Protecting the EU's Submarine Cable Infrastructure: Germany's Opportunity to Transform Vulnerability into Mutual Resilience

Hartmann, Jannik

Veröffentlichungsversion / Published Version
Stellungnahme / comment

No. 23
July 2023

DGAP POLICY BRIEF

Protecting the EU's Submarine Cable Infrastructure

Germany's Opportunity to Transform Vulnerability into Mutual Resilience

Jannik Hartmann
Student Assistant,
Alfred von Oppenheim Center
for the Future of Europe

Submarine cables handle over 95 percent of the world's internet traffic, making them essential for everything from finance to foreign affairs. The September 2022 attack on the Nord Stream pipelines and increased Russian naval activity brought greater awareness of how European – and German – interconnectedness also brings vulnerability. The urgency of tackling this threat offers Germany an opportunity to take a structural and joined-up approach that shows it can act as a "team power."

– **Germany is not home to major submarine cable connections so it must rely on the cable connectivity provided by other EU member states to transfer data to other continents. Thus, it is significantly dependent on them.**

– **Overt attacks on Europe's cable connections remain improbable during peace time. However, the actors that may have an interest in – and the capacity for – disrupting them can disguise their attacks as accidents.**

– **To deal with the downsides of interdependence efficiently, the EU and its member states should bolster both mutual resilience and deterrence. This requires focusing on structural measures.**

– **Germany should push for closer EU cooperation with the new NATO initiative on submarine infrastructure, work with partners to strengthen Europe's cable network, and propose to both increase and centralize EU repair and maintenance capabilities.**

The deliberate attack on the Nord Stream 1 and 2 pipelines in September 2022 brought the topic of submarine infrastructure to Europeans' attention and highlighted how vulnerable to man-made threats the EU and its member states have become. This also includes countries like Germany, which have no major underwater cables of their own but are dependent on the interconnections with other EU states that host such infrastructure. Germany now has an opportunity to demonstrate a new "team power" approach by helping to address the concerns and direct vulnerabilities of others.

In doing so, Germany can help itself while bolstering mutual resilience through both better teamwork within the EU and enhanced, practical cooperation with NATO. This would also help Germany to develop its foreign policy role, showing that it takes the concerns of others seriously and, in practical ways, is willing to lead by example while serving collective interests.

TIES THAT BIND: EU SUBMARINE CONNECTIVITY

Maritime cables handle more than 95 percent of global internet traffic. They are the essential, yet often overlooked, scaffolding of our interconnected digital world. Although we believe ourselves to be increasingly wireless, signals from our cable-free devices are in fact carried only as far as the nearest cell tower. From there, terrestrial cables and eventually submarine cables transfer our data over thousands of kilometers. Satellites, due to their comparatively high costs, are a partial alternative at best, suitable only for the most remote locations. The lower costs and much higher capacities of undersea cables leave us firmly bound to them. In addition to powering our economy by facilitating over ten trillion euros of financial transactions daily, they enable our military command-and-control structures, drones, and other integrated and digital weapon systems vital for Europe's defense.

About 250 active cables ensure the EU's connectivity to the global internet. One third of these are land-based cables that connect EU member states to non-member states in Europe. Although they go through states like Russia, hostile acts on them would amount to self-sabotage. The remaining two thirds are submarine cables, which are not only more vulnerable but also more unevenly distributed. Three littoral member states – Germany, Croatia, and Poland – have no major undersea cables of their own, making them *significantly* dependent on those of fellow EU member states and allies. Island EU member states such as Malta and states with noncontiguous connections such as Finland rely on only 39 cables to ensure their connectivity.

The EU's external submarine connectivity to the rest of the world varies considerably in its strength and quantity depending on the destination. The strongest connection in terms of cumulative transmission capacity can be found between the EU and North America. Even after Brexit, that connection includes more than ten transatlantic links. It can be assumed, however, that official numbers do not include classified (transatlantic) links built by intelligence agencies that are not plotted on public maps.

Other strong connections can be found between the EU and the Middle East and North Africa (MENA) region with a total of twenty-seven fiber optic connections in place. Ten submarine cable systems connect the EU with Eastern and Southern Asia, almost all of which run through the Suez Canal into the Red Sea. Connections to other regions such as South America remain scarce as traffic is mostly routed via North America.

