supplies in the months leading up to its large-scale invasion of Ukraine by declining to take normal market action to inject gas volumes into European storages throughout 2021 and into early 2022 – including many at least partially owned by Gazprom – resulting in wintertime gas scarcity across the European Union. Moreover, in the opening months following Russia's illegal widespread invasion of Ukraine in February 2022, Putin's Kremlin attempted to further **foment an energy crisis** within Europe's democracies, initiating gas cutoffs and reductions along its primary pipeline export routes to Europe.

For example, in April 2022, the Kremlin announced it would be halting gas supplies to Poland and Bulgaria in response to their (entirely justified) refusal to follow a legally-dubious "decree" announced by the Kremlin in March 2022 that all gas payments needed to be made to Gazprom in rubles rather than in dollars or euros as was specified in existing supply contracts. Furthermore, starting in June 2022, the Kremlin began a series of gas cuts along the trans-Baltic Sea **Nord Stream** 1 pipeline route, first cutting the supply volume by 60% beginning on 15 June 2022, then by 80% on 25 July 2022, and then fully stopping gas transit via the pipeline by 2 September 2022.

Throughout Summer 2022, the Kremlin's justification for these cuts were based on another dubious claim – that technical issues at the Russian compressor station required the lifting of sanctions by Canada on Siemens gas-fired turbines that were undergoing maintenance in Montreal. Despite officials from the German government making strong public claims debunking this justification, and pointing to political motivations for this latest set of Russian cuts, the Canadian government eventually acceded to pressure that nevertheless came from Berlin and lifted technology export controls on one of the turbines, which was sent to Germany for onward transit to Russia. Of course, the turbine was never collected by Gazprom, further underscoring the falsehood of a "technical" reason for the cutoffs.

In the end, the political coercion reading of the Kremlin's motivation for the Nord Stream 1 cuts needed no further analysis: on 5 September 2022, Kremlin spokesperson Dmitry Peskov directly cited the desire of the Russian government for the sanctions levied against Moscow by the EU in response to Russia's reinvasion of Ukraine to be lifted for gas transit to resume along the route. Peskov at the time also cynically confirmed that previous Kremlin claims about the "technical" justification for the cuts on Nord Stream 1 were nothing but lies when he added, "other reasons that would cause problems with the pumping don't exist."

Understanding this long-term context demonstrating the phases of politically motivated Russian energy weaponization against Europe is vital given the trends that emerged from Fall 2022 until today. If deliberate Russian gas undersupply across 2021 and high-profile gas cuts to Europe in the opening months of Russia's large-scale war against Ukraine were motivated by a desire to undermine the ability of Western leaders to muster political support for Ukraine's defense and reduce the latitude leaders would have to push back on Russian aggression, the very same motivation can be viewed as the likely cause of Kremlin actions since late 2022.

Most notably, the continuous campaign that the Russian military has launched **targeting Ukrainian civil energy and critical infrastructure via brutal kinetic strikes** is similarly motivated by a desire to exacerbate the already widespread humanitarian crisis across Ukraine, with a vain hope that doing so will undermine the resolve of the Ukrainian population to resist Russia's illegal aggression, thus levying political pressure on President Volodymyr Zelensky to make concessions to end the war on Russia's terms. Thankfully, the resolve of the Ukrainian people has been undeterred by these attacks and, while the breadth of energy infrastructure destruction in Ukraine is nearly impossible to repair and replace at scale in real time, **technical support from global democracies** may still help Ukraine avoid the worst outcomes of successive winters spent suffering from Russia's artificially imposed energy poverty.

In parallel to Russia's military devastation of Ukrainian civil energy infrastructure, the threat of **physical attacks and targeted sabotage against European energy infrastructure has become all too real and is no longer an area of European energy policy that can be ignored.** We have already well established this fact, as demonstrated earlier in this publication, including the September 2022 Nord Stream sabotage incident and the damage against the Balticconnector gas pipeline connecting Estonia and Finland in October 2023. While both incidents remain officially unresolved, the presence of Russian subsea warfare vessels in the direct vicinity of the Nord Stream blast sites just days before the September 2022 blasts at least raises the question of direct Russian involvement. Likewise do reports of the presence of an alleged Russian spy ship, the <*ADMIRAL VLADIMIRSKY*> in the vicinity of the Balticconnector damage site in the months before the incident. And additionally concerning are the circumstances surrounding the Russian ownership links of the suspected Chinese-flagged vessel <*NEWNEW POLAR BEAR*> whose anchor is reported to have inflicted damage on the Balticconnector pipeline and nearby telecommunications cables, and its escort vessel at the time of the incident, the Russian nuclear-powered Arctic class container ship <*SEVMORPUT*>.

