Hertie School
Centre for
International Security

Security Tech Brief

March 2023: The Vulnerability of Subsea Internet Cables

Hertie School

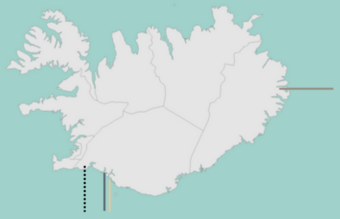
Security Tech Brief:

The Vulnerability of Subsea Internet Cables

Hertie School
Centre for
International Security

About 95% of intercontinental internet traffic, including most government and military communication, travels through approximately 450 privately-owned, garden-hose-sized subsea fiber-optic cables that crisscross the world's oceans. Despite the crucial role that these cables play in global communication, they are relatively fragile and experience an average of approximately 100 faults per year, most of which are caused by shipping activities. When a cable experiences a fault, the information that was being transmitted through it is typically rerouted through other cables. To accommodate this potential increase in traffic, major cables are typically only utilized at approximately 18% of their total capacity. Most countries are connected to multiple subsea cables to ensure redundancy and minimize the impact of cable faults.

Connections to Iceland



— FARICE-1: Faroe Islands, United Kingdom
— DANICE: Denmark
— Greenland Connect: Greenland, Canada
⋯ IRIS (expected in 2023): Ireland

Potential Threats: Sabotage and Espionage

1 Sabotage: Theoretically, it is easy to cut undersea fibre optic cables or attack cable landing stations, but there have been no major attacks on these systems since at least World War II.

Save for isolated areas like Tonga, cutting a single cable is typically insufficient to cause widespread disruption in the targeted country as traffic will be re-routed through other cables. According to open-source literature, a coordinated attack on multiple cables at once is necessary to cut off a European country's internet. Crippling transatlantic communications might therefore require a large-scale military operation, rather than one or two cut cables. The largest but most indiscriminate impact could be achieved by attacking chokepoints where multiple cables run close together, such as off the coast of Egypt or in the Strait of Malacca.

2 Espionage: Placing a tap on a cable on the sea floor may be possible, but it is a highly challenging operation and its feasibility is uncertain. Subsea cables are easier to tap on land.

While Western security services have tapped internet cables, they reportedly did so where the cables make landfall at cable landing stations rather than underwater. Russia operates specialized vessels that are suited for underwater tapping operations, but whether they could execute such operations successfully is unclear.

Europe's Internet: Major Interregional Subsea Cables and their European Landing Points

Cables to North America

Atlantic Crossing-1	United Kingdom, Netherlands, Germany
AEC-1	Ireland
Apollo North	United Kingdom
Apollo South	France
Dunant	France
EXA Express	United Kingdom
EXA North/South	Ireland, United Kingdom
FLAG Atlantic-1	France, United Kingdom
Grace Hopper	United Kingdom, Spain
Havfrue	Denmark, Ireland, Norway
Marea	Spain
Tata TGN-Atlantic	United Kingdom

Cables to South America

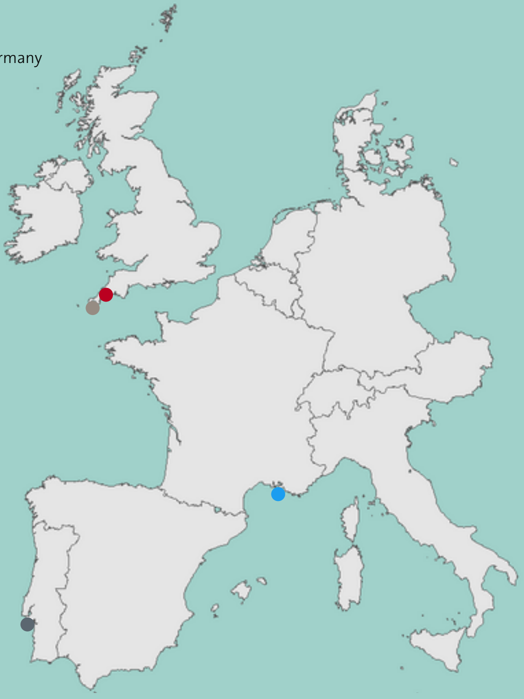
Ella-Link	Portugal

Cables to East Africa

ACE	France, Portugal
Glo-1	United Kingdom
MainOne	Portugal
SAT-3/WASC	Portugal, Spain
WACS	Portugal

Some cables, notably cable connections across the Mediterranean to North Africa, have been omitted for clarity.