THREATS TO SUBMARINE INFRASTRUCTURE

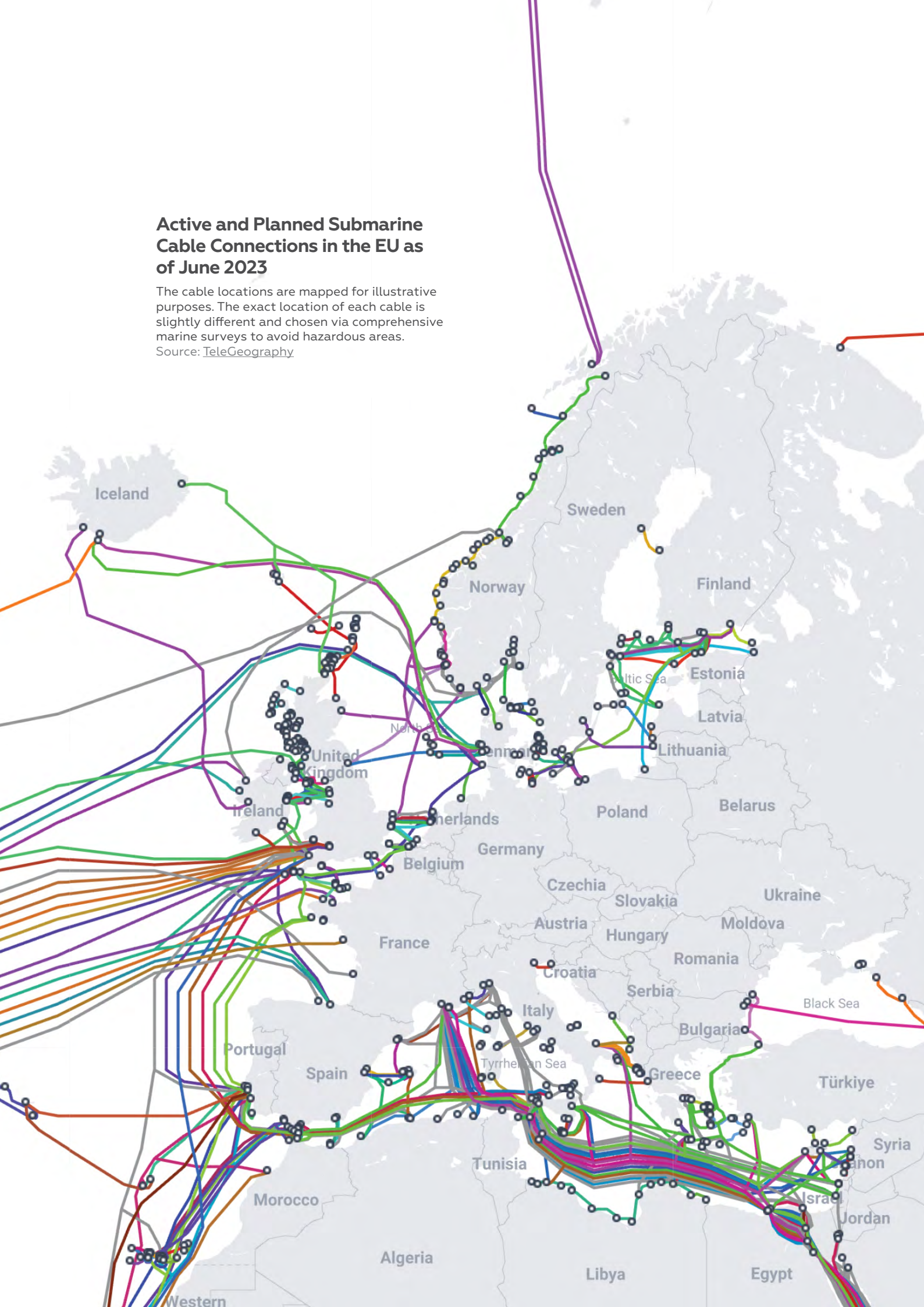
Connections that bring opportunities and benefits also entail exposure to risks and threats. While undersea cables prove this in spades, severe and overt attacks remain improbable during peace time. And while the actors that might have an interest in – and the capacity for – disrupting Europe's cables are relatively clear, the real problem comes from their ability to disguise their actions. Below, I assess three primary potential threats: man-made destruction, systemic disruption, and the targeting of supporting infrastructure.

