S. HRG. 119–520

SABOTAGE IN THE BALTIC SEA, IMPLICATIONS FOR EUROPEAN SECURITY, AND LESSONS FOR THE INDO-PACIFIC

HEARING

BEFORE THE

COMMITTEE ON FOREIGN RELATIONS UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

APRIL 30, 2026

Printed for the use of the Committee on Foreign Relations



Available via http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
64–579 PDF WASHINGTON : 2026

COMMITTEE ON FOREIGN RELATIONS

JAMES E. RISCH, Idaho, *Chairman*

PETE RICKETTS, Nebraska
DAVID MCCORMICK, Pennsylvania
STEVE DAINES, Montana
BILL HAGERTY, Tennessee
JOHN BARRASSO, Wyoming
RAND PAUL, Kentucky
TED CRUZ, Texas
MIKE LEE, Utah
RICK SCOTT, Florida
JOHN R. CURTIS, Utah
JOHN CORNYN, Texas

JEANNE SHAHEEN, New Hampshire
CHRISTOPHER A. COONS, Delaware
CHRISTOPHER MURPHY, Connecticut
TIM KAINE, Virginia
JEFF MERKLEY, Oregon
CORY A. BOOKER, New Jersey
BRIAN SCHATZ, Hawaii
CHRIS VAN HOLLEN, Maryland
TAMMY DUCKWORTH, Illinois
JACKY ROSEN, Nevada

SUZANNE WRASSE, *Staff Director*
NAZ DURAKOĞLU, *Democratic Staff Director*
JOHN DUTTON, *Chief Clerk*

C O N T E N T S

Page

STATEMENTS

Risch, Hon. James E., U.S. Senator from Idaho, Chairman 1

Shaheen, Hon. Jeanne, U.S. Senator from New Hampshire, Ranking Member 2

WITNESSES

Schmitt, Benjamin, Ph.D., Senior Fellow, Department of Physics and Astronomy, Kleinman Center for Energy Policy, and Perry World House, University of Pennsylvania, Philadelphia, PA 6

Prepared statement 9

O'Brien, Hon. James C., Distinguished Visiting Fellow, European Council on Foreign Relations, Washington, DC 17

Prepared statement 19

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Statement Submitted by David Coughlan, Chief Executive Officer, *SubCom* ... 3

SABOTAGE IN THE BALTIC SEA, IMPLICATIONS FOR EUROPEAN SECURITY, AND LESSONS FOR THE INDO-PACIFIC

THURSDAY, APRIL 30, 2026

U.S. SENATE,
COMMITTEE ON FOREIGN RELATIONS,
Washington, DC.

The committee met, pursuant to notice, at 10:20 a.m., in room SD–419, Dirksen Senate Office Building, Hon. James E. Risch, chairman of the committee, presiding.

Present: Senators Risch [presiding], Ricketts, McCormick, Daines, Hagerty, Barrasso, Lee, Paul, Cruz, Scott of Florida, Curtis, Cornyn, Shaheen, and Murphy.

OPENING STATEMENT OF HON. JAMES E. RISCH, U.S. SENATOR FROM IDAHO

The CHAIRMAN. With that we will close that part of this meeting and proceed to a hearing that we have set today regarding sabotage in the Baltic Sea and the implications for European security and lessons for the Indo-Pacific. So I am going to make a few opening remarks. I am going to give it to Senator Shaheen to do likewise. We will hear from our witnesses, and we will then open it to a round of questioning for members of the committee.

As we sit here today, thousands of miles of cables and pipelines running under the sea power the global economy. Subsea cables carry more than 95 percent of the world's telecommunications traffic and transmit more than $10 trillion in financial transactions every day. Let me say that again, $10 trillion in financial transactions. These more than 20,000 miles of underwater oil and gas pipelines and electrical transmission cables are vulnerable to attack by our adversaries, and that has become obvious in recent years.

Since 2022, there have been at least eight undersea sabotage incidents in the Baltic Sea, and likely they are the responsibility of Russia. Russia has developed high-end undersea warfare capabilities, as well as low-tech options that mimic the effects of an anchor dragging on the sea floor to hide its behavior. It maintains a specialized fleet of so-called "research vessels" run by a Russian military unit masquerading as a research agency known by its Russian acronym, GUGI.

Just 2 weeks ago, the U.K. revealed it found Russian military submarines working together to map out subsea infrastructure in the North Atlantic, likely to prepare for future sabotage operations. And in 2024, a Russian shadow-fleet tanker attempting to evade oil

sanctions was seized by the Finnish Coast Guard after it cut four subsea internet cables and a power cable.

In response to these incidents, NATO and the EU have stepped up their efforts, particularly through the NATO Shipping Center, the Maritime Center for Critical Undersea Infrastructure, and military patrols in the Baltic. But as always, more needs to be done.

Russia is not the only bad actor. China's military has conducted research into cable cutting technologies, and Taiwan has reported five incidents of likely sabotage in only the last 2 years—that is not just bad luck. Like Russia, China also uses commercial vessels to hide its sabotage. Additionally, Chinese companies like HMN Technologies leverage State subsidies to dominate the subsea cable market.

Allowing one of our foremost adversaries to operate in such a matter creates significant risk. We cannot allow this.

To end undersea sabotage we need to call it out when it happens and say publicly who did it, if possible. We also need a concerted international effort to improve the resiliency of undersea infrastructure and prevent or mitigate the impact of these attacks when they happen.

I look forward to hearing more from our witnesses about how we can address the growing threat of undersea sabotage.

Senator SHAHEEN.

STATEMENT OF HON. JEANNE SHAHEEN,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator SHAHEEN. Thank you, Mr. Chairman, and welcome to our witnesses. Thank you both for being here today.

Last winter, damage to a telecommunications cable between Finland and Estonia was detected. Finnish authorities looked at maritime traffic in the area and found one ship stood out. It was a cargo ship dragging its anchor, and it was from St. Petersburg, Russia. I am sure that comes as no surprise to either of you. They seized the boat, they gathered evidence, and they opened a criminal investigation, but as we know, it was not an isolated incident.

As the Chairman has said, multiple undersea cables in the Baltic were cut this year, each time involving civilian vessels. This is a strategy that I fear is being carried out by Russia's shadow fleet and by other adversaries of the United States. And it extends beyond the Baltic, to undersea cables near the United Kingdom and oil and gas installations in the North Sea.

Putin is testing a model of conflict, and the question is, are U.S. sanctions keeping pace with how Russia is operating? In my view, they are not keeping pace, and Russia is exploiting the gap. Russia continues to generate billions through its shadow fleet, exploiting gaps between U.S., European, and U.K. enforcement. And at a moment when pressure should be increasing, the signal from the U.S. has been mixed. Ships keep moving, revenue keeps flowing, and Russia keeps pushing the boundaries. This allows Russia to sustain its war in Ukraine and these kinds of activities in the Baltic.

The infrastructure targeted in the Baltic is not unique to Europe. Similar vulnerabilities exist in the Indo-Pacific, including around Taiwan, as we saw from our visit there. A bipartisan delegation including three members of this committee visited there in April.

Mr. Chairman, I would like to enter a statement into the record from SubCom, which is a U.S. company that is based in New Hampshire that builds and maintains undersea cables, as well as a report from the International Connectivity Coalition,[1] for the record. If that is OK.

The CHAIRMAN. It will be admitted into the record. Thank you.

[The information referred to follows:]

STATEMENT SUBMITTED BY DAVID COUGHLAN, CHIEF EXECUTIVE OFFICER, SUBCOM

Chairman Risch, Ranking Member Shaheen, and distinguished members of the committee, thank you for the opportunity to convey to the Senate Foreign Relations Committee some of the important issues to consider regarding undersea communications cables and the importance of maintaining the security of this form of strategic infrastructure. These networks are at the heart of global connectivity and economic stability, serving as the backbone for countless critical operations. It is essential that we address both the challenges and opportunities in safeguarding these cables, ensuring their reliability for generations to come.

As you may know, subsea data cables carry 95 percent of the world's internet traffic. There are over 600 cables active worldwide, with a combined distance of some 1.5 million km that connect the continents. These cables carry everything from everyday materials like emails and social media feeds, but more importantly, they carry bank transactions, engineering documents, financial information, and the information that makes the global economy work. The Federal Reserve has estimated that $10 trillion of transactions are carried across undersea networks every day including 15 million SWIFT transactions across 195 countries.

