United States Senate
Senate Foreign Relations Committee

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

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

Opening Statement of:

Dr. Benjamin L. Schmitt

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

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

The world is at war. We meet 1,525 days since the Putin regime unleashed its full-scale invasion of Ukraine, characterized in part by campaigns of aerial chaos against Ukrainian civilians and civil critical infrastructure. These Kremlin tactics were joined this year by the Iranian Revolutionary Guard, who have launched kinetic drone and missile strikes against civil energy infrastructure across the territories of United States partners and allies in the Middle East.

And for the first time in decades, these ground and air wars have spread into the global maritime domain, with impacts no less dire than the tragic scenes we have witnessed on land. The IRGC has fomented a global energy crisis by continuing to recklessly blockade the Strait of Hormuz, while Iranian proxies in Yemen threaten to multiply the damage by resuming attacks in the Bab al-Mandab Strait.

Meanwhile, the Kremlin continues to work overtime on the high seas to evade Transatlantic sanctions on Russian oil through its array of so-called "Shadow Fleet" oil tankers, some of which have been suspected not only of dodging Western trade restrictions, but of being used as dual-use platforms for espionage and drone launches – including those that have shut down European airports.

But while conflict roils across the ocean surface, another war is being waged globally: a shadow war against the energy and critical infrastructure that has reached from attacks launched on NATO soil, to

a subsea sabotage spree in the depths of the Barents and Baltic Seas. Across Europe, attribution for onshore sabotage attacks on facilities like rail and telecoms lines has pointed to Moscow. The Kremlin's strategy includes recruitment of non-Russian nationals by Russia's military intelligence – the GRU – to do damage to critical infrastructure to sow panic and undermine support for Ukrainian victory across the West. I call this Putin's "Dirty Deeds Done Dirt Cheap" sabotage strategy.

While attribution for onshore attacks has been common, technical and political challenges have remained for attribution – and therefore deterrence – of the many Russia-suspected attacks against seabed gas pipelines, electricity interconnectors, and telecommunications cables across Northern Europe since 2022. And for our partners across the Indo-Pacific region, the challenge has grown as well, including several subsea cable cuts around Taiwan that suggest involvement of the People's Republic of China.

Congress needs to use today's hearing as a starting point to support actions that make it clear to both Moscow and Beijing that its subsea sabotage campaigns to intimidate democracies end here.

And while Congress must lead, I believe academia has a role to play here. For three years, I have led the University of Pennsylvania's UNDERWATER MAYHEM research project, focused on analyzing how both Russia and the PRC now brazenly conduct physical sabotage attacks against seabed energy and critical infrastructure across the NATO Alliance and beyond. This work includes studying policies, technologies, and open-source intelligence methods (including maritime AIS and commercial geospatial imagery) that can be developed and used to counter these active measures.

I have also conducted field research expeditions that are global in scope: meeting with experts and officials and visiting critical offshore infrastructure facilities that have experienced suspected sabotage across the waters of Northern Europe and the Taiwan Strait.

Four such stops have become the central case studies of my research. They provide key examples of the multispectral challenges that exist with infrastructure monitoring, protection, and attribution.

For example:

- I traveled to the Norwegian island of Svalbard – just 400 miles from the North Pole – where we assessed that that it is highly probable that in January 2022, a Russian fishing trawler was responsible for severing a vital subsea fiber optic cable transmitting commercial satellite data from the SvalSAT ground station to the European mainland – commercial data that would prove vital in Ukraine's defense just weeks later. The incident highlights growing Kremlin maritime doctrine to utilize so-called "commercial" or "research" vessels for espionage and sabotage in the European offshore, and that this was likely a "shaping operation" ahead of Russia's full-scale invasion of Ukraine.

- In 2024, I chartered a vessel from Denmark's island of Bornholm, for an expedition to gather seabed sonar data at the site of the September 2022 destruction of Nord Stream 2, perhaps the highest-profile energy sabotage incident to date. Attribution of that blast remains a subject of heated debate, however through a combination of open-source AIS and geospatial satellite data analysis, expert interviews including with Swedish and Danish first responders, and a counter-analysis of competing theories of the case, we assessed as probable that the Russian Federation was involved in the Nord Stream 1 and 2 sabotage.

- I crisscrossed the Gulf of Finland and the Baltic Sea on multiple trips and have visited littoral sites near the site of the October 2023 destruction of the Finland-to-Estonia Balticconnector subsea gas pipeline by a Chinese-flagged container ship with Russian ownership and escorted by a Russian nuclear-powered icebreaker dragging its anchors for hundreds of kilometers. I also visited offshore sites in the Baltic Sea near the site of the November 2024 cutting of the Finland-to-Germany C-Lion 1 and Lithuania-to-Sweden BCS seabed telecoms cables by a Chinese-flagged bulk carrier, as well as near the site of the Christmas Day 2024 cutting of the Finland-to-Estonia seabed electricity interconnector Estlink2 by a Russian shadow fleet vessel.

- And just earlier this month, I traveled to conduct field research in Taiwan, visiting locations close to the sites of the 2025 cut of the Trans-Pacific Express telecoms cable linking Taiwan with the United States and other Indo-Pacific democracies, and the 2023 and 2025 cuts of the telecommunications cables linking Taiwan's Matsu islands and Penghu islands to the main island of Taiwan, respectively. During this visit, I literally conducted research IN the Taiwan Strait itself, donning a wetsuit to see up close what subsea cables look like, visiting cables running through a coral reef in the southern Penghu islands near the center of the Taiwan strait. I also learned about the key legal deterrents that Taiwan is putting in place against further PRC seabed sabotage attempts, including the successful indictment, prosecution, and sentencing of the PRC captain of the Chinese bulk carrier <HONG TAI 58>, who is now serving a three year jail sentence in Tainan, Taiwan for sabotage of the Penghu island subsea telecoms cable. Europe can take away key lessons from Taiwan's proactive legal approach.

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

To this end, I leave you with a few recommendations:

- The Senate should support the invocation of NATO Article 4 consultative mechanisms from concerned Member States to respond to sabotage incidents officially attributed to the Kremlin or Kremlin-backed entities.

- This Committee must reverse the inaction that led to the sunsetting of statutory sanctions in 2024 against Nord Stream 1 and Nord Stream 2 – key steps to ensure that no investor can work to resurrect these crucial tools in Russia's decadeslong strategy of energy weaponization and strategic corruption across Europe.

- Congress should pass S. 3249, the comprehensive "Strategic Subsea Cables Act of 2026" that has been prudently passed by this Committee that would give the White House significant new sanctions authorities to crack down on sabotage-conducting vessels, would give the State Department vital resources to staff up expertise to deter subsea sabotage worldwide, and directs the U.S. Intelligence Community to produce reports to increase understanding of Russian and Chinese tactics in subsea sabotage, including producing a much needed public listing of Russia's GUGI subsea mission directorate fleet that leads the Kremlin's seabed warfare campaign globally while hiding behind the guise of "scientific research."

Through these actions, we can both deter further Kremlin and PRC sabotage, support our partners and allies worldwide, and make it clear to those that would propose otherwise: **there can NEVER again be a return to energy "business as usual" with the Putin regime. Ever.**

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