Since the time of these two high-profile incidents involving the damage to European subsea critical energy infrastructure, the string of suspected Russian sabotage incidents against both onshore energy, transportation, and critical infrastructure has only grown. Furthermore, in many of the most recent cases, European officials are now stating publicly that they suspect they have taken place through the **recruitment of low-level criminals and other European citizens with sympathies toward Moscow by Russia's military intelligence agency, the GRU.**

Among other incidents this year: a German rail line has had been sabotaged via the cutting of vital electricity cables; an arson attack was carried out against a Ukrainian business in east London in which investigators allege GRU support of the arrested individuals who are allegedly involved; German authorities arrested individuals allegedly with Russian ties who are charged with plotting sabotage bombing attacks against targets on German soil, including on U.S. military facilities in the country; and reports emerged that the gas pipeline under construction from the Brunsbüttel LNG terminal at the mouth of the Elbe river, had been sabotaged via the drilling of holes in pipe segments aimed at connecting the terminal with the German gas grid near Hetlingen, Germany.

Like its kinetic military strikes against civil energy infrastructure in Ukraine, the possible Russian targeting of offshore and onshore energy and critical infrastructure across Europe is likely aimed at the same level of political coercion that Russia's earlier gas cutoffs had sought: to force political concessions on given issues, which over the past few years has undoubtedly focused on attempting to **undermine Transatlantic support for Ukraine's defense and to mount pressure on European democracies to lift sanctions and technology export controls measures.**

Providing a transatlantic response

While the motivations may well be the same, the shift in methods by the Kremlin means that the traditional areas of focus that Transatlantic diplomatic efforts have centered on for the past few decades, will need to accordingly expand. For context, the high-level policy frameworks across the EU, and U.S. support for Europe's energy security especially since the rollout of the European Energy Union framework by Brussels in 2015, has focused on two main areas of policy engagement: development of what is sometimes called **the "hardware" and "software"** core to Europe's energy security.

In terms of "hardware," European energy security was bolstered by policies that have supported the **diversification of energy infrastructure**, allowing for a reduction in the overall traditional reliance the continent had on the Russian Federation, and includes many examples, including the aforementioned Balticconnector pipeline, the Swinoujscie LNG import terminal in Poland, and the gas interconnector Greece-Bulgaria (IGB). On the "software" side, European energy security was advanced by the development of **antimonopoly policy frameworks** that would undermine Russia's ability for market manipulation via its state-owned enterprises, most notably measures that were advanced and deployed within the EU Third Energy Package framework, including provisions for third party access and ownership unbundling of European energy infrastructure.

These two areas of European energy security policy, which have been strongly supported by U.S. energy diplomacy efforts over the past decade, must continue, as they have been effective at undermining Russia's ability to use energy as a geopolitical tool, and support **economic security through needed energy market liberalization**. Likewise, other energy policy areas need to be continued, such as increases in **sanctions and technology export controls** enforcement aimed at Russia's energy sector, as they can have a direct impact on EU, U.S., and NATO programs aimed at supporting Ukraine on the battlefield, since they can reduce the funds and materiel that the Kremlin is able to bring to bear against Ukraine.

