United States Commission on Security and Cooperation in Europe (CSCE)
U.S. Helsinki Commission

Hearing on: "Russia's Shadow War on NATO"

24 September 2024, 14:00-15:30 Hrs.
Cannon House Office Building, Room 210
Washington, D.C.

Written Testimony of:

Dr. Benjamin L. Schmitt

Senior Fellow, Department of Physics and Astronomy and Kleinman Center for Energy Policy, University of Pennsylvania
Associate, Harvard-Ukrainian Research Institute, Harvard University
Senior Fellow, Democratic Resilience Program, Center for European Policy Analysis
Space Diplomacy Lab Co-Founder and Rethinking Diplomacy Fellow, Duke University

"European Energy and Critical Infrastructure Protection: From Russia's Summer of Sabotage to NATO's Autumn of Action"

I. Overview:

Chairman Wilson, Co-Chairman Cardin, Distinguished Senate and House Members of the United States Commission on Security and Cooperation in Europe and honored fellow witnesses. Thank you for the opportunity to testify today to highlight the unprecedented rash of sabotage attacks that have taken place across the European continent against energy and critical infrastructure installations, from the early stages of Russia's large-scale invasion of Ukraine to the present day. Given this growing spate of hybrid attacks, there is an urgent need for the Transatlantic community to take immediate action to blunt this ongoing shadow war that is being waged by Putin's Kremlin against the NATO Alliance to undermine our collective support for Ukrainian victory.

My name is Dr. Benjamin L. Schmitt. I've previously served as European Energy Security Advisor at the U.S. Department of State, under both Democratic and Republican Administrations. I'm now a Senior Fellow at the University of Pennsylvania (Penn), with a joint appointment in both the Department of Physics and Astronomy and the Kleinman Center for Energy Policy. In addition to experimental cosmology work helping to develop telescope instrumentation and renewable energy support infrastructure for the Simons Observatory in Northern Chile, I also conduct research

directly related to European energy security, Russia sanctions regimes, and open-source intelligence (OSINT) methods. I teach a graduate course on these subjects entitled Energy Geopolitics and National Security, and in fact, the students in this semester's class are watching this hearing live from the Penn campus right now.

In addition to my role at Penn, I am also an Associate of the Harvard-Ukrainian Research Institute, a Senior Fellow at the Center for European Policy Analysis (CEPA), a Term Member of the Council on Foreign Relations, and co-founder of the Duke University Space Diplomacy Lab, a part of Duke's "Rethinking Diplomacy" Program.

Since moving to my joint academic position at Penn in January 2023, I have been especially focused in my research on increasing our collective understanding of the way in which the Russian Federation has increasingly utilized clandestine physical sabotage attacks in a steadily expanding and brazen campaign against energy and critical infrastructure across NATO Member States in the past few years. This research, funded internally by Penn's Kleinman Center for Energy Policy, has allowed me to embark on a research expedition that is continental in scope, visiting an array of critical infrastructure facilities across Europe that have either experienced physical sabotage incidents, or those that are operational and whose operators are now working to prevent any such attack in the future.

I have traveled to Longyearbyen on the Norwegian island of Svalbard, just 400 miles from the North Pole to better understand the case of a subsea telecommunications cable that was cut in January 2022, likely by a Russian-flagged fishing trawler – just weeks before Russia's large-scale invasion of Ukraine. I have crisscrossed stretches of the Barents, North, and Baltic Seas to better appreciate the intersection between maritime security and critical infrastructure protection in the region, from Svalbard in the Barents Sea to the Port of Bergen, Norway on the North Sea, to the Danish straits and island of Bornholm in the Western Baltic, to the Gulf of Finland in the East.

I have met with an array of experts, senior officials, law enforcement, military leaders, academics, investigative media, and energy and subsea infrastructure developers to better understand the growing multispectral threats that Putin's Russia is now bringing to bear against infrastructure on NATO soil and in NATO's offshore maritime domain, and how each of these multidisciplinary areas of expertise need to now be urgently synergized to better counter this growing trend of Kremlin-backed irregular warfare. This included a meeting with the leadership of the recently founded Critical Undersea Infrastructure Coordination Cell at NATO Headquarters in Brussels which is working to lead the policy support effort for infrastructure monitoring, data synergy, and response protocols from NATO Member States to recent offshore sabotage incidents.