Data based on the Submarine Cable Map provided by TeleGeography. Available at :https://www.submarinecablemap.com/



Cluster of Cable Landing Stations

● **Marseille, France**
6 Europe-Asia-Africa Cables

● **Bude, England**
3 Transatlantic Cables, 1 Europe-Asia-Africa Cable, 1 Europe-East-Africa Cable

● **Porthcurno, Skewjack, Whitesands Bay, England**
2 Transatlantic Cables, 1 Europe-Asia-Africa Cable

● **Sesimbra, Seixal, Carcavelos, Portugal**
2 Europe-Asia-Africa Cables, 4 Europe-East-Africa Cables

Cables to Asia, Africa, the Middle East

Asia Africa Europe	France, Italy, Greece
Europe India Gateway	United Kingdom, Monaco, Portugal, Gibraltar
FLAG Europe-Asia	United Kingdom, Spain, Italy
Hawk	France, Cyprus
IMEWE	France, Italy
PEACE Cable	France, Cyprus, Malta
TE-North	France, Cyprus
SeaMeWe-3	Belgium, United Kingdom, France, Portugal, Italy, Greece, Cyprus
SeaMeWe-4	France, Italy
SeaMeWe-5	France, Italy

What are subsea cables?

The global internet relies on fiber-optic subsea cables that carry around 95% of all international internet traffic.[1] Currently, about 450 operational cables connect every continent except Antarctica to the internet. These cables are more efficient and cost-effective than satellites for transmitting data, making them the current technology of choice for global communication.[2] Each cable contains a strand of glass called an optical fiber, which is so thin – the diameter of a human hair – that several can be bundled into one cable. For example, the *Marea* cable from the U.S. to Spain has eight fiber pairs, each able to transmit up to 28 terabits per second - enough to stream five million HD movies at once. [3] Optical amplifiers are placed every 60-100 km to keep the signal strong and are powered by electricity running through the cable's copper sheathing. Since cable systems are expensive to build, they have typically been funded by a consortium of telecom companies. AT&T, France Télécom and British Telecom built the world's first fiber optic subsea cable in 1988.[4] In recent years, however, content providers like Microsoft, Google, and Amazon, who accounted for 91% of used capacity on transatlantic routes in 2020, have begun investing in their own subsea cables.[5] Most online communication, including military and government traffic, runs through privately-owned subsea cables, although there are reportedly unmarked military cables as well.[6] Western officials have warned that a state actor – usually Russia – could target subsea cables, potentially threatening the global internet and related financial activity, which the US Federal Communications Commission estimates to be worth about $10 trillion per day.[7]

How vulnerable are cables to sabotage or espionage?

Despite their economic significance, subsea cables break relatively easily. They are thin, below ten centimeters in diameter even when double armored in shallow waters. In deeper waters, cables are often only as thick as a garden hose, about two centimeters in diameter.[8] There are approximately two cable faults per week, amounting to about 100 to 150 faults every year.[9] Two-thirds of these faults are caused

[1] L. Carter et al., "Submarine Cables and the Oceans – Connecting the World," UNEP-WCMC Biodiversity Series 31 (UNEP, 2009), 8.

[2] Nicole Starosielski, "In Our Wi-Fi World, the Internet Still Depends on Undersea Cables," *The Conversation*, January 25, 2019, https://theconversation.com/in-our-wi-fi-world-the-internet-still-depends-on-undersea-cables-49936.