Upwards of 100 of these major subsea data cables land in the United States from overseas, connecting with our domestic telecommunications networks via dozens of landing stations. These cables connect our country with the major hubs of Europe, South America, East Asia and Australia—with many networks extending further into Africa, the Middle East and every corner of the globe. Beyond the major networks, there are numerous smaller cable systems that provide connectivity to more remote or specialized areas, including along the Alaskan coast, the island networks of the Pacific and Indian Oceans, and to Greenland and the Arctic.

With perhaps the exception of our national electrical grid, the subsea fiber optic networks are our country's most important commercial infrastructure allowing our modern economic system to work in an efficient and effective manner.

Despite the vast expanse and incredible importance of these systems, there are actually very few companies in the entire world that design, manufacture, install and maintain these networks. SubCom is the only domestic company that provides this high level of capability. Located in New Hampshire, Maryland and New Jersey, SubCom designs, engineers, manufactures the electronic systems, builds the cables, integrates the systems, lays the networks across the seven oceans, and has the capability to maintain and repair these networks on behalf of our customers. It has installed over 1 million km of fiber optic undersea cables and remains the global leader in this industry.

SubCom is unique in that we have the capabilities and experience to install end-to-end solutions—from landing stations into near shore water, across continental shelfs, through entire oceans, and back to landing stations located thousands of miles from the initial connections. We operate nine ships throughout the globe, laying new systems and maintaining existing ones. Our ships are specially designed for fiber optic cable installation and maintenance and utilize advanced plows and remote operating vehicles (ROVs) to service the cables. SubCom's investment in these industry-leading ships and tools is testament to its commitment to serving its customers and our nation in building and maintaining this vital infrastructure.

With the increasing importance of these networks to global commerce and government activity, there is also a growing need to ensure cables are secured and properly maintained. This has become more of a priority as we have seen cable disruptions—accidental, natural, and malicious—become more prevalent over the past 10-20 years. Additionally, the rise in digital dependency has amplified the consequences of cable failures, affecting everything from internet connectivity to financial transactions.

[1] https://www.internationalconnectivitycoalition.com/

In order to address the needs for securing and repairing these systems it is important to understand the extent and scope of the problems. Cable faults happen, but 70 percent of most faults are due to fishing vessels and ships dragging anchors. Environmental factors like earthquakes also contribute to damage. Less common are subsea component failures such as repeaters, or cable integrity issues. Deliberate sabotage, while a real threat, is still exceedingly rare, but when it does happen it can generate significant headlines. Regardless of the reason for a cable fault, depending on the location and the options to reroute the cable traffic, the impacts can range from inconvenient to debilitating.

Despite most faults not being caused by malicious intent, it does not mean SubCom feels that these issues are not relevant to this committee or important to address. On the contrary, these issues are critical to consider in terms of protecting this type of strategic infrastructure and maintaining our country's connectivity with the rest of the globe. SubCom wants to ensure the members understand the extent of the problem in order to develop good policies that improve on the security and sustainability of these subsea networks.

The reason the majority of cable problems occur due to fishing/anchor drags is that the cables nearshore are in shallower waters. These are where the cables are most vulnerable, especially cables which are in areas that do not allow burial. It should also be noted that the landing points for these cables are typically chosen in more densely populated areas which have extensive telecommunications infrastructure—providing the vital interconnectivity for the systems. But more dense urban areas are also where you have more boat traffic—shipping, pleasure craft, commercial fishing, etc.

The general location of subsea data cables, especially near-shore, are well known, and choke points around important landing stations could allow for rapid and near simultaneous attacks using minimal resources that may be difficult to identify in areas that naturally have high maritime traffic. This is where the threat exists from a national security standpoint. Asymmetric actions from hostile state and non-state actors can be coordinated to cause substantial damage to our subsea data networks. The world-wide cable repair capacity (and to some extent the domestic capacity) is not equipped to rapidly repair multiple, simultaneous breaks along major cable routes. These repairs typically take 1-2 weeks or more, depending on the location, depth and type of repair.

Over the years there has been severe competitive pressures to reduce O&M costs which has led to the reduction of the number of cable maintenance ships. The majority of repair ships are owned and operated by foreign entities and crewed by foreign mariners, which effectively increases response time and increases the foreign influence over these issues. The number of ships that can handle mid-ocean deepwater repairs is also a much smaller subset of the global cable ship fleet. As you consider how to optimize our nation's ability to respond to cable breaks—especially those from bad actors—the makeup and sophistication of the cable fleets need to be weighed as you make policy.

Recent cable disruptions in the South China Sea and the Baltic have brought cable security issues to the forefront. We commend the Senate and Congress as a whole for wanting to better understand the importance of these networks and possibly develop better policies and programs to improve security and repair response. We also want to work with you and the administration on making sure that any legislation or administrative changes are effective, efficient, do not overburden the industry, and do not impair the country's domestic capabilities which we all rely on to install, maintain and repair these networks.

For example, policies that can address the accidental cable faults which typically occur near shore may not be ideal for other failures. When midocean problems occur—whether from environmental factors or component failures—they require specific platforms and skillsets which few companies have, and SubCom is the only domestic company that can provide this type of service. In order to repair deep ocean systems you have to actually identify the cable located several miles below the surface in pitch black depths, raise the cable to the surface, splice and/or repair the cable and components and return the cable safely to the ocean floor. Our marine capabilities enable us to mitigate risks, effectively and efficiently make repairs, and quickly restore operations.

While we are all learning firsthand about critical chokepoints with respect to global energy resources, we have to consider that there are several key telecommunications chokepoints related to undersea cables. The Red Sea, the Straits of Malacca, and the Persian Gulf are all bottlenecks for numerous cable systems. When faults occur in these areas—possibly multiple cables being attacked by bad actors—there are global communications issues that affect all the other networks. These are areas where rerouting traffic is more difficult and often repairs could take much longer if hostilities are ongoing. These are located far from United States territorial waters, but the implications of cable failures in these regions impact US systems, US companies and the US economy.

So, what can be done to improve upon how SubCom and the United States as a whole protects and maintains these subsea data systems?

One aspect to consider is what other nations do—including France, Japan and China—to support and enhance their undersea cable industry which protects their undersea networks. In many cases those countries heavily subsidize their national "champions" in the industry though direct support, tax advantages, and other mechanisms.

The United States Cable Security Fleet was established with a fleet of two active, purpose-built commercially viable cable vessels which meet national security requirements. Two of SubCom's vessels were reflagged to the US and crewed with US maritime personnel to fulfill the CSF requirements. This helps ensure a US presence in the international submarine cable market and keep a broad US deep-water maritime labor base. Most importantly, the CSF allows the United States to quickly re-establish critical undersea networks the keep our country connected to the global economy in times of crisis.

While SubCom does contract with MARAD to supply ships under the Cable Security Fleet, the company does so at a disadvantage. The structure of the CSF contracts doesn't account for the specialized nature of the ships which are used to repair and maintain cables under the program, nor does it account for the large and specialized crew required to operate these ships. It also neglects the shore-based expertise often required to reconstitute these complex networks and restore them to their maximum capacity. The CSF was structured in a way that mirrored the Maritime Security Program (MSP) which provides for transport services during times of war or other national emergencies. Unfortunately, the funding structure does not account for the real world cost structure of operating a cable repair ship vs a transport ship, nor the expertise necessary to complete the repair. One area for Congress to consider with respect to undersea cable security would be ensuring adequate funding for the CSF that reflects the specific requirements of the program, and provide that funding on a long-term basis so that we can make sure these ships and expertise can be available when needed.

Along with the support of our domestic cable ship capabilities, there is growing pressure to have the federal government subsidize additional cable ship construction—both here and overseas. While there may be short-term advantages to do so, the longer-term implications should be considered. As mentioned earlier, SubCom is the only vertically integrated supplier of these systems in the United States. Undercutting our ability to compete with foreign service providers by subsidizing the construction of additional cable ships that will compete against our commercial services will have a detrimental impact on the company. For over 100 years, SubCom and its predecessor companies have pioneered undersea cable manufacturing and technologies while competing against the likes of Alcatel, NEC, and Huawei. SubCom wants to continue in its role to help maintain our domestic telecommunications industrial base, as well as our maritime base. We hope that the Congress and administration would work with us before considering any programs that would alter the competitive dynamics of the industry.

Finally, one area to consider is important cable systems for national defense and security locations around the world. Many of these places are remote, are served by a single cable, have limited alternative communications options, and are serviced by outdated systems. Some of these networks need to be upgraded and some of the networks likely need redundancy to maintain uptime if there is a cable fault. Continued diligence is necessary to ensure reliable connectivity for these important locations.