I have met with experts and officials in both Finland and Estonia, and visited energy infrastructure sites adjacent to both ends of the Balticconnector pipeline in Paldiski, Estonia and Inkoo, Finland, to probe the destruction of the Balticconnector natural gas pipeline in October 2022, in tandem with the use of open-source intelligence tools such as maritime automatic identification system (AIS) tracking and commercial satellite platforms like Planet.

And most recently – just two weeks ago – I chartered a fishing vessel with high-resolution sonar for a research expedition from the port of Nexø on the island of Bornholm in Denmark, to visit and gather seabed sonar data at the Nord Stream 2 blast site, a location which saw perhaps the highest-profile act of sabotage against energy infrastructure on the continent back in September

2022. Attribution of that blast remains a subject of heated debate, and early findings from this study call into question some of the current narratives.

In this testimony, I will highlight how Russia's acts of energy weaponization against Europe have reached their logical apex in Ukraine and should be seen as the ultimate cautionary tale to ensure that the NATO Alliance does more to deter Russian energy infrastructure sabotage, and take sanctions actions to ensure that there can never be a "return to business as usual" with Putin's Kremlin on energy. I will then cover trends observed, preliminary conclusions, and policy recommendations that have come from this Penn research study on the incidents of NATO infrastructure attacks in the past few years. In the coming weeks, I will share with Congress the final version of this published report, which is slated to be released later this year.

Lastly, I am glad to be back speaking before the U.S. Helsinki Commission today. Commissioners, I would be remiss not to note that just two weeks after my previous appearance before this body in June 2022, I received a personal sanctions designation from Putin's Kremlin, apparently for – in the eyes of the Russian Foreign Ministry – the audacity to call for a sharp increase in the scope and enforcement of existing energy sanctions on Russia in response to Moscow's war crimes in Ukraine at the time. Before you all today, I will endeavor to call for redoubled security action, sanctions pressure, and other countermeasures against Putin's war machine in Ukraine and widening sabotage campaign against civilian targets across NATO Member States.

II. Russia's History of Energy Weaponization Reaches Logical Apex in Ukraine:

We meet exactly 943 days since the Putin regime unleashed its expanded onslaught of human misery in Ukraine. That's 943 times – 943 chances – that we have had where we could have done more to stop Russia's overt, kinetic strikes against Ukrainian energy systems.

Russia's campaign against Ukraine's civil energy infrastructure epitomizes the Kremlin's longstanding weaponization of energy, the hallmarks of which have included security of supply threats, monopolistic practices, disinformation, and the corruption and capture of elites. We must urgently do everything possible to support Ukraine's air defense and long-range strike capability before the Winter so that the Kremlin is unable to further expand the humanitarian nightmare it has caused across Ukraine.

After two-and-a-half years of near constant infrastructure bombing, the scale of Russia's energy destruction in Ukraine has become enormous, and its aims no less depraved. The attacks Ukraine has faced against its energy infrastructure will continue to result in a worsening of the already dire Kremlin-fabricated humanitarian nightmare faced by innocent Ukrainian civilians, via widespread energy poverty. The resultant grid intermittency has and will continue to contribute to heating and critical infrastructure limitations across the country, with the onset of a third Winter at war just weeks away.

As of September 2024, Ukrainian President Zelensky's government has revealed via reports that half of Ukrainian electrical capacity has been devastated by Russian strikes, which includes 80% of Ukraine's thermal power generation capacity being shattered by Kremlin-led kinetic assaults aimed at incapacitating Ukraine's existing array of coal- and gas-fired power production facilities.

Beyond humanitarian concerns, Russia's onslaught on Ukraine's energy system continues to throttle expected growth in industrial production according to recent estimates reported by the Wall Street Journal, impacting both Ukrainian economic self-sufficiency, and capacity to ramp up domestic production of military equipment and munitions.