[3] Rob Verger, "A 10-Million-Pound Undersea Cable Just Set an Internet Speed Record," *Popular Science*, March 5, 2019, https://www.popsci.com/submarine-cable-data-transfer-record/; Dan Swinhoe, "Infinera Reaches Record 30Tbps Speeds on MAREA Trans-Atlantic Submarine Cable," *Data Center Dynamics*, January 13, 2021, https://www.datacenterdynamics.com/en/news/infinera-reaches-record-30tbps-speeds-marea-trans-atlantic-submarine-cable/.

[4] Alternatively, individual companies can fund a cable and lease capacity to telecommunication companies. Yevgeniy Sverdlik, "How Hyperscale Cloud Platforms Reshaped the Submarine Cable Industry," *Data Center Knowledge*, February 17, 2021, https://www.datacenterknowledge.com/networks/how-hyperscale-cloud-platforms-are-reshaping-submarine-cable-industry.

[5] "The State of the Network" (TeleGeography, 2022), 5; Meta and Google for example funded the *Marea* cable. Christopher Mims, "Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power," *Wall Street Journal*, January 15, 2022, https://www.wsj.com/articles/google-amazon-meta-and-microsoft-weave-a-fiber-optic-web-of-power-11642222824.

[6] Bryan Clark, "Undersea Cables and the Future of Submarine Competition," *Bulletin of the Atomic Scientists* 72, no. 4 (2016): 234, https://doi.org/10.1080/00963402.2016.1195636; Michael Sechrist, "Cyberspace in Deep Water" (Harvard Kennedy School, 2010), https://www.belfercenter.org/sites/default/files/files/publication/PAE_final_draft_-_043010.pdf, 4–5; For an example see: Carol Rosenberg, "Navy Plans $40 Million Fiber-Optic Link to Guantánamo Base," *Miami Herald*, August 20, 2014, https://amp.miamiherald.com/article1941012.html.

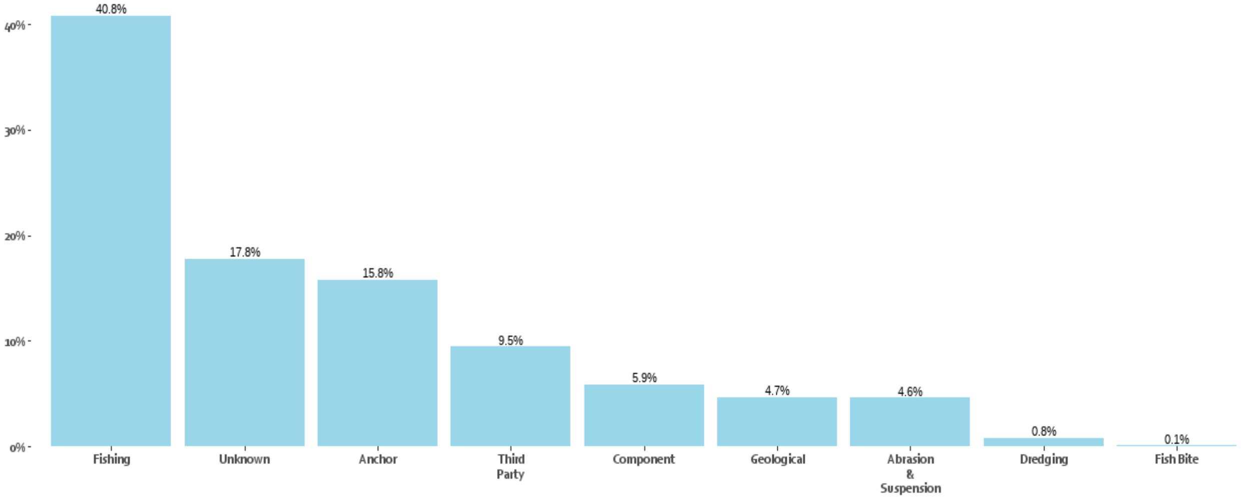
[7] See for example: David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *New York Times*, October 25, 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0. For the Federal Communications Commission Chairwoman's statement, see here: https://docs.fcc.gov/public/attachments/FCC-16-81A4.pdf.