SubCom has worked for 100 years designing, building and maintaining our undersea communications networks. It has worked with the US Government to provide important services and connect remote regions. We look forward to continuing to provide guidance and support to you and the administration to ensure the security and reliability of these subsea data networks on a national and global level.

Senator SHAHEEN. Thank you. As we know, much of this infrastructure for undersea cables is privately owned and is unevenly protected. Repair capacity is limited, and it takes time to fix breaks. So attribution for attacks still takes weeks, and even then, intent is hard to prove. So, we need to recognize that that infrastructure is national security.

I am sure we are going to hear lots of good recommendations from our witnesses this morning about how we can impose costs when attribution is slow and intent is hard to prove, and what we should be doing in terms of ensuring the security of these undersea cables.

Again, thank you both for being here and I look forward to your testimony.

The CHAIRMAN. Thank you so much, Senator Shaheen. We now are going to hear from our witnesses. First we have Dr. Benjamin Schmitt, who is a Senior Fellow at the University of Pennsylvania, where he holds a joint academic appointment with the Department of Physics and Astronomy and the Kleinman Center for Energy Policy. He also serves as the Director of the Perry World House Graduate Program at Penn.

Mr. Schmitt recently completed a 2-year investigation into suspected sabotage incidents in the Baltic Sea, and is currently researching sabotage activity near Taiwan.

Dr. Schmitt, the floor is yours.

STATEMENT OF BENJAMIN SCHMITT, PH.D., SENIOR FELLOW, DEPARTMENT OF PHYSICS AND ASTRONOMY, KLEINMAN CENTER FOR ENERGY POLICY, AND PERRY WORLD HOUSE, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA

Mr. SCHMITT. 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 previously served as European Energy Security Advisor at the U.S. Department of State, and I am currently a Senior Fellow at both the University of Pennsylvania and the Center for European Policy Analysis, and I am honored to speak with you all today.

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

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

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

Meanwhile, there is another war being waged, a shadow war in Europe against energy and critical infrastructure undermining the security of NATO member states not only on land, but offshore, roiling the depths of the Barents and Baltic Seas. European partners have confidently attributed to Russia attacks on such onshore facilities as rail and telecoms installations. The Kremlin's strategy includes recruitment of non-Russian nationals, including Ukrainians, to damage critical infrastructure to sow panic and undermine support for Ukrainian victory across the West.

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

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

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

And while the Senate must drive the policy conversation, I believe academia has a role to play as well. For 3 years, I have led the University of Pennsylvania's Underwater Mayhem research project, focused on analyzing how Russia and the PRC now brazenly conduct physical sabotage attacks against seabed energy and critical infrastructure across the NATO Alliance and beyond.

Four key case studies from our research include the following:

No. 1, Svalbard. My travel to the Norwegian island of Svalbard, just 400 miles from the North Pole, supported our assessment that it is highly probable that in January 2022, a Russian fishing trawler was responsible for severing a vital subsea fiber optic cable transmitting commercial satellite data from the SvalSAT ground station to the European mainland. Such commercial data would prove vital in Ukraine's defense just weeks later, leading to our conclusion that this was likely a "shaping operation" before the full-scale invasion.

No. 2, Nord Stream. Official attribution of the September 2022 Nord Stream 1 and 2 sabotage remains absent, and despite continued public debate, our research team assesses as probable that the Russian Federation was involved in this high-profile sabotage incident, and assesses as improbable the media narrative that a so-called "pro-Ukraine sailboat" launched from a marina next to a Nord Stream logistics hub was to blame. We arrived at this assessment after exhaustive open-source AIS and satellite data analysis, interviews with first responders and experts across Europe, and a technical counter-analysis of competing theories of the case. I also chartered a vessel from Denmark's island of Bornholm to travel to the blast site itself and gathered seabed sonar data in 2024.

No. 3, the Baltic Sea. We have heard a little bit about this already. I sailed on vessels offshore in the Gulf of Finland and the Central Baltic near the sites of several extended anchor drag incidents by Russia-and China-connected vessels which crippled seabed installations, including the 2023 Balticconnector gas pipeline break, the 2024 C-Lion-l and BCS telecoms cable cuts, and the 2024 Estlink 2 electricity cable cut. The circumstances of these incidents suggest sabotage, not accidents.

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

Senators, it is time to turn the tables on the Putin and Xi regimes and restore deterrence against maritime sabotage. And to this end, I leave you with three very brief recommendations:

No. 1, the Senate should support the invocation of NATO's Article 4 consultative mechanisms by concerned Member States whenever there are sabotage incidents attributed to Russia or its agents, which is essential to solidify political and operational support to counter these threats.

No. 2, this committee should revive the statutory sanctions against Nord Stream 1 and Nord Stream 2 that were allowed to sunset in 2024, key steps to ensure that no investor, American or otherwise, can work to resurrect these symbols of Russia's energy weaponization and strategic corruption.

And finally, Congress should pass S. 3249, the comprehensive Strategic Subsea Cables Act of 2026, and S. 2222, the Critical Undersea Infrastructure Resilience Act, both that have been prudently passed already by this committee. Through these actions, we can deter further Russian and Chinese sabotage, support our partners and allies worldwide, and make it clear to those that would think otherwise, there can never again be a return to so-called "business as usual" with regimes that continue to attack the physical foundations of our economy, prosperity, and freedom.

Thank you so much, and I look forward to your questions.

[The prepared statement of Mr. Schmitt follows:][1]

[1] Dr. Schmitt appended an additional report to his opening statement—*Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond, Volume 01."* That report can be viewed by clicking on the following url:
https://upenn.app.box.com/s/wvrobfk9j1h34agng36chj73ibtkcx0h

Prepared Statement of Dr. Benjamin Schmitt

UNCLASSIFIED (U)

United States Senate
Senate Foreign Relations Committee

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

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

Written Statement Document Package of:

Dr. Benjamin L. Schmitt

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

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

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

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

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

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

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

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

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

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

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

Four key case studies from our research include:

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

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

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

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

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

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

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

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

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

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

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

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

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

Europe's Energy Security Playbook

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

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

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

Outrunning the Weapon

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

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

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

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

The Pivot

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

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

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

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

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

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

Underwater Mayhem

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

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

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

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

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

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

Looking for Legal Remedy

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

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

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

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

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

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

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

Transatlantic Troubles

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

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

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

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

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

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

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

The CHAIRMAN. Great remarks and recommendations. We will now hear from Mr. O'Brien. Mr. O'Brien is the Distinguished Visiting Fellow at the European Council on Foreign Relations, where he focuses on efforts to strengthen the transatlantic relationship. Previously, Mr. O'Brien served as Assistant Secretary of State for European and Eurasian Affairs in the Biden administration and as head of the Office of Sanctions Coordination.

Mr. O'Brien, the floor is yours.

STATEMENT OF HON. JAMES C. O'BRIEN, DISTINGUISHED VISITING FELLOW, EUROPEAN COUNCIL ON FOREIGN RELATIONS, WASHINGTON, DC

Mr. O'BRIEN. Thank you, Mr. Chairman, ranking member, and Senator Ricketts from my home State. Your statements made the case. Undersea infrastructure is critical for America's prosperity and security. Russia and China are attacking it. We at least have to plan as though they will attack it in a time of greater tension.

I can't compete with Dr. Schmitt's field activities, especially the wet suit, so I am going to focus on the policy implications of this.

What is the first?

The first is we can deter now or pay later. It is just a simple, timeless lesson. Russia and China are testing. They are testing where they can. They are doing it undersea. They are doing it on the surface. They are doing it on land in a wider sabotage campaign. And if we do not call them out and respond, we are going to face increased pressure.

And I note how that cuts against basic objectives of this administration. Diplomats are now out trying to get European countries to sign up to long-term American LNG contracts. That has to be delivered through terminals that have large undersea exposure. Why are they going to sign up to that if we are not acting robustly to protect the infrastructure? So that is an important point.

There is a real risk of escalation with our current posture because all the tinder is laid. You have European countries facing pressures at home to answer Russian threats. You have Russia and China seeking if they can push things further. And I think you need to have a strong U.S. hand to demonstrate that there is no escalation edge to Russia and China if they continue down this path.

So this is the way of getting more peace by moving now. And that is especially because the group of countries most affected in the Baltic are the fighting flank of NATO. They are going to be the ones who spend enough, who stand with us, who go with us, who protect the Arctic. If we do not help defend them, Russia and China will believe we will not help defend anyone. It is very simple.