To be clear, the Russian Federation bears all responsibility for its crimes against humanity in Ukraine, including its deliberate actions to target civil energy facilities in its terror bombing campaigns. But it is the responsibility of the United States and all global democracies worldwide to help mitigate the worst of Russian attacks on Ukrainian soil via the rapid delivery of military equipment to Ukraine, and to ensure that Putin pays a price for these crimes via robustly enforced sanctions and technology export controls on the Russian Federation – especially across the energy sector. On both fronts, the Transatlantic alliance still has a considerable amount of work to do.

As a researcher, lecturer, and practitioner of European energy security, I have often been asked what the best energy security strategy for Ukraine might be during wartime. While those asking the question are usually expecting an energy-markets- or economics-analysis-based response, my answer has always been consistent and straightforward: air defense.

Since the outset of Russia's assault against Ukraine, overly incrementalist and always delayed Transatlantic decisions on supporting various weapons systems, defensive strike options, and deliveries of localized air defense systems has left much of Ukraine's sprawling energy landscape vulnerable to Russian strikes. In mathematical terms, the policy equation of some U.S. and European leaders has consistently fit an ***(x - 1)*** equation, where ***'x'*** represents the defense system *du jour* needed to support Ukrainian defense and ultimate victory. In other words, our collective support of Ukraine has been and continues to be consistently one step behind the military reality on the ground.

When it comes to the Western response to support the defense and resilience of Ukraine's civil energy system – just as with the Western response to support broader Ukrainian victory – the cycle of incrementalist measures to support Ukraine needs to be broken, whether it be on the supply of weapons systems and longer-distance strike options urgently needed by Kyiv to defend its population, preserve its civil energy systems, and push Russia from its territory, or on sanctions and technology export controls measures to reduce Putin's ability to wage war against Ukraine in the first place. The time for incrementalism is over.

And to those policymakers that still aren't swayed by arguments to rally to Ukraine's moral cause at the front lines of the global democratic struggle against revanchist authoritarianism, I remind you of some simple economics: rebuilding the majority of the energy infrastructure damaged by the Russian military across a country the scale of Ukraine will ultimately cost far more than surging the needed air defense equipment and allowing Ukrainian long-distance strikes on launch sites around Ukraine's periphery in Russian territory to protect Ukrainian energy systems now.

III. Russia's Actions Across NATO Territory Since 2021 – More Energy Weaponization, More Hybrid Warfare:

In a hearing entitled "Russia's Shadow War on NATO" an opening discussion of the current dynamics of an overt, large-scale, hot war against Ukraine – who is yet not a NATO Member State

– might seem out of place, despite the moral imperative of the United States and its democratic Allies worldwide to support the defense and ultimate restoration of full Ukrainian sovereignty.

However, the current Kremlin strategy of targeting Ukrainian energy and critical infrastructure through traditional military means illustrates what is arguably the logical apex of Russia's longer-term strategy of energy weaponization against the entire European continent. In my previous testimony before the U.S. Helsinki Commission in June 2022, a hearing entitled "European Energy Security Post-Russia," I described how Putin's Kremlin has weaponized energy against both the European Union and Ukraine for much of the past two decades, using multispectral methods.

Among other examples, some of the most notable energy weaponization vectors demonstrated by the Putin regime over the years have included:

(i) the repeated use and threat of politically-motivated Kremlin gas cutoffs of pipeline routes across the continent, including multiple times along the Ukrainian Gas Transmission Route and the Nord Stream 1 and Yamal-Europe pipelines;

(ii) monopolistic practices of Russian state-owned-energy enterprises in Europe, including the use of challenges and lawfare to undermine European energy regulatory development to establish and enforce open market norms, and related corrupt schemes to evade Western sanctions, most notably the funneling of millions of Euros from the Gazprom-backed Nord Stream 2 consortium to establish a so-called "Stiftung Klima- und Umweltschutz M-V" ("Climate and Environmental Protection Foundation M-V") in the German state of Mecklenburg-Vorpommern for the explicit purpose not of urgent climate action, but of enabling the construction of the Kremlin-backed pipeline project;