[8] Valerie Coffey, "Sea Change: The Challenges Facing Submarine Optical Communications," *Optics and Photonics News* 25, no. 3 (2014): 28, https://doi.org/10.1364/OPN.25.3.000026.

[9] Carter et al., "Submarine Cables and the Oceans – Connecting the World," 43–47; Alan Mauldin, "Cable Breakage: When and How Cables Go down," *TeleGeography*, May 3, 2017, https://blog.telegeography.com/what-happens-when-submarine-cables-break.

by fishing and shipping activities – anchors and nets snagging the thin cables (see figure 1). Most such failures go unnoticed because the information is re-rerouted through other cables and most states are connected to several subsea cables (and land cables in the case of non-island nations). Tonga is one of the few exceptions, highlighting the consequences of a lack of redundancy: a volcanic eruption damaged the island nation's sole cable in 2022, taking most of Tonga offline until the cable was repaired a month later.[10] In contrast, Great Britain is connected to almost 60 cables, so a single cable failure would likely not cause any disruptions. Even if all transatlantic cables failed, Britain could still communicate with the U.S. via cables in the Pacific, albeit in a much reduced quality, provided that Britain is still connected to the European mainland.[11] Cables also typically do not run at their full capacity. On average, major cables have only used 18% of their total capacity since 2015 to create ample buffer to handle rerouted traffic after a cable fault.[12] Researchers have calculated that in the unlikely case that the U.S. loses its three highest-capacity cables simultaneously, it would still retain about 70% of its overall capacity: ca. 421 terabytes per second (TB/s) compared to 42 TB/s, the estimated actual bandwidth the U.S. needed in 2020.[13]

Figure 1: Cable Fault Causes Between 1959 and 2021[14]



While multiple cable connections usually provide security against cable faults, many cables often land at the same cable landing station. Eight cables for example land in the port of Marseille, a major connection

[10] Even redundancy might have limits: Four subsea cables connect the British island Jersey to France and Britain. Nevertheless, in 2016, a single ship dragged its anchor across three of island's four cables within five hours. *BBC News, "*Ship's Anchor Severs Jersey's Undersea Internet Cables," November 29, 2016, https://www.bbc.com/news/world-europe-jersey-38141230.

[11] See for example: Louise Matsakis, "What Happens If Russia Attacks Undersea Internet Cables," *Wired*, January 5, 2018, https://www.wired.com/story/russia-undersea-internet-cables/.

[12] "2022/2023 Industry Report" (Submarine Telecoms Forum,), https://subtelforum.com/products/submarine-telecoms-industry-report/, 40.

[13] Jonas Franken et al., "The Digital Divide in State Vulnerability to Submarine Communications Cable Failure," *International Journal of Critical Infrastructure Protection* 38 (2022): 8.

[14] Recreated based on the following article by the International Cable Protection Committee, which based their analysis on a database of reported cable damages kept by Global Marine Group, a subsea cable manufacturer. Mike Clare, "Submarine Cable Protection and the Environment" (International Cable Protection Committee (ICPC), 2021), https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/?id=2, 7.

point between Europe, the Middle East and Asia (see figure 2). This creates a risk of disruption to several cables at once. There are a number of geographical (and often geopolitical) chokepoints where cables are close to each other, creating the risk that "a single disaster could cause catastrophic loss of regional and global connectivity" according to a 2010 industry report.[15] The most critical chokepoint is Egypt, through which almost all internet traffic between Europe and Asia travels: between 17 and 30 percent of the global internet.[16] Cables usually bypass the congested Suez Canal and travel overland. That means that up to thirty percent of the world's internet enters Egypt via two stations on the Red Sea and leaves Egypt through a handful of stations in the Mediterranean.[17] Here, accidents or sabotage could have widespread consequences.[18]