Now, what is it that we should do? One lesson is that solidarity works. Mr. Chairman, you laid out many of the steps that have been taken by NATO and the European Union and others, with really strong bipartisan support from this committee and members of other committees. It has been a great effort. When I speak to colleagues in the Baltic states or across the nine countries that are on those waterways, they say that these NATO missions, air and sea, have made a tremendous difference. The transparency of where the infrastructure is and how to track the ships is very helpful.

And this carries to the Indo-Pacific. We have built very strong, across administrations, very strong ties between European countries and the Asian countries who are most dependent on undersea infrastructure, and that has to continue so that the lessons can be learned.

Second, we need to name and sanction the ships, individuals, and institutions responsible, and I strongly support the two bills this committee is putting forward that include sanctions authority. It helps a great deal to have authority that is tied to disruption of undersea infrastructure.

We could use maybe some of the sanctions authorities pertaining to Russia, but there will be those, particularly in this administration, who say that we do not want to name and shame particular Russians. We can do this with a sanctions authority that is targeted to undersea infrastructure, and I think we can do it in a way that avoids raising gas and oil prices.

The third thing is we have to confront the Russian shadow fleet. This is between 400 and 900 vessels. Two hundred of them were designated by January 2025, none since by the United States. This

is the deniable weapon that Russia and China use to attack undersea infrastructure.

Now, let me talk about a second lesson. We need stability in our partnerships. I believe the future of the United States, our prosperity, depends on innovative sections like life sciences, technology, energy, and defense. Operating in a marketplace of more than 1 billion rich consumers, they will provide us—these are our traditional partners, and they will provide us with the materials, the supply chains, the markets, and yes, the competitors, but ones who operate under rules that we all share. That is the future for us. It will work only if undersea infrastructure is protected.

And the problem we have is that it is like any shopping center. Somebody has to provide basic security, has to make sure it is cleaned up, has to make sure that the place is reasonably attractive. That has always been the United States. Middle powers cannot provide these public goods against predatory superpowers like Russia and China. The U.S. has to organize and sometimes has to be the one to provide them.

And you do not do that on a pay-as-you-go basis, by saying this country uses this waterway more and this country uses that waterway less, so we pay differently. You have to do that with a certain amount of stability and an understanding that America will benefit with the stability of having a relationship that extends from Australia, up across northeast Asia, across North America, into Europe. That set of friends and partners will guarantee us prosperity and security in the future, but only if we commit to providing the public goods that make it possible, and the undersea infrastructure this committee is calling our attention to is the first, along with space, communication, and a few other things.

But this is the place to begin work, so I thank you for your attention to it.

[The prepared statement of Mr. O'Brien follows:]

PREPARED STATEMENT OF JAMES C. O'BRIEN

Mr. Chairman, Ranking Member Shaheen, thank you for inviting me.

I am Jim O'Brien, currently a fellow at the European Council on Foreign Relations and completing a term as a fellow at the Institute for Human Sciences in Vienna, where I worked on several of the themes discussed below. I have served in the U.S. Government at various times since 1989, most recently as Assistant Secretary of State for Europe and Eurasian Affairs and as the Secretary of State's coordinator for sanctions, a post created at the urging of this committee. I have also spent half my career working with private sector and civil society groups. I have no financial interest in the topics raised today, nor do I work for any entity with a commercial or advocacy interest.

Thank you to the committee for highlighting the importance of the Baltic Sea and the infrastructure under its surface. The committee—and my fellow witness, Dr. Schmitt—have laid out the factual context very well. Simply put, the globe's 500 or so cables carry more than 99 percent of the world's digital traffic, and undersea infrastructure will be increasingly important for the transmission of energy and electricity. Over the last decade undersea infrastructure has become a site of considerable investment by America's largest companies, adding another strong U.S. interest in its protection. There are 100–200 outages in a typical a year. Most are accidental, but there is a growing and troubling pattern of disruption by Russian and Chinese ships.I will focus on some policy implications of this last point. The first lesson is timeless: we can deter now or pay later. Russian and Chinese ships have been involved in multiple attacks in the Baltic over the last several years, and those countries are learning how and whether the U.S. will answer. The Allies affected directly by sabotage in the Baltic—Estonia, Latvia, Lithuania, Poland, Finland, Sweden, Denmark, Germany through to Belgium, France, and the UK—are NATO's fighting

flank. They are critical to defending the Arctic as well as Russia's northern sea routes to the globe. If we do not stand with them potential adversaries will believe that we will not stand with anyone.

Also, our current posture poses a risk of escalation. Russia is reported to be placing armed personnel on shadow fleet vessels, raising the cost of stops intended to ensure that the ships do not threaten lives, other ships, and the environment. Ukraine is targeting Russian export infrastructure used in the region, arguably because without further U.S. action in the Baltic it is difficult to stop Russia from earning funds from oil exports. Our NATO Allies may face strong domestic pressure to answer Russian provocations. In short, the conditions are ripe for miscalculation or error to lead to more violence. A stronger U.S. presence can persuade everyone that escalation is in no one's interest.

Finally, the Baltic Sea presents a test case of an issue that will face U.S. administrations for decades: how can the U.S. ensure that the basic conditions of prosperity and security—including undersea cables and pipelines, freedom of navigation, and assets in space—are provided and protected?

These global public goods benefit the U.S. but also many countries, with the exact balance shifting over time and in different places. This leads some to suggest that the U.S. should treat each of these goods as reason to have a separate negotiation. This ignores how intertwined U.S. security and prosperity is with others and how quickly the ratio of benefits can shift. For decades the U.S. and our longtime partners have adjusted our respective roles and responsibilities in providing these goods. In the late 1940s, when the U.S. economy was half of global GDP and more than half of global manufacturing, it may have been fair for the U.S. to organize the provision of these goods and even to provide them by ourselves (although I will let others debate that).

That allocation has changed and will always be under negotiation. As just one example of increased commitment from our partners, in July 2024 NATO approved regional defense plans (including undersea needs) that require members to spend approximately 3–3.5 percent of GDP on defense priorities, along with an additional amount on infrastructure. Under the current administration this commitment has been made both more specific and very public, in the form of a targeted cap of 5 percent of GDP. The publicity is helpful politically, but the priorities are decided by planning. A commitment to continue the planning as situations change lies is essential to success.

In addition, by early 2025 NATO had prepared a center focused on undersea threats in the Baltic, and a mission at sea had been launched. The EU in 2024 approved a program to improve civilian resilience for undersea cables, and civilian consortia such as the International Cable Protection Coalition (ICPC) offer venues for doing more, particularly by addressing normal business of laying, maintaining, and repairing cables (where more capacity is urgently needed).

As we agree with our partners on a new allocation of responsibilities and costs we should not hide from a basic fact: middle powers cannot ensure the conditions of prosperity, especially against predatory superpowers. The U.S. has to be the long pole in the tent, and our partners need to understand that we are in one long struggle to ensure that our societies control the conditions of our own prosperity and security.

Getting this partnership right is fundamental to America's prosperity and security for the next generations. Innovative sectors such as life sciences, artificial intelligence, new defense technologies, and energy developments will grow more quickly and in ways that benefit our people with reliable markets, sources of materials, supply chains, partners, and—yes—competitors who will play by the same rules as our companies. We have spent 80 years building exactly this community with our traditional partners in Europe, North America, Japan, Korea, Australia, New Zealand, and now across the Indo-Pacific.

Now we can choose to hang together, or to hang separately. It is simple arithmetic. Together, the U.S. and our partners offer markets, supply chains, and partners with more than a billion, well-off consumers, more than capable of meeting a challenge from Russia and China. If we go it alone, smaller countries will waver against the superpowers, and America will be 350 million people facing more than a billion. I believe in America's ingenuity and determination but size helps, too.

Undersea infrastructure provides the connective tissue to make this work. With our partners we can find fair allocations of responsibility to protect it. Or we can spend more to do more ourselves and be just a bit poorer as we lose opportunities from partnership.

Policy Recommendations

First, the administration should acknowledge Russia's role explicitly. Clarity and action will set expectations that can make negotiations more successful. Having nice conversations with Russian investment advisers does nothing to change the calculations of the Russian security apparatus, which knows that the country is bound to China for now. Russian activity seems to have stepped up since 2025, and the U.S. response—preferably with our partners— is being watched closely in Moscow and Beijing.