(iii) weaponizing the information environment pertaining to European energy security policy, Russia energy sanctions, and energy diversification initiatives via the use of bot and troll accounts across social media platforms, as well as so-called "zombie" disinformation websites to spread Kremlin-energy propaganda tropes and narratives;

(iv) the use of strategies of strategic corruption and elite capture, by which Western senior officials have left the public trust following their time in office only to receive plumb positions working for Russian state-owned enterprises, often in the energy sector. These Western officials often appeared to tee-up their post-government employment at Kremlin-backed state-owned entities, having pursued policies that have either benefited the Kremlin or have at least undermined Western initiatives to hold the Putin regime to account for its criminal activities at home and abroad. This practice of former senior officials from global democracies being able to leave the public trust to work for state-owned-enterprises of authoritarian adversaries remains largely legal across Western jurisdictions today, and if not corrected by urgent legislative action, will only further erode public trust and democratic resilience across global democratic states.

These forms of Kremlin energy weaponization – security of supply threats, challenges of EU antimonopoly regulations, disinformation campaigns, and elite capture – had been seen for years in both Ukraine and across the European Union prior to Russia's large-scale invasion of Ukraine in February 2022. Likewise, both Ukraine and the European Union have faced examples of Russia-backed cyber-attack and physical disruption of energy and critical infrastructure from the 2010s

until February 2022, however insufficient Western response to the Kremlin after these incidents over the years have led us to the current crisis.

In Ukraine, Russia has moved from clandestine cyber- and physical-sabotage tactics against Ukraine's energy infrastructure to an all-out war – the *de facto* end state or apex of energy weaponization. And in Europe, a widespread, regularly occurring clandestine campaign against energy and critical infrastructure, both onshore and offshore, across NATO Member States is well underway, some of which already has been attributed to Russian government or Kremlin-backed actors. It can be reasonably argued that if the Transatlantic Alliance does not sufficiently support Ukrainian victory (and therefore, Russian defeat in Ukraine), and does not increase its response to deter Russian sabotage in Europe, that Russia could eventually take steps to move to its apex energy weaponization strategy in Europe like it is demonstrating against Ukraine, should it take military action against at NATO Member State in the future – a grave, but now not unthinkable prospect.

Therefore, it is vital to take a moment to examine several examples of Russia's cyber and physical threats toward energy infrastructure across both Ukraine and NATO Member State land and maritime jurisdictions to both contextualize Russia's current shadow war tactics against Europe, and to see how the warning lights presaging our current crisis were flashing red. After all, although Russia's attributed and potential sabotage actions against energy and critical infrastructure on NATO soil has made increasingly regular headlines this year, the Kremlin had been practicing for the current contingency for years.

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

(i) repeated reports of Russia's development of systems, dual-use vessels, and military platforms that could enhance the Kremlin's ability to conduct subsea and seabed warfare, including reports that Russian submarines and a specially-designed surface vessel – the <YANTAR> – were publicly revealed by U.S. Naval Intelligence in 2015 to have been patrolling off the U.S. East Coast and loitering near vital Transatlantic telecommunications cables. A follow-up report in Naval News by the subsea warfare expert H. I. Sutton in 2021 showed that using OSINT data sources like AIS signals displayed on the commercial maritime-tracking platform MarineTraffic the <YANTAR> was again spotted operating near key transatlantic subsea cable infrastructure off the coast of Ireland, and pointing out the fact that while the <YANTAR> was often referred to by the Russian Federation as an "oceanographic vessel" for research, the vessel is operated by none other than "Russia's secretive Main Directorate of Underwater Research (GUGI) who also operate Russia's 'special mission' (read 'spy') submarines."

(ii) repeated cyber attacks by Russia or Russia-aligned groups in 2015 and 2016 against Ukrainian power grid operators that resulted in widespread power outages for civilians across large areas of Ukraine. The December 2016 attacks specifically targeted Ukraine's capital city, Kyiv, and resulted in an outage of roughly "…200 megawatts of capacity, equivalent to about a fifth of the capital's energy consumption at night." Ultimately, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provided an update on 20 July 2021, stating that "The U.S. Government attributes this

activity to Russian nation-state cyber actors and assess that Russian nation-state cyber actors conducted a cyber campaign against Ukrainian critical infrastructure."