Moreover, the Transatlantic community needs to urgently continue its work to recognize and counter Russian malign influence in the European energy sector, including passing national legislation in countries on both sides of the Atlantic aiming to **end the ability of former senior officials from democratic nations to take post-government positions working for Russian state-owned energy enterprises**. Legislation that would stop this trend, such as the proposed Stop Helping Adversaries Meddle in Everything, or SHAME Act, that was first introduced in the U.S. Congress in 2022 needs to be passed, and mirroring laws passed across Transatlantic democracies to help counter the erosion of democratic resilience should this practice be allowed to continue. In the end, Transatlantic leaders must remain firm that there **can be no return to "energy business as usual" with Putin's Kremlin ever again.**

But beyond these core policy areas supporting European energy security, Transatlantic leaders must ensure that **policy frameworks and technical solutions that can help protect energy and critical infrastructure** from physical attacks and sabotage incidents are brought to the forefront of energy diplomacy efforts. It should be noted that cyber protections for energy and critical infrastructure have for many years seized the attention of Transatlantic policymakers given the manner by which cyberattacks became an emerging and persistent threat over the past few decades, while policies related to physical threats have perhaps been thought of as more a relic of history. Of course, cyber policy must continue to be a priority and evolve at the speed of the technologies that can manifest the threat. But Russia's recent spate of hybrid attacks – those that don't reach the level of overt military attacks, but are nevertheless aimed at undermining the democratic resilience of European nations – have reminded policymakers on both sides of the Atlantic that new and sophisticated policies aimed at **countering the threat of Russian physical sabotage attacks is again a threat vector in need of urgent attention.**

Fortunately, NATO leaders have begun to elevate their recognition of the vital role that energy security and energy infrastructure protection play in the overall security environment across Europe. In June 2024, NATO Secretary General Jens Stoltenberg himself stressed this new reality in public remarks given in Canada, stating that "...we are threatened by something which is not a full-fledged military attack, which are these hybrid threats ... everything from meddling in our political processes, (undermining) the trust in our political institutions, disinformation, cyber-attacks (...) and sabotage actions against critical infrastructure."

NATO's response to the threat to energy and critical infrastructure has gone far beyond rhetoric. In addition to the **EU-NATO Task Force on resilience of critical infrastructure** mentioned earlier, NATO has also stood up efforts of its own to help advance infrastructure security across the continent. In the wake of the Nord Stream sabotage incidents, on 9 October 2023 the NATO Parliamentary Assembly passed a resolution aimed at "Enhancing the Protection of Allied Critical Maritime Infrastructure," while on 15 February 2023 NATO stood up a **Critical Undersea Infrastructure Coordination Cell** to elevate the strategic policy planning related to this multispectral issue set within the Alliance.

The Alliance followed up these early efforts building on decisions taken at the 2023 NATO Vilnius Summit into this year through the opening of a new **Maritime Center for Security of Critical Undersea Infrastructure** based at Allied Maritime Command (MARCOM) headquarters in Northwood, United Kingdom, which reached its Initial Operational Capability, or IOC, on 28 May 2024. This new MARCOM center will become the de facto operational companion to the policy-focused Critical Undersea Infrastructure Coordination Cell that was opened at NATO Headquarters in 2023, and will "coordinate efforts between NATO Allies, Partners, and the private sector" according to a press release marking the opening of the center. Moreover, NATO is also engaging the expert community through the first meeting of its newly-formed Critical Undersea Infrastructure Network, held on 23 May 2024, and aimed to bring together academic, technical, and policy expertise to advance critical energy infrastructure protection policy across NATO's maritime theatre moving forward.

These are all important steps to frame Europe's energy security and the protection of energy and critical infrastructure squarely within the military and national security policy planning process within each NATO member state. The urgency of these actions is well-merited, as **sabotage incidents have not only targeted nominally private sector or state-owned-enterprise led energy infrastructure projects across Europe, but, concerningly, dedicated NATO energy infrastructure itself**. On 21 May 2024, reports in Germany's Süddeutsche Zeitung reported that workers near a section of the NATO's Central Europe Pipeline System (CEPS), found a cache of explosives and detonators that had been deliberately buried just meters from the pipeline route.

Often referred to as the "NATO Pipeline Network," CEPS was developed during the Cold War as a dedicated pipeline system to bolster NATO's operational capacity by moving oil and refined products of military utility within its infrastructure extent – which still only includes Belgium, France, Luxembourg, the Netherlands, and the area comprising what was former West Germany. The fact that this **dedicated NATO energy supply system effectively stops at the Fulda Gap remains an impediment to Alliance-wide operational energy security** during a time of conflict or otherwise and has led to calls in recent years for direct expansion for interconnection across nations along NATO's Eastern Flank, including statements by Poland's President Andrzej Duda in July 2023. And in light of the most recent reports from Germany, **NATO must take action to ensure the enhanced physical monitoring and protection of the CEPS network**, both as it stands now, and any future expansion eastward.