Figure 2: Subsea Cable Landings in the Port of Marseille

Asia Africa Europe-1 (AAE-1)
Active since 2017
Length: 25.000 km
Landing Points in 19 countries

Atlas Offshore
Active since 2007
Length: 1.634 km
Landing Points in 2 countries

Hawk
Active since 2011
Length: 3.400 km
Landing Points in 3 countries

IMEWE
Active since 2010
Length: 12.091 km
Landing Points in 8 countries

Med Cable Network
Active since 2005
Length: 1.300 km
Landing Points in 2 countries

PEACE Cable
Active since 2022
Length: 21.500 km
Landing Points in 13 countries

SeaMeWe-4
Active since 2005
Length: 20.000 km
Landing Points in 14 countries

TE-North
Active since 2011
Length: 3.634 km
Landing Points in 4 countries

Planned Cables:

2Africa
Expected in 2023
Length: 45.000 km
Landing Points in 33 countries

Africa-1
Expected in 2024
Length: 10.000 km
Landing Points in 9 countries

Medusa
Expected in 2024
Length: 8.700 km
Landing Points in 9 countries

Such accidents have already occurred: in 2008, three submarine cables broke within thirty minutes of each other near Alexandria – possibly caused by an anchor – causing widespread disruption in the Middle East and Asia.[19] Notably, this outage also disrupted U.S. military operations in Iraq. According to a 2010 report, the U.S. Defense Information Systems Agency (DISA) relies on commercial infrastructure for 95 percent of U.S. strategic communication.[20] When service was interrupted in 2008, DISA experienced a 60 percent loss of capacity in the Gulf. Without a stable connection, the U.S. military had to reduce drone operations out of Iraq from a hundred a day to ten and the outage lasted for three days.[21] The submarine cable industry has long tried to circumvent the Egyptian chokepoint – both to add redundancy and to avoid high fees for crossing Egypt.[22] Egypt is however not the only problem zone. Any high

[15] Karl F. Rauscher, "Reliability of Global Undersea Cable Communications Infrastructure (ROGUCCI Report)" (IEEE Communications Society, 2010), 24.

[16] Paul Cochrane, "'Digital Suez': How the Internet Flows Through Egypt - and Why Google Could Change the Middle East," *Middle East Eye*, March 3, 2021, https://www.middleeasteye.net/news/google-egypt-suez-digital-internet-flow-change-middle-east; Nicole Starosielski, "Strangling the Internet," *Limn* 10 (2018), https://limn.it/articles/strangling-the-internet/.

[17] Doug Madory, "Outage in Egypt Impacted AWS, GCP and Azure Interregional Connectivity," *Kentik Blog*, June 14, 2022, https://www.kentik.com/blog/outage-in-egypt-impacted-aws-gcp-and-azure-interregional-connectivity/.

[18] Starosielski, "Strangling the Internet"; Sébastian Seibt, "Threat Looms of Russian Attack on Undersea Cables to Shut down West's Internet," *France 24*, March 23, 2022, https://www.france24.com/en/europe/20220323-threat-looms-of-russian-attack-on-undersea-cables-to-shut-down-west-s-internet.

[19] Kim Zetter, "Undersea Cables Cut; 14 Countries Lose Web," *Wired*, December 19, 2008, https://www.wired.com/2008/12/mediterranean-c/; James Regan, "UDPATE 3-Undersea Cable Breaks Cut Internet in Mideast, Asia," *Reuters*, December 20, 2008, https://www.reuters.com/article/internetNews/idUSTRE4BJ0FV20081220.

[20] Sechrist, "Cyberspace in Deep Water," 9.

[21] Sechrist, "Cyberspace in Deep Water," 9; Deb Riechmann, "Could Enemies Target Undersea Cables That Link the World?," *Associated Press*, March 30, 2018, https://apnews.com/article/moscow-north-america-ap-top-news-politics-russia-c2e7621bda224e2db2f8c654c9203a09.