(iii) repeated disruption of the construction of Sweden-to-Lithuania subsea electricity interconnector cable in 2015 within the exclusive economic zone (EEZ) of Lithuania by Russian naval vessels operating in the central Baltic Sea region.

If the actions highlighted here – and many more – that took place against onshore and offshore energy and critical infrastructure by the Russian Federation in Ukraine and in the maritime jurisdiction of NATO Member States over the past decade served as a prelude to the operations that Putin's Kremlin would undertake in the immediate runup to and following its large-scale invasion of Ukraine in February 2022, then I often argue that the turning point in the scale and severity of these Russian operations was most notably highlighted by a dramatic incident that took place not on NATO land or maritime environments, but instead far above the heads of Transatlantic leaders in low-Earth orbit.

On 15 November 2021, the Russian military conducted a destructive "…direct-ascent anti-satellite test [(DA-ASAT)] that blew Kosmos-1408, a derelict Russian spy satellite, into more than 1,500 pieces of space debris." The event, which took place as the Russian military was building up troop and materiel presence along the Ukrainian periphery, was likely aimed at further warning Transatlantic leaders that support for Kyiv against Russia's large-scale invasion of Ukraine would be met with threats to critical infrastructure – even against advanced orbital military and intelligence platforms, as well as potentially against communications and geospatial imagery satellites that have been deployed over the past five years in what is commonly considered our current commercial space renaissance.

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

On 07 January 2022, one of two subsea fiber telecommunications cables connecting the Norwegian archipelago of Svalbard with mainland Norway were cut, reducing the bandwidth for data traffic to and from the island. The damage site, which was located just off of the western coastline of Svalbard, was identified using AIS data analysis by investigative journalists Håvard Gulldahl and Inghild Eriksen from Norwegian public broadcaster NRK as having corresponded to a location that a Russian-flagged fishing trawler, the <MELKART-5> had "crossed the Svalbard cable more than 140 times, and more than a dozen times before the damage occurred in January 2022."

While Gulldahl and Eriksen reported that "the shipowners have denied having anything to do with the damage" the potential that this was in fact Russia-backed sabotage remains non-trivial. First, a pan-Nordic public broadcasting investigation reported in 2023 that the Russian Federation is increasingly using purported "commercial," "fishing," and "research" vessels to conduct espionage around energy and telecommunications installations and infrastructure across Northern Europe – a trend that appears to be a growing central tenet of Russian maritime warfare and intelligence doctrine. For example, in early-October 2022 reports emerged from NRK that a

Russian "research" vessel, the <AKADEMIK B PETROV> had been spotted transiting near strategic Norwegian offshore oil and gas infrastructure, with Norwegian academic researchers commenting that the vessel had "…more antennas than normal ships, it seems to have a large sensor capacity…" and that the ship "…has winches that can put things into the water…therefore [having] equipment that makes it well-suited to carry out missions other than pure research."

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

Russia's attacks against ground and space communications infrastructure with impacts on energy infrastructure continued during the opening hours of its large-scale invasion of Ukraine in late-February 2022. This included an attack reported by MIT Technology Review in which "…just an hour before Russian troops invaded Ukraine, Russian government hackers targeted the American satellite company Viasat." That attack, which was nominally meant to impede Ukraine's communications systems needed for its defense, in turn, according to a June 2024 report from the United Kingdom's Alan Turing Institute "affected space-based assets engaged for command and control of Enercon's wind turbines in Germany, leading to the loss of remote monitoring access to more than 5,800 wind turbines."

With examples of Kremlin energy weaponization via cutoffs and cyber/physical sabotage well-established, the incidents of offshore and onshore energy and critical infrastructure sabotage incidents that either have been attributed to Russia or Russian involvement has at least been suspected, began to skyrocket. This includes attacks against onshore infrastructure like rail lines, logistics hubs, and telecommunications infrastructure, as well as energy installations.