Considering these developments, NATO should ensure that the protection of energy and critical infrastructure – including NATO's own network – is a key element of its 75th Anniversary Summit to be held in Washington, D.C. from 9-11 July 2024. NATO leaders should not only announce the rhetorical importance of protection of Europe's energy infrastructure, but should work to **push forward vital investments, such as increasing involvement of the commercial geospatial industry in energy and critical infrastructure** to build out further open-source monitoring data from orbit and a **commitment to expand the CEPS system** for interconnection with NATO's Eastern Flank countries.

NATO leaders should also **increase their support for the protection of Ukraine's energy infrastructure through further investments in both active air defense, counter-drone, and passive defense systems** to support the resilience of Ukraine's remaining operational energy systems. And finally, NATO should acknowledge that it has much to **learn from Ukrainian military tactics** that have been adept at defending its energy infrastructure and make clear that the protection of energy infrastructure across the NATO alliance itself would be a high-priority to help deter any future thought by the Kremlin to expand its military targeting of energy infrastructure beyond Ukraine's borders into NATO territory.

THE CHALLENGES OF PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE

By Dr. Frank Umbach

Dr. phil. Frank Umbach is Head of Research of the European Cluster for Climate, Energy and Resource Security (EUCERS) at the Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn, Germany. He is a Senior Lecturer at the University of Bonn, Adjunct Senior Fellow at the S. Rajaratnam School of International Studies (RSIS) at the Nanyan Technological University (NTU) in Singapore, and an international consultant on international energy and climate security, raw material supply security, geopolitical risks (management), cyber security and critical (energy) infrastructure protection (CEIP), and (maritime) security policies in Europe-Eurasia and Asia-Pacific.

In May 2024, NATO officially expressed concerns about Russia's hybrid warfare and hostile "intensifying campaign of activities" - such as "sabotage, acts of violence, cyber and electronic interference, disinformation campaigns, and other hybrid operations." In the same month, the Alliance held the first meeting of its new "Critical Undersea Infrastructure Network" for enhancing the security of undersea critical infrastructures (CIs) of its member states - including subsea data, telecommunication, internet, and electricity cables as well as oil and gas pipelines. According to unofficial NATO sources, around 25 percent of transatlantic-European data cables have also been put out of service since the beginning of the Ukraine war in February 2022 - and this is by no means exclusively due to technical accidents and fishing nets.

Since the physical sabotage of three of four Nord Stream pipelines in September 2022, the vulnerabilities of European CIs have become an important topic for NATO's and the EU's security agenda. As mentioned earlier in this publication, for the previous 15 years the **security focus had been on the ever-increasing risks and vulnerabilities of CIs to cyberattacks** – particularly of state-backed attacks on Western electricity infrastructure, as all CIs are dependent on a stable supply of electricity and access to the internet. These concerns were confirmed in 2015 and 2016 when Russia targeted Ukraine's electricity sector, leaving almost 300.000 people without electricity supply for more than 6 hours in a large area. These were the first state-supported cyberattacks on another country's electricity system.

With the focus primarily on cybersecurity, the **scale of the threat of physical sabotage was largely overlooked**, particularly for subsea pipelines, internet and electricity cables, whose technical safety and security had never really been addressed by private sector operators and national governments. But since the sabotage of the Nord Stream and the Balticconnector gas pipelines – as well as the two undersea telecommunication cables of the Baltic Sea in October 2023 – the security and protection of those undersea CIs have spurred **greater EU-NATO cooperation** and collaboration. As mentioned in the second article of this publication, NATO also opened a Critical Undersea Infrastructure Coordination Cell at NATO HQ, a new Centre at the Maritime Command in the UK and set up a network to bring these new NATO entities together with Allied governments, industry operators and other experts.