[22] Madory, "Outage in Egypt impacted AWS, GCP and Azure interregional connectivity." A Google-led project aims to construct two cables that bypass Egypt entirely, connecting the Middle East, Europa and Asia by going through Israel and Jordan. See; Cochrane, "'Digital Suez': How the internet flows through Egypt - and why Google could change the Middle East"; Rory Jones and

concentration of routes or landing stations – e.g. in the Strait of Malacca – creates the risk of multiple disruptions at once.

Thus far, intentional damage of subsea cables has been very rare. Reported cases involve thefts and attempts to sell cables as scrap.[23] There has been no reported terrorist attack on the cable network and the last clear-cut incident of a military attack dates back to World War II.[24] Yet, the threat of attacks persists. Russia could disrupt transatlantic cables, "catastrophically" affecting the West's economy and "ways of living", a top UK defense official warned in 2017.[25] Western officials expect such attacks not necessarily at chokepoints where an attack might create the largest but also indiscriminate impact, but in deep waters, where repairs would be a lengthy process.[26] Most cable faults occur in shallow waters (less than 100m).[27] Faults in deep waters are rare; depth protects cables against their usual threats: anchors and nets.[28] A modern navy, however, could cut a cable in the middle of the Pacific, which would take some time to repair. When Tonga's sole cable went down in 2022, the nearest cable repair ship was 4.700 km away.[29] Nevertheless, for most countries, a single cut cable will have little impact given the redundancy built into the undersea network, leading most experts to conclude that cutting off a major country's internet access is unlikely.[30]

Spying on the undersea network has been a more frequent occurrence. In 1971, a U.S. submarine placed a tap on a telephone cable within Soviet territorial waters that connected a Soviet naval base to the Soviet Pacific Fleet headquarters. The tap remained undetected for nearly ten years and more Soviet cables were tapped, giving the U.S. a wealth of information described as the "crown jewels" by former intelligence officials.[31] Such operations are still possible today, but difficult. Copper telephone cables were easier to tap than today's fiber optic cables. The copper cable tapping devices wrapped around the cable and registered the electromagnetic signals through induction. This would no longer work with fiber optic cables, which rely on light to transfer data. Here, the cable needs to be opened to access the fibers.

Drew Fitzgerald, "Google Plans Fiber-Optic Network to Connect via Saudi Arabia and Israel for First Time," *Wall Street Journal*, November 23, 2020, https://www.wsj.com/articles/google-plans-fiber-optic-network-to-connect-via-saudi-arabia-and-israel-for-first-time-11606143590.

[23] Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis," *Catholic University Journal of Law and Technology* 24, no. 1 (2015); A well-known but unexplained incident occurred in 2013, when Egyptian authorities arrested three scuba divers for attempting to cut an undersea cable near Alexandria. See: Charles Arthur, "Undersea Internet Cables Off Egypt Disrupted as Navy Arrests Three," *The Guardian*, March 28, 2013, https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests.

[24] Nicole Starosielski, *The Undersea Network,* Sign, storage, transmission (Durham: Duke University Press, 2015), 80; Douglas R. Burnett, Robert C. Beckman and Tara Davenport, eds., *Submarine Cables*: *The Handbook of Law and Policy* (Leiden: Martinus Nijhoff Publishers, 2014), 283; There have been reports that Russian forces cut a submarine cable during the 2014 annexation of Crimea. This, however, does not seem to have been the case. While Russian forces did take over an internet exchange point in Simferopol, they did not cut a submarine cable because at the time Crimea was not connected to any submarine cables. The state-owned Russian company Rostelecom installed a submarine cable in April 2014 via the Kerch Strait. See: Sebastian Moss, "Fact Check: Russia Did Not Cut Submarine Cable When It Invaded Crimea," *Data Center Dynamics*, February 3, 2022, https://www.datacenterdynamics.com/en/news/fact-check-russia-did-not-cut-submarine-cable-when-it-invaded-crimea/; In the early Cold War, the U.S. government accused the Soviet fishing fleet of intentionally severing transatlantic cables, see: David F. Winkler, *Incidents at Sea: American Confrontation and Cooperation with Russia and China, 1945-2016* (Annapolis, Maryland: Naval Institute Press, 2017).