From Accidents to Deliberate Attacks

Thus far, there have been no officially verified incidents of deliberate damage inflicted by any state or non-state actor on submarine cables. Given the prevalence of genuine accidents, however, it is eminently possible to disguise deliberate attacks as such. Nearly two thirds of all yearly cable disruptions are caused accidentally during commercial activities that include

Active and Planned Submarine Cable Connections in the EU as of June 2023

The cable locations are mapped for illustrative purposes. The exact location of each cable is slightly different and chosen via comprehensive marine surveys to avoid hazardous areas.
Source: TeleGeography



anchoring and dredging.[1] Cables are plotted on navigational charts in coastal and shallow waters to prevent accidents, but their "protection zones" are often violated due to ignorance or compromised through recklessness. Attacking cables in deep water, where their position remains classified and can be shifted by currents, is more difficult. Once located, however, they too can be destroyed by remotely triggered explosives and crewed or uncrewed submersible vehicles. A recent report, which identified several alleged Russian spy ships disguised as fishing and research vessels in the Baltic Sea, added to such concerns, as they were suspected of gathering information on the exact location of submarine infrastructure.[2]

Damaging a few outgoing cables from the EU's mainland would not cause significant overall disruption as the traffic can be rerouted. But the EU's island member states and other territories linked to it by undersea cables lack diversified infrastructure, which puts them at much greater risk. While individual cases of damage may be repaired within two weeks, it should be noted that private repair agreements can only provide threadbare capacity for addressing wider problems. Moreover, the availability of repair ships is sparse. Only three such ships are located in the EU (one in northern France and two in the Mediterranean); one more is based in the UK and an additional one on the Atlantic coast of the United States. Despite its unlikelihood, a simultaneous attack on cables, key landing stations, and repair capabilities would certainly wreak great destruction and could lead to a full-scale EU blackout.[3]

Systemic Disruption

The governance of submarine infrastructure involves an intricate set of stakeholders. Most submarine cables are owned by former state telecommunication companies but are operated and repaired by other private sector actors, creating scope for systemic disruption by firms owned or controlled by foreign governments. Between 2015 and 2021, companies with ties to the Chinese state have significantly increased their share of both the construction and ownership of cables in the framework of China's Digital Silk Road (DSR) project, which is part of its Belt and Road Initiative (BRI).[4]

HMN Tech (formerly Huawei Marine Networks) owns ten percent of the global cable infrastructure and has built or repaired more than one quarter of all 400 active cables worldwide.[5] This not only compromises critical infrastructure but also creates scope for the interception of data. Built-in back doors could be used to tap into transferred data or to limit traffic volumes. Although deliberate Chinese sabotage of cable infrastructure is considered unlikely to occur outside the Indo-Pacific – where China was recently accused of using sand dredgers as "grey-zone warfare" tactics against Taiwan – it cannot be fully ruled out given the EU's interests in this region.[6]

Network Disruption

Finally, it is worth noting that submarine cable connections need a whole infrastructure of their own to function, creating vast new vulnerabilities. Much of this infrastructure is land-based and comparatively easy to access. Cable Landing Stations (CLS) connect submarine cables onshore and ensure that all cables that exceed 150 kilometers in length are supplied with the electricity they require to function. Internet Exchange Points (IXPs) enable local internet providers – and thus their customers – to connect to international networks. Data Centers function as storage facilities for webpages and their contents.

Attacks on IXPs and Data Centers are unlikely to cause mass outages as plenty of them exist in the EU (Germany alone houses 83 IXPs and 54 Data Centers). The greater threat comes down to Cable Landing Stations. Here, hub zones where dozens of cables enter one station – such as in Marseille, France or Sesimbra, Portugal – make tempting targets and significant weak spots. The location of these stations is not

1 Jiexin Zheng et al., "Indentation and external pressure on subsea single wall pipe and pipe-in-pipe," *Ocean Engineering* 81, no. 19 (2014), pp. 125–132: https://www.sciencedirect.com/science/article/pii/S0029801814001176 (accessed July 1, 2023).

2 Oliver Moody, "Russian naval vessels 'near Nord Stream' days before attack," *The Times* (March 26, 2023): https://www.thetimes.co.uk/article/russian-naval-vessels-near-nord-stream-days-before-sabotage-v5fgl9tjn (accessed June 15, 2023).

3 European Parliament, Security threats to undersea communications cables and infrastructure – consequences for the EU (June 2022): https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf (accessed June 13, 2023).