The alliance has also increased its maritime patrols in the North and Baltic Seas. But these missions are time consuming, costly and resource dependent. At the national level, France has taken a pioneering role in the EU and NATO and adopted a "Strategy for Warfare on the Seabed" as early as February 2022.

From Espionage to Open Sabotage of Western Critical Infrastructures

Simultaneously, Russia has upgraded its hybrid warfare and **moved from intensified espionage and information gathering missions** to identify the vulnerabilities of European CIs - including harbors and undersea infrastructure - **to sabotaging them through Europe-based proxies** (Russian diaspora groups, criminal gangs and extremist groups). Such proxies are hired on the internet, darknet, and openly on Telegram channels, and often paid in cryptocurrencies, which makes any direct attribution to the Russian secret services much more difficult for Western security investigations.

The Russian navy operates special submarines for deep sea operations and has been training for sabotage missions, even in the much-deeper Atlantic Ocean, for years to prepare for a larger future conflict with NATO. Such actions also involve Russian research ships and institutions such as the Kremlin's Main Directorate for Deep Sea Research and GRU intelligence units. Russia has also reportedly created "Committees of Special Influence", which coordinate the Kremlin's intelligence operations on a country-by-country basis to overcome traditional rivalries.

A new investigative journalism analysis of Russian commercial fishing activities concluded that almost 1,000 loitering events (referring to vessels deviating from normal routes) by nearly 170 different Russian "ghost ships" occurred within less than a mile from offshore wind turbines, underwater data and electricity cables, or energy pipelines. These are part of intelligence collection activities aimed at covertly mapping maritime CIs across the North Sea and preparing for disruption and sabotage. These ships, despite being officially registered as fishing trawlers and research vessels, often switch off their automatic identification system (AIS) transponders to make them invisible to conventional tracking.

As part of its escalating war on Ukraine, Russia's increasing prowess in "grey zone" activities has made its hybrid warfare much more unpredictable and makes Western deterrence and retaliation more difficult and riskier.

Challenges of Protecting Undersea Infrastructure

Underwater infrastructures such as data and telecommunication cables form the backbone of the global Internet and, increasingly, of European electricity supply. The protection of subsea CIs is therefore of the greatest political, economic and social importance. As mentioned earlier, recent years have seen increasing cybersecurity investment across network operators, but one crucial aspect often took a back seat: physical security.

Internet Submarine Cables

Europe's and the world's dependence on a limited but growing number of fibre-optic cables that make up the global Internet network and connect continents and islands has become a growing security problem in the face of new geopolitical conflicts. Currently, 95 percent of international Internet traffic is ensured via around 200 large submarine cables – each of which can transmit about 200 terabytes per second – and a further 340 main cables. These 1.3 million kilometres of cables guarantee global financial transactions worth an estimated 10 trillion US dollars every day. These are interconnected at 10 vulnerable key locations in different countries worldwide.

Power Cables

In addition to traditional pipelines, critical subsea infrastructures also include an increasing number of subsea power cables, which connect an expanding network of offshore wind and solar farms to the onshore power grid. The future security of electricity supply in Europe and many other regions of the world will increasingly depend on these offshore renewable energy sources and submarine power cables. Thus, the security and resilience of critical maritime and submarine infrastructures is becoming increasingly strategic for the EU and NATO, and Russia's hybrid and conventional warfare against Ukraine's CIs and the lack of resilience of Germany's internet and power cables underline the risks and vulnerabilities.

Protection Requirements

So far, the necessary protection requirements against physical attacks have not been a priority. Cost efficiency, rather than resilience, has been the *Zeitgeist* in politics and business. But in the age of hybrid warfare at all levels, this is no longer sufficient. Within the framework of institutionalized public private partnerships (PPPs) and cooperation and consultations (since 80% of CIs are operated by private companies), **policymakers and industry need a shared and clearly defined understanding of security, to be sustainably implemented** via regulatory requirements to increase resilience, as an integral part of an overall state defense concept.

The **three key concepts of *diversification, redundancy and resilience*** play a decisive strategic role in this. Of course, the possibilities of active defense of CIs will remain limited in the future, especially against state or state-backed sabotage attacks with correspondingly sophisticated military capabilities. Therefore, a certain **prioritization of critical underwater infrastructures** - as with other CIs - is needed. This applies to the most critical and vulnerable landing points and distribution stations.