[25] Ben Farmer, "Russia Has Ability to 'Disrupt' Britain's Internet Access, Head of Armed Forces Warns," *The Telegraph*, December 14, 2017, https://www.telegraph.co.uk/news/2017/12/14/russia-has-ability-disrupt-britains-internet-access-head-armed/.

[26] See for example: Sanger and Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort."

[27] Clare, "Submarine Cable Protection and the Environment," 5.

[28] Coffey, "Sea Change: The Challenges Facing Submarine Optical Communications," 29.

[29] Jane Wakefield, "How Will Tonga's Broken Internet Cable Be Mended?," *BBC News*, January 24, 2022, https://www.bbc.com/news/technology-60069066.

[30] Matsakis, "What Happens If Russia Attacks Undersea Internet Cables"; Patrick J. Kiger, "Could an Attack on Undersea Cables Take down the Internet?," *HowStuffWorks*, January 4, 2018, https://computer.howstuffworks.com/could-attack-on-undersea-cables-disrupt-internet.htm.

[31] Sherry Sontag and Christopher Drew, *Blind Man's Bluff*: *The Untold Story of Cold War Submarine Espionage* (London: Arrow, 2000), 245. For more information, see pages 158-184, 231-258.

Then, a prism could be placed into the cable to split the light beam into two, creating a copy of the original light beam which continues on to its destination, while the other copy can be analyzed.[32] However, cable operators can detect any disruption to the light beam while the prism is inserted.[33] Doing this underwater is also difficult. After locating the cable, a section of it has to be brought up to a submarine or ship without damaging the remaining cable. The protective coating has to be removed without disrupting the cable's power supply or electrocuting oneself, the tap must be inserted without being detected and the cable placed back on the sea floor.[34] The U.S. submarine *Jimmy Carter* is rumored to have a floodable chamber to allow such an operation, but naval experts argue that there are easier ways to tap undersea cables – on land.[35]

Accessing a cable's information is easier where the cable makes landfall, making cable landing stations a key vulnerability.[36] Despite their importance, these stations are often unassuming buildings with little physical protection. In 2018, a journalist was able to walk into two stations in England unopposed and through unlocked doors.[37] Tapping cables is even easier with the cable operator's cooperation. In 2013, former National Security Agency (NSA) contractor Edward Snowden revealed that British intelligence (GCHQ) had tapped around 200 fiber-optic cables by placing "intercept probes" at cable landing stations in the UK, usually with agreements from the cable operating companies.[38] This allowed GCHQ to access, store, and analyze the data, and share it with the Five Eyes network (Australia, Canada, New Zealand, US, and the UK).[39] The Five Eyes cable tapping operation also involved many other countries, highlighting the possibilities of cooperating with both the cable operator and cable host country. Denmark for example has reportedly cooperated with the NSA to tap Danish cables since 1997, directed mainly at Russia and China.[40] This has deepened over the years and, with the help of NSA technicians, the Danes built a data processing center with a cable – paid for by the NSA – connected to the access

[32] Monica Blaylock, "Before PRISM, There Was Underwater Cable Tapping," *VICE*, August 1, 2013, https://www.vice.com/en/article/jppwek/before-prism-there-was-underwater-cable-tapping-5886b6e95908fb459f96b9d6.

[33] Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis," 104–5; Alternatively, the cable could be bent to such an angle that light leaks out but without disrupting significantly the signal, making detection more difficult. See: Blaylock, "Before PRISM, There Was Underwater Cable Tapping."

[34] See for example comment by Tim Stronge, vice-president of research at TeleGeography, a telecoms market research firm. James Griffiths, "The Global Internet Is Powered by Vast Undersea Cables. But They're Vulnerable," *CNN*, July 26, 2019, https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html.