4 David Gordon, "The Digital Silk Road: Introduction," IISS, Online Analysis (2022): https://www.iiss.org/online-analysis/online-analysis/2022/12/digital-silk-road-introduction (accessed July 2, 2023).

5 Anthony Bergin, "Digital age lies vulnerable to threats from underwater," Online Analysis ASPI, (2021): https://www.aspi.org.au/opinion/digital-age-lies-vulnerable-threats-underwater (accessed June 31, 2023).

6 Yimou Lee, "China's latest weapon against Taiwan: the sand dredger," Reuters (February 5, 2021): https://www.reuters.com/article/us-taiwan-china-security-idUSKBN2A51EJ (accessed June 15, 2023).

publicly available but tends to appear in so-called spotting-communities.[7] While a full EU blackout caused by such an attack remains unlikely, significant ruptures remain possible and would be difficult to fix in the short term.

AWARENESS AND CAPABILITIES ARE STILL UNEVEN AND INSUFFICIENT

Denmark, France, Italy, Portugal, Spain, and the islands of Malta and Ireland are the EU's most important member states when it comes to worldwide underwater cable connectivity. Yet it is only in Ireland, France, and Portugal that a significant level of political awareness and sufficient capabilities vis-à-vis maritime infrastructure can be found. The reason is clear: bitter experience. For instance, Ireland's Defense Forces, prompted by Russian naval activity, issued a report in 2021 that called for enhancing submarine surveillance capabilities.[8] In September 2022, the French Navy escorted a Russian submarine spotted off the coast of Brittany out of its contingency zone.[9]

But it is not just experience that matters; public and political support do too. While Italy, Spain, and Malta have now acknowledged the issue in national security documents, there was little public debate on increasing protection prior to Russia's war in Ukraine. Even since that war, public debates have surfaced only marginally. Lastly, Denmark appears as an outlier with relevant cable infrastructure but there is still an overall low level of public awareness and response in that country – despite recent Russian submarine activity off its coast.

This lack of awareness comes despite NATO's 2017 warning of precisely such dangers.[10] They were further stressed at the meeting of NATO ministers of defense in 2020[11] and – most recently – prompted the Alliance to launch a new center in Northwood, England that is dedicated specifically to submarine infrastructure in June 2023.[12] Given that states such as Germany rely on the cables of others and that the protection of maritime infrastructure in territorial waters is in the hands of member states, the persistence of uneven awareness is a cause for concern.

On EU-level this insufficient political prioritization was rather matched than compensated. With Russia's large-scale invasion of Ukraine in 2022 and the ramifications of (un)wanted critical infrastructure dependencies, this changed and prompted the European Parliament to commission a comprehensive risk analysis in June 2022.[13] Heightened urgency, however, only came after the Nord Stream attacks of September 2022, spurring the European Council to issue a five-point plan to increase awareness in October.[14] This was followed by a Council directive in December 2022 to "strengthen the resilience of critical infrastructure," including undersea cables.[15] Yet no EU entity is leading on this issue or explicitly tasked with the protection of submarine cables.

In general, the maritime security of the EU involves three technical agencies beyond the armed forces of its member states: the European Fishery Control Agency (EFCA), the European Maritime Safety Agency (EMSA), and the European Border and Coast Guard Agency FRONTEX – with only the latter having meaningful law enforcement capabilities. The European Border Surveillance System (EUROSUR), which FRONTEX operates, integrates assets such as

7 Paul Newbury, "Submarine cables – resources on the web" (September 23, 2014): https://paulwalternewbury.wordpress.com/2014/09/23/submarine-cables-resources-on-the-web-serious-nerd-alert (accessed June 23, 2023).

8 Commission on the Defence Forces, Report of the Commission on the Defence Forces (February, 2022): https://www.rte.ie/documents/news/2022/02/215358-a21b9438-45a6-4c26-a508-c0d1aeeeb336.pdf (accessed June 28, 2023).

9 Alex Richardson and Jonathan Oatis, "Russian submarine spotted off French coast end-September – French Navy," Reuters (October 14, 2022): https://www.reuters.com/world/europe/russian-submarine-spotted-off-french-coast-end-september-french-navy-2022-10-14 (accessed June 23, 2023).