While incidents of likely Russian energy and telecommunication infrastructure sabotage and cyber-attacks began to pick up after its reinvasion of Ukraine, perhaps the highest-profile incident that has not yet reached any on-the-record public attribution against any nation thus far (as of the time of this hearing on 24 September 2024), is of course the sabotage attacks against the Gazprom-backed Nord Stream 1 and Nord Stream 2 trans-Baltic subsea natural gas pipelines in late-September 2022.

In a report section for the European Initiative for Energy Security (EIES) report "Building Energy Resilience from the Seabed Up" that I authored in July 2024 entitled "Responding to Russia's Longstanding Weaponization of Energy" I highlighted the context under which the Nord Stream 1 and Nord Stream 2 attacks took place following Russia's gas cutoffs along the Nord Stream 1 line over the Summer of 2022:

> *"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 02 September 2022.

Throughout Summer 2022, the Kremlin 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 05 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 previous Kremlin claims about the "technical" justification for the cuts on Nord Stream 1 to be nothing but lies when he added, "other reasons that would cause problems with the pumping don't exist.""

This is the context under which the late-September 2022 subsea bombings of the Nord Stream 1 and Nord Stream 2 trunklines took place at sites northeast of the Danish island of Bornholm in the Swedish EEZ (destroying two Nord Stream 1 trunklines at that location), and a site southeast of Bornholm in the Danish EEZ (destroying one of two of the Nord Stream 2 trunklines at that location). Just a year later, in early-October 2023 the Balticconnector natural gas pipeline, as well as several subsea telecommunications cables connecting Sweden and Estonia, and Estonia and Finland, were destroyed amidst the growing count of energy and critical infrastructure sabotage incidents across the European continent. As I pointed out in the report section for EIES in July 2024:

"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 the circumstances surrounding the Russian ownership links of the suspected Chinese-flagged vessel <NEWNEW POLAR BEAR> who's anchor is reported to have inflicted the damage, 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 to 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 seek 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."

In addition to these attacks, the Summer of 2024 has in some way become a Summer of Sabotage when it comes to energy and critical infrastructure attacks across the European continent. Just some of the latest attacks, only some that have been attributed to Russia by authorities thus far, include:

(i) a cache of explosives and detonators was found deliberately buried in May 2024 next to a section of NATO's Central Europe Pipeline System (CEPS), as I wrote about for CEPA this year. CEPS, also referred to as the "NATO Pipeline Network" is a dedicated network of pipelines that was built during the Cold War and is still in use to support NATO operations across its current reach in Western Europe;

(ii) in July 2024, a cell communications tower operated by Finnish telecommunication provider Elisa in Janakkala near Helsinki, Finland was knocked down following what authorities credit as "vandalism" when the tower support guy-wires were found cut;

(iii) in July 2024, an arson attack on a cable shaft supporting DeutscheBahn rail lines near Bremen, Germany was responsible for a train outage in northern Germany;

(iv) in August 2024, reports in Germany emerged that long-range, military-grade surveillance drones had been tracked by German authorities operating over the ChemCoast Park in Brunsbüttel, Germany, adjacent to the Brunsbüttel floating LNG facility – the onshore pipeline for which, as previously mentioned, was itself damaged in a sabotage action in late-2023 near Hetlingen, Germany;

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

IV. Enhancing NATO Deterrence Against Russian Energy and Critical Infrastructure Sabotage – Action and Inaction So Far:

The previous section has provided robust evidence of the Kremlin's long-term strategy of weaponizing energy across the European continent, and the current plague of Kremlin-attributed or Kremlin-suspected sabotage incidents against both onshore and offshore energy and critical infrastructure installations within the jurisdiction of NATO Member States.

There remains much work to do by the Transatlantic alliance to become more adept at monitoring and reaching public attribution for attacks against distributed energy and critical infrastructure in Europe, however some key steps have already been taken by NATO at both a policy and operational level that should be highlighted. As I illustrated in the aforementioned EIES report section that I wrote in July 2024:

> *"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 09 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 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."