Second, the administration should act against the Russian shadow fleet. As we have seen, these ships are the perfect, deniable assets for Russia to use in threatening the undersea infrastructure of the Baltic Sea. Russian shadow fleet vessels tend to travel through the Baltic Sea, carrying as much as 2/3 of the Russian oil exports that finance the invasion of Ukraine. The administration's use of sanctions and seizures against shadow fleet vessels elsewhere show that it still has the toolbox open. It just needs to use the tool.

By January 2025 the U.S. had designated nearly 200 vessels in the Russian shadow fleet (around half of the Russia-only shadow fleet known at the time), and our partners in the U.S. and EU have since designated more. States bordering the Baltic Sea and other waterways have taken strong measures to ensure that these ships comply with regulatory requirements. As a result, and due to lower oil prices starting in 2024, by the spring of 2025 many of these ships were no longer operating regularly. Sadly, U.S. efforts against the shadow fleet serving Russian exports seem to have declined over the 15 months. With the increase in global oil prices, those ships are again active.

Third, the bill proposed by Ranking Member Shaheen and Senator Barrasso is a good step toward ensuring that the U.S. Government has the knowledge it needs, venues to coordinate with others, and tools to respond when the infrastructure is threatened.

The bill's sanctions authority is also welcome. Existing sanctions authorities would allow action due to the benefit that Russia receives from these disruptions, but the current administration seems to find it difficult to target Russian entities. This sanctions authority would offer an alternative approach that might be more palatable to people concerned about linking U.S. action to Russia's ongoing invasion of Ukraine, and its global reach would be useful.

If the opportunity arises, the bill's sanctions authority should be extended to allow designations for foreign persons who participate in commercial activity in undersea infrastructure projects linked to Russian energy exports. There has been much speculation about a possible reopening of the NordStream 2 pipeline, for instance. The prospect of U.S. sanctions, now or under a future administration, could depress interest in this and other projects. I am not implying a link between current disruptions and any commercial plans. Still, without this authority it might be tempting for someone to pick up infrastructure at prices lowered by the prospect of violence against others in the neighborhood.

I look forward to your questions.

The CHAIRMAN. Well, thanks to both of you. One of the most important things you said is this is bipartisan. We do not hold a lot of hearings that are absolutely, totally, 100 percent bipartisan, but this is certainly one of them.

One of the questions I have is I think both of you made reference to the fact that countries—well, the two obvious violators are Russia and China—that they are still testing. Why would they be testing? Maybe they are testing us. But, I mean, this is not rocket science. You do not need engineers. You need a salty, old captain who is a lousy boat driver, it seems to me, and you can disrupt these cables and find where they are in relatively shallow water.

Why do these continue to happen? Is it a test of our response? Is that what they are looking for? Why are they continuing to test? Because this really riles people up. I mean, it gets people fired up. There is no question about it. Why don't you start, Dr. Schmitt.

Mr. SCHMITT. So I would say you have referenced and we have heard already the incidents that have taken place in the Gulf of Finland.

First I want to make it clear. The Baltic Sea is center of these sort of incidents, in part because it is strategic for the Russian Federation and for NATO, but also because it is a relatively shallow body of water that has a high density of subsea infrastructure to begin with. So that is why I think statistically we are seeing more in the Baltic Sea than in other locations.

But one of the things I want to say is that in 2024, on Christmas Day, the "EAGLE S", a Russian shadow fleet vessel, dragged its anchor through both telecoms cables and the Estlink 2 electricity interconnector, connecting Finland and Estonia. And when it broke those, the Finnish authorities came out in helicopters and their special police forces descended dramatically on the deck, and seized the vessel and brought it into port.

Part of the reason, I believe, that this specific infrastructure was targeted was because the Baltic states were trying to synchronize with the EU grid, their electricity infrastructure and finally throw off the yoke of the Russian and Belarussian electricity grid. So by severing that electricity in their connector it increased the risk of that operation just planned for about 4 or 5 weeks later.

But the other thing is the response, and that is, to your point, Senator Risch, I think the biggest thing here. The Finns put the captain on trial, put part of the crew on trial, and at the end of the day they let them go because they said they did not have the jurisdiction because they were in the Exclusive Economic Zone and not the territorial waters of Finland. So that is a problem, but we saw a solution in Taiwan. I visited the prosecutor in Tainan City, Taiwan, just 2 weeks ago, and had a long interview with him, who put this PRC captain of the "HONG TAI 58" in jail after sabotaging the Penghu island cable. And the reason for that was something called the "Results Principle," basically saying that no matter where these cables go, outside of the territorial waters, Exclusive Economic Zone or beyond, that the Taiwanese Government can prosecute and put away these folks for doing this because it has impact on their society. And that is a lesson I think Finland can take from here, and the EU can.

The CHAIRMAN. You brought up something that has been really important to me, and that is I was really disappointed when I heard what happened in Finland. You know, this jurisdictional question is just nonsense. I mean, we prosecute people all the time who send drugs into the United States but have never set foot in the United States. A good example of that is a guy sitting in jail right now in New York.

So I do not know what Finland has to do to change its laws to grab jurisdiction, but like you say, the causation factor seems to me to be very easy. I hope they will do it. I hope everybody will do it. So I appreciate you underscoring that; and like I said, it was incredibly disappointing.

How many other countries do you think are in that same boat? I cannot imagine we would have that problem. If somebody did that to us, we would [unclear] easily under the causation doctrine.

Mr. SCHMITT. Yes. I mean, I think this is a great point. You mentioned Maduro being in jail in New York. Obviously that is a precedent that the Taiwanese pointed out to me, like if there was a scam artist in Cambodia that was preying on citizens in Taiwan, they

would indict that person. They might not be able to extradite him, but they could at least indict him. And we certainly do the same thing against corrupt actors around the world and sanctions on Russian oligarchs and all these sort of thing.

The CHAIRMAN. Let me interrupt you for a second. Extradition is an entirely different issue than jurisdiction. I mean, extradition is simply putting the "habeas grabus" on the guy and getting hold of him. The jurisdiction is a legal principle that is entirely different than that. And again, I think the causation issue was resolved decades ago, if not centuries ago.

Go ahead and finish up.

Mr. SCHMITT. I want to say the problem that you mention for Finland, so the first thing I had, my reaction in November of last year when that was dismissed because of jurisdiction, I said this is going to happen again. And sure enough, on New Years Eve, just 6 weeks later, last year, the "FITBURG", another Russia-connected vessel, did another sabotage run through that same water. So we are going to have to find out what the Finns do this time to get that right.

Mr. O'BRIEN. Mr. Chairman?

The CHAIRMAN. Do you want to comment on that?

Mr. O'BRIEN. If I may. It would help to have some U.S. assertion of jurisdiction. If we were using our sanctions authority then you would be able to maybe apply some material support, criminal investigative capacity to this, and not get into arguments with—I used to be a Law of the Sea lawyer, briefly, at the State Department, and it gave me a headache. But I think you could avoid this not by just calling out others but by asserting U.S. jurisdiction.

We have something in common. The Law of the Sea treaty has given me many, many, many headaches.

[Laughter.]

The CHAIRMAN. Senator Shaheen.

Senator SHAHEEN. Well, yes, I was just going to try and followup on that a little bit, because if Taiwan was able to do that, was it under existing law that Taiwan has, and why do we think—I guess this is for both of you—why do we think that that would be an issue in Europe?

Mr. SCHMITT. So yes, Senator Shaheen, it was Article 4 of the Taiwanese Criminal Code that says that basically wherever these crimes happen, if they impact Taiwanese citizens or the government they have jurisdiction.

Senator SHAHEEN. And do either of you have any insights into why this would not apply to Finland or to other European countries?

Mr. O'BRIEN. I think I would be happy to do a little research and find it. The key is we are seeing this now in the Straits of Hormuz. There are a lot of these waterways that were sources of warfare for a long time, so the European states reached agreement to say the Straits off Copenhagen, the international waterways through these narrow areas, like the Baltic Sea, nobody is going to put their hands on them. And that sort of hands-off thing has been a basis of peace in the region. But it is fraying, and they need to take a look at it, but the exact sort of rule that they should adopt, I don't have a quick recommendation.

Senator SHAHEEN. So you were talking about sanctions and the idea that we should be thinking about sanctioning more vessels, which I totally agree with. Senator Risch and I have a shadow fleet bill that would virtually sanction the shadow fleet, wherever it exists.

But one of the things that I am concerned about right now is the decision by this administration to lift the sanctions on Russia's shadow fleet, basically, so that they can continue to gain revenue from oil in the war in Iran. So can you talk about what that may mean for Russia and their ability to continue to operate, both in Ukraine and with respect to other nefarious activities that they are engaged in?