10 Michael Birnbaum, "Russian submarines are prowling around vital undersea cables. It's making NATO nervous," *The Washington Post* (December 22, 2023): https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html (accessed June 27, 2023).

11 NATO, Online press conference (October 22, 2023): https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en (accessed June 28, 2023).

12 Lorne Cook, "NATO moves to protect undersea pipelines, cables as concern mounts over Russian sabotage threat," PBS (June 15, 2023): https://www.pbs.org/newshour/world/nato-moves-to-protect-undersea-pipelines-cables-as-concern-mounts-over-russian-sabotage-threat (accessed June 28, 2023).

13 European Parliament, Security threats to undersea communications cables and infrastructure – consequences for the EU (June 2022): https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf (accessed June 13, 2023).

14 European Commission, Critical Infrastructure: Commission accelerates work to build up European resilience (October 18, 2022): https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238 (accessed June 28, 2023).

15 European Council, EU resilience: Council adopts a directive to strengthen the resilience of critical entities (December 8, 2022): https://www.consilium.europa.eu/en/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities (accessed June 29, 2023).

drones, radar, and aircraft, but these are mainly used to counter irregular migration.

RECOMMENDATIONS

Although the recent reconsideration of resilience and deterrence regarding cables may have been prompted by the Nord Stream attacks and Russian activity around submarine infrastructure at a time of war, it points to a wider issue. To deal with the downsides of interdependence efficiently, the EU and its member states should proactively consider how to address their vulnerabilities by bolstering both mutual resilience and deterrence. In the absence of public outcry, this requires structural measures. Accordingly, the EU should focus on increasing protection to prevent malicious behavior and strengthen the resilience of the cable network through stricter regulation and enhanced response mechanisms.

Working closely with other European actors, Germany, should seize the momentum created by the Nord Stream attacks to address underlying shortcomings. It can show a "team power" approach in action by prioritizing the following steps:

Deterring Attacks, Preventing "Accidents," and Enforcing Protection: EU institutions should seek and facilitate enhanced coordination with NATO – especially via the Alliance's new dedicated center in Northwood – to better police EU waters, identify and interdict vessels engaged in hostile or suspicious activity around critical infrastructure, and enforce undersea cable protection zones.[16] Building on its high-level representation to NATO on this issue, Germany should float the possibility of establishing an EU mission to undertake some of these tasks or of having an agency such as EMSA directed to do so by sharing resources with FRONTEX. Building on the Council's recent steps, better coordination of national security strategies and identification of common vulnerabilities, including collective stress testing, should be mandated.

Strengthening the Network: As a state that is indirectly vulnerable, Germany should push for greater collective oversight of the ownership and operation of cables and related infrastructure with member states reporting to a common watchdog body. Particular effort should be made to avoid dependencies on systemic rivals – something Germany would also need to implement in practice, thus demonstrating another aspect of acting like a "team power." Companies such as HMN Tech should be banned from owning or operating cable infrastructure in the EU.[17] Encouraged and overseen by the European Commission, member states should keep such dependencies below an agreed threshold and eliminate them entirely as soon as possible and no later than 2030. Current and future Cable Landing Stations should be dispersed according to mutually agreed guidelines to make concerted attacks leading to greater damage more difficult.

Centralizing and Increasing Repair and Maintenance Capabilities: Instead of relying on ad hoc private sector repair capabilities, the EU should take over the responsibility for repairing cables in the event of damage. Germany could again show "team power" in action by agreeing to fund a repair ship despite having few connections of its own. The number of repair ships and stock of raw materials should be increased to a commonly agreed minimum level and stationed where critically relevant. Additional capacity should be funded by common mechanisms. In the short term, it should be concentrated on hub zones on the Baltic and Portuguese coasts that currently lack fast response coverage.

16 Lorne Cook, "NATO moves to protect undersea pipelines, cables as concern mounts over Russian sabotage threat," PBS (June 15, 2023): https://www.pbs.org/newshour/world/nato-moves-to-protect-undersea-pipelines-cables-as-concern-mounts-over-russian-sabotage-threat (accessed June 28, 2023).

17 Elisabeth Braw, "Decoupling Is Already Happening – Under the Sea," *Foreign Policy* (May 24, 2023): https://foreignpolicy.com/2023/05/24/china-subsea-cables-internet-decoupling-biden (accessed June 29, 2023).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Helga Beck

Layout Lara Bührer

Design Concept WeDo

Author photo(s) © DGAP