Despite these positive, tangible steps taken at the NATO level, Member States still have had difficulty – either for technical reasons, or, potentially, political motivations – to thus far not publicly attribute some of these attacks to Russia. As I wrote for CEPA in June 2024:

"While the infrastructure sectors and methods differ, they are all linked by a continued lack of attribution by European authorities. Investigation can be difficult from a purely technical perspective as there are tens of thousands of miles of rail, pipeline, and cable networks, a fact that makes nabbing would-be-saboteurs in the act a challenging proposition.

But the fact that a great many of these incidents have still not been attributed suggests a possible political calculus. Decisions may have been taken to avoid pointing to Russia even where a reasonable evidentiary threshold may have been met. Some Transatlantic security leaders may be wary of taking any "escalatory" steps in their support of Ukraine — the same leaders who have advanced policies resulting in less-than-comprehensive enforcement of Russian sanctions and a dangerously slow supply of military equipment to Kyiv.

But Moscow's track record should give them pause. Its longstanding focus on projecting hybrid threats against Transatlantic security, with action below the threshold of large-scale war, has for many years posed a risk to energy and critical infrastructure across Europe. This risk skyrocketed after Russia prepared for its full-scale invasion of Ukraine and has increased as the war has ground on.

For years, Putin's Kremlin has emphasized the development of capabilities to sabotage or collect intelligence on European infrastructure, especially in remote maritime environments. This includes Russian government investment in subsea technologies and expertise via such organizations as the Kremlin's Main Directorate for Deep Sea Research (GUGI), the Russian Navy, and GRU military intelligence units. Likewise, the Putin regime has long-conducted so-called grayzone operations, including cyberattacks, energy cuts

and disinformation campaigns against Western democracies, aiming to undermine their democratic resilience. It makes no secret of its intentions. Russia's ambassador to the UK, Andrei Kelin, openly stated in May that the UK's aid to Ukraine made it a "de facto participant" in the war. Kremlin officials have made similar statements about the US.

Given the growing list of offshore attacks on subsea pipelines and telecommunications cables, as well as onshore attacks against energy and transportation infrastructure, it would be reasonable at least to assess the significant likelihood that Russia is to blame. It has both the technical capabilities and the motivation. It could, in the Kremlin's view, be an effective strategy to sow doubt about the ability of European security organizations to protect energy and critical infrastructure, and thereby degrade public support for military aid to Ukraine.

If it was shown that Russia was behind the sabotage attacks, it would necessitate a response from Western capitals, and at least calls for Article 4 consultative mechanisms among NATO member states. It's surprising that Article 4 hasn't yet been invoked — unless, of course, it is part of a misguided "escalation management" strategy.""

V. Countering Russian Energy Weaponization and Sabotage Against European Energy and Critical Infrastructure – From Russia's Summer of Sabotage to NATO's Autumn of Action:

To close this written testimony, I would like to provide U.S. Congress with a selection of policy recommendations that, if enacted, will not only take further steps to ensure that our European partners and Allies are more resilient to Russian energy weaponization in the future, and that Ukraine is supported to protect its energy infrastructure from Russian kinetic strikes and push toward victory now, but also that tangible actions are taken to move from Russia's Summer of Sabotage to NATO's Autumn of Action:

(i) U.S. Congress Should Support the Invocation of NATO Article 4 from Concerned Member States to Respond to Energy and Critical Infrastructure Attacks Officially Attributed to the Kremlin or Kremlin-backed Entities.

NATO Member States who have sustained energy and critical infrastructure sabotage attacks in which an official attribution to Russian government actors or actors recruited and paid by Russia's military intelligence (GRU) should collectively invoke NATO's Article 4 provision. Unlike NATO Article 5, in which direct actions are expected to support a Member State that is victim of a military assault, Article 4 is a consultative mechanism, which states that "the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence, or security of any of the Parties is threatened." Enacting NATO's Article 4 provision would serve as a public reminder to the Kremlin that NATO's political leadership is taking steps to counter and deter further Kremlin-backed actions to undermine Alliance support for Ukrainian victory via sabotage attacks against Member States.

(ii) The United States Should Support the Further Integration of OSINT Data Sets (such as open-source government and commercial, multiwavelength satellite data)

and Solicit the Development of OSINT Analysis Methods from the Academic, Expert, and Commercial Communities to Aid in Energy and Critical Infrastructure Monitoring and Protection Across Europe.