Mr. O'BRIEN. Yes, it is a windfall for Russia in a couple of ways, and then I will talk about the rationale for what the administration did. It is a windfall, just factually. Russia, in the first few weeks it was making $150 million a day in tax revenue off the extra sales, off the general license. Oil prices have gone up since then. We have extended the general license so more ships have loaded and are heading to sea, so they will be selling at whatever the price is when they land.

So it is going to produce, I don't know, multiple billions of dollars by the time we work our way through this, assuming that the Iran conflict ends soon.

Russia spends between $150 and $200 billion a year on the war in Ukraine, and if they make, say, $40 billion, $50 billion as a result of this, that goes right to the bottom line. That is not a good thing.

There is a long-term benefit to Russia. They have had some difficulty locking in long-term supply arrangements with China because the Chinese do not really want to be tied down. But now with difficulties in the Straits of Hormuz and the difficulties elsewhere, there is a possibility that Russia and China will tie up with a great infrastructure, including a gas pipeline and an oil pipeline. That will mean U.S. sanctions will be even less effective next time we want to use them. So both of those things are a real cost.

Now, the administration was doing it to alleviate the concerns of specific partners about a rapid increase in oil prices. I think the cost-benefit analysis is difficult to make. For the oil that was already at sea at the time the Straits were closed, I think you could see something. But then allowing the ships to reload and emerge again is a real problem.

And this gets to the nature of the shadow fleet. It is outside our normal tools for stopping shipping. Because of the initial sanctions, and the 600 ships that the EU and U.K. have designated, more than half of the Russian shadow fleet really was not operating. But now with a general license from the United States, more of those ships can set, so the numbers I gave earlier are going to underestimate the benefit that they are going to get.

There were ways to provide relief to the global oil market that would have involved just allowing Russia to load up and sell, and I think there is a real cost that ought to be examined.

Senator SHAHEEN. Well, I could not agree more, and I think that cost also goes to benefit Iran. Because if we look at the drones that Iran is using in this war and the number of those drones that they

are still getting from Russia, and Russia's ability to produce those drones, they are getting a huge benefit that we are basically providing to a country that is targeting not just our servicemembers in the Middle East, with intelligence information, but our allies in the Middle East. I mean, it makes absolutely no sense. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Shaheen. Senator Ricketts.

Senator RICKETTS. Thank you, Mr. Chairman. Dr. Schmitt, you have been tracking the disturbing pattern in the Baltic. Russian research vessels and tankers coincidentally stop over critical infrastructure right as it fails. The Indo-Pacific has this problem, only it is magnified. You are not just seeing the actions of a few rogue ships, but you have got the Chinese Maritime Militia, which as a fleet of thousands of civilian fishing vessels, which are just CCP proxies. These dual-use vessels provide Beijing with a perfect screen for their ICAD activities—illegal, coercive, aggressive, and deceptive operations that target these subsea cables and threaten the digital life blood of the regional countries like Taiwan, which we have already talked about, but also Vietnam, the Philippines, and Singapore.

And you also talked about the core problem being attribution. When a fishing boat snags a cable, Beijing calls it an accident.

Given the difficulty in attribution, how can the U.S. and our partners move from this posture of reactive concern to one of rapid attribution?

Mr. SCHMITT. Well, that is a big focus of our Underwater Mayhem project, Senator Ricketts. And I will just give a few examples, maybe of a couple of the case studies that we have done.

No. 1, you mentioned fishing vessels that just kind of snag a cable. The cable in the case of the Svalbard cable cut was the Russian fishing vessel, the "MELKART–5". And we saw in AIS that it traced its line and basically dragged its fishing equipment 126-some-odd times, maybe a few more, a few less, but 126-some-odd times, for one of the two cables. Unless there is incredibly good fishing in that very specific spot, in the middle of the Barents Sea, that is a sabotage operation.

In terms of Nord Stream, we know that there were Russian seabed warfare vessels over the Nord Stream 1 blast site 3 days before the blast, 3 months before the blast, and in addition to that, the Nord Stream 2 blast site, south of Bornholm, had Russian construction vessels where there were Russian vessels sitting directly at the eventual blast site for almost 18 months ahead of that.

You also had a situation in which one of the so-called pro-Ukrainian sailboat operatives, the person that actually helped rent this so-called sailboat, was a person that had a passport that showed that they lived in Kerch and that they were posting live tweets and social media messages from the Russian Federation after the incident took place. And what's more, this sailboat went from a marina that was physically adjacent to a Nord Stream 2 logistics center.

All of these together, again, need to be taken into account and use a data-driven approach to looking at each of these cases. That is why we thought it was probable in our study that the Russians were behind the Nord Stream case.

The last thing I will say is on all of these incidents, whether it be in China or in Russia, these two countries may or may not be officially cooperating in this case, but they definitely are learning from each other. And there a few cases, including the Balticconnector pipeline that was broken in 2023, in which a Chinese-flagged cargo ship, the "NEWNEW POLAR BEAR", was being escorted a few meters away by the Russian nuclear-class icebreaker, "SEVMORPUT".

We have also seen these same vessels show up inside of the Antarctic Treaty System as Russia breaks that treaty, looking for oil and gas, and they are stopping above cables as they go up and down.

So this is a global phenomenon, both for China and for Russia, and we need to do more to basically have a little more political courage to call out and call a spade a spade as quickly as possible.

Senator RICKETTS. So are there technical or regulatory things we need to change, or is it more just a matter of us trying to determine the attribution quickly and then just calling them out?

Mr. SCHMITT. I think the biggest thing that we can do is increase our level of satellite geospatial imagery from commercial actors because the time that it takes to declassify military and intelligence satellite data is simply too long. And even though we eventually may get there, if you have commercial data, that can be—I mean, it is never classified, so it is ready to go right away, and investigators can use this.

I saw a case in which the OFAC, the Office of Foreign Assets Control, of the Treasury Department was able to basically quickly sanction Russian vessels that off-took LNG from a facility near Murmansk that was under sanctions because that was out in the press because there was commercial satellite data. So supporting these and supporting the sort of regulatory oversight and NATO operations that it needs to take, in Europe's case, to get attribution.

Senator RICKETTS. So would you say that Russia and China are relatively less dependent on undersea cables than our allies and the United States? Is this an asymmetric advantage they have?

Mr. SCHMITT. No. There is no asymmetric advantage that I am aware of. Ninety-nine percent of the global internet runs through those cables, and it impacts Russia and China just as it does with us.

Senator RICKETTS. So if somebody was cutting the cables to Russia and China that would also potentially impact them, as well.

Mr. SCHMITT. Absolutely.

Senator RICKETTS. OK. Thank you very much, Mr. Chairman. I see my time is up.

The CHAIRMAN. Thank you. Let's go back for a minute to that jurisdictional question. It seems to me, my impression is we do not have a statute that is directly in point as far as a causation statute that gives us jurisdiction. Am I right on that? I suppose some U.S. attorney would have to stick his nose in the books and maybe find some way to do that. It would be easier if we had a direct statute that prohibited this kind of conduct, because again, you get in front of a judge and they get goosey too, on stuff that is not direct. Do you have——

Mr. O'BRIEN. I do not know about a direct criminal statute. I do know that if we use a sanctions authority, that then that does provide for criminal investigations subsequent to that. And that is why I think both using the authorities we currently have, which tend to be Russia-based as they apply here, but the new authorities you are proposing would help address some of this gap.

The CHAIRMAN. I guess criminal investigation is a long ways away from a criminal prosecution. It seems to me we probably need a direct statute here, that would make it a lot easier. If nothing else, it would allow an indictment, even if you could not get your hands on the person and underscore it, that this was going on.

Mr. O'BRIEN. If I may, just as a policymaker, what I would hate to see is these cases disappearing into a legal process that takes years and years.

The CHAIRMAN. And I agree with that. I agree 100 percent, that disappearing is a problem. As long as that warrant is standing out there, it is not going to disappear.

Mr. SCHMITT. I just want to point out that I totally agree on the sanctions point. The U.N. Law of the Sea can only go so far. We saw, in the case of a Russian shadow fleet vessel, the "KIWALA", it was interdicted and brought into Muuga Bay, Estonia. I actually went and saw this vessel as it was being interdicted, I believe it was in April 2025.