For critical submarine cables and pipelines, ways to improve resilience include more **active patrols by maritime forces** above and below water, as NATO has been implementing since last year. NATO's capacity to effectively monitor the vast areas of the North and Baltic Seas, the Atlantic and the Mediterranean is ultimately very limited, but the increasing use of autonomous unmanned underwater vehicles (UUVs) offers new, more effective and cost-effective surveillance and defense options that will increasingly replace traditional patrols, and herald a maritime technology revolution. Unmanned Aerial Vehicles (UAVs) are also increasingly used to monitor maritime traffic.

In addition, presence and **real-time monitoring** to provide a 24-hour security-relevant situational picture of the maritime domain can be significantly improved through a combination of satellite, radar, camera, sensor, and sonar data, as well as with new fibre-optic sensor technology. For example, German company AP Sensing uses existing fibrr-optic networks along electricity and internet cables as acoustic sensors (Distributed Acoustic Sensing). Movements and activities near grids generate vibrations that are recorded, localized, and classified in real-time. These can then be made available to the operators and institutions in real time for them to take the right (counter)measures quickly. Ideally, future patrols will also be able to be controlled efficiently and precisely.

This also includes **providing sufficient repair capabilities, spare parts for submarine cables and reserve cables in a strategic reserve**. At present, there are only around 50 laying and repair vessels for Internet cables worldwide. In Europe, there are only 4 stationed cable ships, which are also privately owned. This is insufficient in light of ongoing hybrid warfare and state-backed sabotage campaigns - especially since these privately-owned assets are by no means automatically available immediately after major acts of sabotage.

Strategic Perspectives for NATO, the EU, Governments and Industry

Given the difficulties of attributing multiple small-scale arson and other sabotage attacks to the Russian secret services and responding to them effectively below the level of NATO's Article 5, NATO and the EU have been struggling to form consensus on an appropriate response.

There is no silver bullet to deter, contain and stop Russia's grey-zone strategies and hybrid attacks. To be able to respond, NATO and EU members need new holistic national security concepts, regulations and guidelines, with various strategies and (counter)instruments, as follows:

(1) National resilience must be enhanced by **hardening the physical security of CIs and cyber-proofing computer systems**, but also by providing critical information to the public, and sufficient resources against Russian disinformation campaigns.

(2) The West should also consider proactive **counter-information strategies** inside Russia, as it did during the Cold War.

(3) Holistic national security concepts must include effective **crisis mechanisms, with clearly defined responsibilities** for operators of (maritime) CIs as well as national authorities - in Germany's case, the federal ministries and state authorities. This is essential to overcome the dilution of responsibility and bureaucratic wrangling over competencies.

(4) Those national concepts also need to **create an effective point of contact for NATO and EU institutions.**

(5) They also require the **deployment of new technological capabilities** to improve the resilience of subsea CIs, sufficient stockpiles of maritime Internet, communication and power cables, as well as sufficient ships and capabilities for rapid repairs.

Resilience capabilities must be considered an essential component of both the protection of CIs and of the West's deterrence strategy against large-scale hybrid warfare. In the future, resilience and redundancy capabilities, with state-of-the-art sensor technology, must be made mandatory and installed, integrated and adequately financed "by design" in CIs.

The collective resilience of our CIs is only as strong as the weakest link of the chain, and the EU and NATO should further deepen their security and defense cooperation on this front to enhance the resilience of the infrastructure of their member nations.

In closing: this paper has attempted to cover the immediate threat from Russia. Many of the same vulnerabilities and concerns apply to China which, though lacking Russia's geographic proximity to Europe, deploys extensive cyber and global maritime capabilities, has much greater financial resources than Russia, and even with recent trade restrictions has the opportunity to insert technology into European networks. Thus, Western intelligence services expect to face even more espionage and potential sabotage from China in the near future. In 2022 the head of the German Federal Office for the Protection of the Constitution (BfV), Thomas Haldenweg, warned that China is "the greatest threat in terms of economic and scientific espionage [...] Russia is the storm, China is climate change".