(iii) **U.S. Congress Must Extend Existing Sanctions Packages Targeting the Kremlin-Backed Nord Stream 2 Pipeline that would Otherwise Sunset in Late 2024, and Soon Thereafter Propose and Enact Sanctions Against Other Russian Energy Export Pipelines, such as the Nord Stream 1 and TurkStream Pipeline Systems.**

I have published an analysis coauthored with Ambassador John Herbst in Foreign Policy Magazine in September 2024 that highlights the urgent need to enact these sanctions measures to help ensure that the era of Gazprom weaponizing energy against European democracies is over.

(iv) **U.S. Congress Should Reverse the 2021 Decision of Biden Administration to Avoid Sanctions Designations on the Nord Stream 2 Construction Vessel <BLUE SHIP> and its then Owner the So-Called "Stiftung Klima- und Umweltschutz M-V".**

The Biden Administration's decision to waive bipartisan, Congressionally-mandated Nord Stream 2 sanctions in July 2021 was an avoidable policy error. However, the decision was ultimately reversed and full blocking sanctions were imposed against Nord Stream 2 AG and that company's CEO, reported former Stasi agent and Putin crony Matthias Warnig just hours before Russia's large-scale invasion of Ukraine in February 2022. However, another decision the Biden Administration took later in 2021, to avoid sanctioning a Nord Stream 2 construction vessel – the <BLUE SHIP> – and its owner, the so-called "Stiftung Klima- und Umweltschutz M-V" needs urgent reversal as well. In this case, the the German state of Mecklenburg-Vorpommern used millions of Euros from the Gazprom-backed Nord Stream 2 consortium to create the "Klimastiftung" NGO not for the primary purpose of urgent climate action, but of enabling the construction of the Kremlin-backed Nord Stream 2 pipeline project. The ship and its owner remain unsanctioned to this day. If this decision is not reversed, it will provide a sanctions evasion playbook for authoritarian nations worldwide to set up misleading NGOs inside the jurisdiction of U.S. allied and partner nations to circumvent sanctions, which in turn would weaken broader sanctions and counter-threat financing regimes advanced by global democracies. (NOTE: the <BLUE SHIP> has since 2021 changed its vessel name to <BLUE SKY> and has International Maritime Organization (IMO) number 9381990.)

(v) **U.S. Congress Should Reintroduce and Pass an Updated Version of the Bipartisan Stop Helping Adversaries Manipulate Everything (SHAME) Act Originally Introduced in October 2022 to End the Ability of Former U.S. Officials from Ever Working on Behalf of U.S. Adversaries, their State-Owned-Enterprises, or their Subsidiaries like the Russian Federation Ever Again.**

(vi) **U.S. Congress Should Seek to Significantly Build Capacity within the U.S. Department of the Treasury Office of Foreign Assets Controls (OFAC) to Increase Sanctions Monitoring, Evasion Mitigation, and Enforcement Actions Against the**

Russian Federation – the Largest Sanctions and Technology Export Controls Regime Ever Developed by the United States and its Allies.

(vii) **U.S. Congress Should Pressure the Biden Administration to Allow the Ukrainian Military to Conduct Necessary Longer-Range Strikes Against the Very Launch Facilities on the Territory of the Russian Federation from which the Kremlin's Energy Infrastructure Strikes Against Ukraine are Carried Out.**

Enacting these measures will not only significantly push back on the current scourge of Russian energy and critical infrastructure sabotage across NATO Member States as well as support the future resiliency of a free Ukraine. Such measures will, as I told the Canadian Parliament during testimony last year, make it abundantly clear to the realist, "it's just a commercial deal" bloc across the West, that there can never be a "return to business as usual" with Putin's Kremlin.

Ever.

It's a vital message that authoritarian regimes around the globe need to hear as well.

Thank you for your attention, and I look forward to your questions.

The views expressed by Dr. Benjamin L. Schmitt in this written testimony are his own and do not necessarily represent those of the organizations he is affiliated with, the names of which organizations have been provided for identification purposes only, and which may take no institutional position on the issues conveyed in this testimony.