They could not keep that vessel there, even though it was under EU sanctions, because of the authorities that they had. And guess what? Just 6 months later or so, in September, that same vessel, that had been reflagged and renamed the "BORACAY" or the "PUSHPA" or a number of these other names, was the one that was suspected of launching drones, military drones, from the Russian Federation that, as it was passing Denmark, shut down the Copenhagen Airport. And I flew from the Warsaw Security Forum directly to Copenhagen to work with investigative journalists to look at the satellite data, and we found that vessel.

So ultimately the French Navy was able to interdict that vessel, and during the proceedings that have taken place legally, they have admitted that there are Russian security personnel, unaccountable to the captain or the crew, that are on those vessels. So that is something we need to really, really be concerned about.

The CHAIRMAN. Thank you.

Senator Shaheen.

Senator SHAHEEN. Well, that is a really frightening point.

Mr. SCHMITT. Sorry.

Senator SHAHEEN. And as we think about how do we do that, obviously sanctions are one option that we have. But what else should we be thinking about? I was in Copenhagen and I met with the person in their government who is working on this issue, their head of infrastructure. And one of the things that she said to me, I was asking her about this whole issue of how are you all dealing with this, because this is more of an issue for you than it is for us, and she said, "Well, the EU is working on the idea of having ships that can do the repairs in a timely manner."

Because the options, as I understand, are the CODEL that went to the Indo-Pacific met with a Japanese company that does subsea cables, and we were talking to them about how do you deal with

cable breaks. And they said, "Well, we track those, but we don't repair them. That has to be done by whoever owns the cables." And in order to do that they said there are basically two options. One is you need a bunch of ships that can do the repairs, and you need to have duplicate cables so that if one goes out you have got another one that can replace it.

But it seems to me, based on your testimony and sort of the conversations that I have had, that that is not the answer to the problem. The answer to the problem is to figure out how we can put in place ways to go after the vessels and the countries that are trying to disrupt these subsea cables. And clearly, to date, the U.S. Government has not been willing to sanction the vessels that we seem to be aware of, and, in fact, as we discussed earlier, Mr. O'Brien, we are actually giving a windfall to Russia so they can do more of this in the future.

So what should we be thinking about, if we are really going to address this? Dr. Schmitt, is the data that you have made public?

Mr. SCHMITT. Yes, Senator, it is. We have a first volume in Underwater Mayhem Volume 1, that is already out. We will have, in the next few months—and it is like don't ask when a Ph.D. dissertation is going to be submitted—but we will say in a few months Volume 2 is coming out, as well.

There are two points I want to make, Senator. First of all, in the case of repair vessels, there has to be more redundancy. There has to be more put on the water. Two years ago, when I was in Taipei, the interlocuters that I talked to asked me specifically, "Should we have a domestic repair capability in Taiwan?" and I said yes. Two years later, just a few weeks ago, they asked me the same question. I said, "Absolutely yes."

The Matsu Island cables that were cut, these islands of Taiwan that are near the PRC coastline, those had an internet outage of weeks and weeks, which could have been much shorter if they were not waiting for consortia vessels to come in. And I told them, in a case of a quarantine or an invasion of Taiwan, it is going to be very difficult. We saw this in the Straits of Hormuz situation with commercial vessels. They will not take that risk. Maybe governments will, but they will not take that risk in a time of war.

So that is No. 1. We need, obviously, as you said, consistent sanctions policy, having sanctions, your shadow fleet bill, that you and Senator Risch. We had Senator Whitehouse at the University of Pennsylvania a few weeks ago, that I hosted, talking about this. Those are essential. That will deprive the Putin regime of these oil windfalls. And we need consistent sanctions policy, whether it be no waivers in the previous administration for Nord Stream 2, and no waivers for Russian oil today. It has got to be consistent to keep the Putin regime in check.

Senator SHAHEEN. I agree, and I am sure, Mr. O'Brien, you are going to add to this. But not only would it have an impact on Putin but it would have an impact on Xi in China, and what they are doing, because obviously, they are benefiting from the oil that is being delivered by the shadow fleet, below market prices. Yes, go ahead.

Mr. O'BRIEN. Yes, I think two things: One is the information that is available now, I think, increases the responsibility of U.S. policy-

makers. If I had had access to the kind of information Dr. Schmitt is providing, we would have designated everybody he just listed in the Svalbard incident.

So that and the fact that it is public makes it easier to bring other countries on board. And that is the main point. We need the U.S. to organize a very active coalition. So I focused on sanctions, but I think it also means some physical presence at sea. The straits off Copenhagen are a particular point of concern, and there are examples of the U.S. doing this, based on the kind of authorities we already have, as long ago as the W. Bush administration. They organized a really effective voluntary coalition to address North Korea's activities. And I think that kind of thing is available in this area if we put our effort in.

Senator SHAHEEN. Well, I could not agree more, and thank you both. I am actually headed down to an Armed Services hearing where I will raise the same question. So thank you both.

The CHAIRMAN. Thank you, Senator Shaheen.

Senator Barrasso.

Senator BARRASSO. Thanks so much, Mr. Chairman. Thanks very much for your attention to this very critical matter. We are seeing undersea infrastructure is central to the functioning of our economies, our militaries, our alliances all around the world.

There is a very interesting book called "The Web Beneath the Waves," that outlines all of the damage that has been done. And you look at some of the undersea cables, in terms of where they are, we intentionally wanted to map them when they were laid so there would not be accidental injury to that method. So people know where they are, but it does seem that there is ongoing sabotage.

We discussed the situation of where cables are cut. I want to know if there are backups that exist within the networks to ensure communications can continue if cables are cut.

Mr. SCHMITT. Senator Barrasso, thank you. That is an incredibly important point. I will just say, No. 1, just to remind everyone, since this is for the record, there is no satellite-based panacea for all of the global internet that is going beneath the sea. I think everyone hears of Starlink and says, "Oh, if the cable is cut I will just use that." Well, in the case of Taiwan they have built 700-some-odd satellite uplink stations as backups. That is not for all of society. That is for government, emergency use. They have microwave links from their outlying islands of Penghu and Matsu to the main island of Taiwan. So that is important.

I think, Senator Barrasso, what you raised is, yes, there are maps. That is on purpose, so these actors do not cut it. We need to make sure that some of these cables in the future are buried, deliberately buried below the seabed, to make sure the anchor drags can be mitigated, to some extent. These are the sorts of technical measures and monitoring. Of course, we need subsea drones and underwater unmanned vehicles, as well.

Senator BARRASSO. Which leads to my next question. What is accidental and what is not? And I do not know. Do you have an assessment yet of how much of these so-called accidental patterns are truly accidental and what is deliberate gray zone testing?

Mr. SCHMITT. I will give you a preview of Underwater Mayhem Volume 2, which is coming soon, just to let you know. We will look and have talked to ship captains, technical experts, subsea divers, all sorts of the technical people that actually work in this industry, not just think tank experts. And what we have found is that there is no chance, in a lot of these cases, that these are, quote/unquote, "just accidents."

Dragging an anchor for one nautical mile because you lost steerage, that is possible. Dragging it at full speed through the Gulf of Finland for 200 nautical miles, severing cables and pipelines along the way, that is not normal action, and that is not what we should be accepting.

I will say one last thing. We are conflating the issue of the shadow fleet with some of these vessels, and people are saying, "Oh, well, the shadow fleet is really in low grade of repair. They have bad captains. Of course, they are accidentally cutting these." The truth is only one or two have been cut by shadow fleet vessels. Most of these are vessels that are in good repair.

Senator BARRASSO. So I think of our two newest NATO allies, Sweden and Finland. What is happening in that area? Have there been discussions about NATO members possibly coming together and invoking Article 4 to force a formal consultation on these emerging shadow of war, if you will? What are your thoughts on this in terms of the Article 4?

Mr. SCHMITT. I have briefed the North Atlantic Council's energy security version. They do this once a year. And I called on member states to invoke Article 4. My understanding is that one or two member states have pushed back on this.

Look, Senator, we have seen Article 4 used this year when drones flew from the Russian Federation into Polish airspace. We have seen it in Estonia last year, when Russian fighter jets went into their airspace. Why haven't we seen it for subsea cables? And I think part of the reason is this is something that some political actors in Europe and possibly in the United States do not want to, quote/unquote, "escalate." So we need to say, look, we need to raise this to the political level, because what that does, it also unlocks operational support to build out things like Operation Baltic Sentry, which has, I think, been quite successful to deter some of these actions.

Senator BARRASSO. You know, a couple of years ago the United States established a cable security fleet to subsidize some commercial cable repair ships, to help address the risk. In your opinion, are the current capabilities for repair sufficient for the level of sabotage that we are seeing?

Mr. SCHMITT. No. Absolutely not. We have very limited capabilities in the Taiwan Strait. Taiwan does not have a domestic capability. They have a domestic deployment capability but not repair capability. And in a time of war, that is insufficient.

And we also see that there are consortia of cable repair vessels in Europe, but not enough. You need more redundancy of the cables, more redundancy of the repair capabilities, and that can start to make bad actors think, well, maybe it is not so useful to do this, because, guess what, we are not going to get away with it.

Senator BARRASSO. Are there important steps we ought to be taking now to reduce the leverage that Russia is gaining from these attacks?

Mr. SCHMITT. Yes. I think that we need to be absolutely increasing sanctions, especially through the shadow fleet bill that has come up through this committee, and make sure that we are holding the Putin regime to account for these sorts of activities. And also name and shame. I know that is not the biggest and flashiest thing, but that is important, sanctioning all of the shadow fleet vessels.

I know that the Subsea Act that has been passed out of this committee also says that the U.S. intelligence community and the State Department need to send a list, publicly, and list out all of the GUGI vessels, this subsea mission directorate that does these sorts of heinous acts. They need to list those publicly so that we do not just say, oh, it is probably a shadow fleet vessel or it is probably an intelligence vessel. This is a vessel specifically built by Russia to inflict pain on global democracies, and we need to know this early and often so that then states can take action to bar them from their ports or issue sanctions and other things like this.

Senator BARRASSO. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator CURTIS.

Senator CURTIS. Thank you, Mr. Chairman. Thank you, witnesses. This committee recently passed a bill that I have with Senator Rosen, the Critical Undersea Infrastructure Resiliency Act. The bill contains an initiative to harden and monitor Taiwan's undersea cables and proposes new sanctions.

I am going to jump into a few questions, but I want to pick up where my colleague left off. I was in Taiwan with the ranking member just a couple of weeks ago. We visited one of the factories that actually produces the cable. We were all very curious about what they were doing to prevent breaks, whether it is undersea monitoring or cameras. And what we found is zero motivation because they produce cables. Their answer was to just lay more cables.

And I am curious what your experience is. Do we have a motivation problem here, and it just feels like there was very little effort to put in equipment that could monitor and see a problem coming before it got there. What is your experience?

Mr. SCHMITT. Well, look. I actually visited the Walsin Lihwa factory in Kaohsiung. I didn't go in because the back half of the building is still under construction. But that is for electricity cables, so this is an energy security question for Taiwan, as well, as these cables connect to their offshore wind and can interconnect to their outlying islands.

One of the things, and this is more from a physics standpoint, if you put a fiber optic cable on the seabed you can start to monitor the vibroacoustic environment, the vibrations of subsea vessels, sea surface vessels, and things like this around it.

So this is actually what happened in the case of the Chungwa Telecom line, when last year the "HONG TAI 58", this vessel from China, cut the cable. The Taiwanese Coast Guard was alerted by Chungwa Telecom right before that cable cut took place, because

they knew this vessel was sitting there. And then they acted just a few hours later when they got their kind of armada together, to seize this vessel.

And what they found, this was an empty Chinese vessel that was a bulk carrier that had no bulk on it. Its cargo doors were actually rusted shut, so that it could not be used for that. So it was only used as a sabotage vessel, and the prosecutor that I talked to likened it to a pawn sacrifice from the PRC. In other words, Xi is sending out a vessel that he does not care if he loses. I wanted to see that vessel, but it has already been deconstructed and scrapped. So I asked for a piece of it, and I do not know if I am going to be able to get one.

Senator CURTIS. It would be a good paperweight.

I know I am late to this hearing, and if you have already discussed this please indulge me. But give me a sense of if there is major disruption to Taiwan with multiple cables, the impact militarily and economically that potentially could happen.

Mr. SCHMITT. So there is often a discussion of, OK, Taiwan does have redundancies. There is something like 14 cables connecting out to the global internet. There are also cables to the Penghu Islands, Matsu Islands, and Kinmen, and others like this.

I have often been asked, "We have this redundancy, so China couldn't possibly cut all 14 cables." I said, "You've got another thing coming, because guess what? If they can cut one or two cables by dragging an anchor pretty easily, in an all-out military assault or invasion, or even a blockade or a quarantine, those can be cut pretty quickly."

What that will have is an immediate impact on the global economy. It is kind of like the Straits of Hormuz closure by the IRGC for the internet. And it means that all of our economic trade with Taiwan, which is significant, will be cutoff, not just for us but for our partners and allies. And I will tell you, it will make military coordination more difficult. It will not stop it, because there is satellite backup, but it is something that we really need to think of.

And I have talked with folks in Taiwan that are in the military. I think that it needs to be part of the military's doctrine in Taiwan that rapid cable repair, under fire, is important, as well, to deter this.

Senator CURTIS. Yes. So another question. We have learned a lot from Taiwan, what is happening there. What lessons can be applied to the Baltic, and what should we be doing in the Baltic that we have learned from the Indo-Pacific?

Mr. SCHMITT. Sure, yes. I think that one of the biggest things is, again, repair capabilities. We need more repair capabilities in Europe. We need a legal system that allows for attribution and jurisdictional questions, we have mentioned already in this hearing. And again, just like in Taiwan, where they are aware of this, we need European democracies to be ready to act, and have that capability through NATO to do so.

Senator CURTIS. Mr. O'Brien.

Mr. O'BRIEN. I will just add, Senator, and thank you for your bill, the motivation problem, I think, is with the U.S. Government. All of the undersea infrastructure, separate companies, others, they

are all doing their work. It is unrealistic to expect them to monitor the activities of a predatory superpower.

The same thing with middle powers. They do not have the ability to stand up. So this is for the U.S. Government to say the future of our economy depends on this infrastructure. We have to make sure that we have enough of it, and that we can repair it, but that we can protect it. And that involves both a more robust sanctions program, I think more physical presence, and coordinating with others who are affected so that they are able to operate effectively.

Senator CURTIS. It feels to me like the technology is not that difficult. It is the will, right, to put it in. And along these lines, and let me defer to you, you mentioned the one incident in Taiwan where they were able to find the actor. How prepared are we to find the bad actors, just generally speaking?

Mr. SCHMITT. I mean, we are prepared. I think the U.S. geospatial intelligence is strong. I think we need more commercial data to make sure that satellite data can be released quickly, so that these sorts of indictments can happen rapidly.

But the other thing I want to point out, and I am going to bring it back to the Nord Stream case really briefly, and say we need to listen not only to policymakers—no offense—but technical experts like those that work in the industry——

Senator CURTIS. I am so offended.

Mr. SCHMITT [continuing]. People that build the cables, people that are captains of these ships, people that actually dive to the bottom of the seabed. We talked with many of these experts, and they said that the idea that using a rental sailboat to blow up Nord Stream is not technically impossible, but that it would never be used in this way. And they said it is an insufficient platform. It would have a large radar profile to begin with, because of the sail, obviously, and that you would use a drone, a cheap drone.

And I will tell you what, there is a lot of media that have gone out there and put a drone in the seabed and looked at the damage site, and they have proven you can put a drone down there. You can put one down there with a camera. You can put it down there with explosives. I went out and actually got seabed sonar data at the Nord Stream 2 blast site, and you can just go out there.

So again, listening to the experts in a way that is integrated not only into our policy but our media and discussions of these, because it takes so long for attribution that disinformation can be sowed. And obviously in the case of Nord Stream, Russia pointed the finger at the U.K., Poland, the United States, of course, and all these different directions to sow chaos right after this happened. Again, a disinformation campaign that seems kind of precooked to me.

Senator CURTIS. Yes.

Mr. O'BRIEN. I will just add, we know much more today than even 2 and 3 years ago. The NATO efforts, the EU efforts provide information very quickly, and having the access to the work that Dr. Schmitt and others are doing in the public sphere, it increases the responsibility of policymakers to act quickly, because we can no longer say we do not know or we cannot share.

Senator CURTIS. Thank you both.

Mr. Chairman, I yield.

The CHAIRMAN. Thank you, Senator Curtis.

Thank you, gentlemen, for being here. Incredibly interesting and important, and it has really spurred some ideas, I think, amongst the committee here, which Jeanne and I are already talking about.

With that, I will leave the record open until close of business tomorrow for further submissions. Again, thank you so much for being here. And with that the committee is adjourned.

[Whereupon, at 11:19 a.m., the hearing was adjourned.]

○