[35] *Reuters, "*The Navy's Underwater Eavesdropper," July 19, 2013, https://www.reuters.com/article/idUS20767877420130719; *New York Times, "*New Nuclear Sub Is Said to Have Special Eavesdropping Ability," February 20, 2005, https://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html.

[36] Felicity L. Sherryn Groch, "A Dozen Undersea Cables Connect Australia to the Internet. What Happens If They Get Hacked – or Cut?," *Sydney Morning Herald*, November 5, 2022, https://www.smh.com.au/technology/the-internet-is-run-under-the-sea-not-in-the-cloud-what-happens-if-the-cables-get-hacked-or-snipped-20221025-p5bsov.html; Sechrist, "Cyberspace in Deep Water"; In 2010, WikiLeaks released a document compiled by the U.S. Department of Homeland Security that listed foreign infrastructure which if attacked would have a critical impact on U.S. security. These included dozens of cable landing stations around the world. Nicole Starosielski, "Warning: Do Not Dig': Negotiating the Visibility of Critical Infrastructures," *Journal of Visual Culture* 11, no. 1 (2012): 38, https://doi.org/10.1177/1470412911430465. For more information, see: https://en.wikipedia.org/wiki/Critical_Foreign_Dependencies_Initiative.

[37] The cable operators claimed that the reporter did not gain access to the station's "critical" equipment. Gabriel Pogrund, "Revealed: How Reporter Strolled into UK's 'Secure' Data-cable Sites," *The Sunday Times*, February 4, 2018, https://www.thetimes.co.uk/article/revealed-how-reporter-strolled-into-uks-secure-data-cable-sites-f6fx2hndv.

[38] These intercept probes could for example have been the aforementioned prisms. See: Olga Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping," *The Atlantic*, July 16, 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

[39] Julian Borger, "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications," *The Guardian*, June 21, 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. The other Five Eyes also participated in the tapping operations; New Zealand intelligence for example tapped the Southern Cross Cable, which connects New Zealand, Australia, Fiji, and the U.S.; Philip Dorling, "Edward Snowden Reveals Tapping of Major Australia-New Zealand Undersea Telecommunications Cable," *Sydney Morning Herald*, September 15, 2014, https://www.smh.com.au/technology/edward-snowden-reveals-tapping-of-major-australianew-zealand-undersea-telecommunications-cable-20140915-10h96v.html.

[40] Jens A. Bjørnager, "Et Pengeskab På Kastellet Har I Årtier Gemt På Et Dybt Fortroligt Dokument. Nu Er Hemmeligheden Brudt," *Berlingske*, September 13, 2020, https://www.berlingske.dk/samfund/et-pengeskab-paa-kastellet-har-i-aartier-gemt-paa-et-dybt-fortroligt.

point where the data is originally intercepted and copied.[41] All of this indicates that there are far easier options to access a subsea cable's information than to tap it on the sea floor a thousand meters beneath the surface. A cable landing station remains the most vulnerable access point, but access could also be gained through a cyberattack. In April 2022, U.S authorities disrupted such an attack on a Hawaiian subsea cable.[42] A cooperating cable manufacturer could also include 'backdoors' in a cable to facilitate espionage – a key concern in the U.S.-China confrontation over digital infrastructure.[43] Although secret high-risk underwater tapping missions are possible, the most pragmatic location for such an operation is still on land.

Does Russia have the capabilities to cut or tap subsea cables?

Manipulating submarine cables and the prevention thereof is often subsumed under the term 'seabed warfare', which, in short, refers to the placement and retrieval of items on the ocean floor. Here, seabed sensor systems that can detect and track enemy submarines play a key role. Advances in sensor technology coupled with complex unmanned underwater vehicles (UUVs) could threaten traditional submarine operations.[44] Seabed sensors, pipelines, subsea communication and power cables therefore place an emphasis on protecting one's undersea infrastructure. A challenge with such operations is reaching the seabed, which on average is about 3700 meters deep. The operating depth for most submarines is around 200 meters. Only a few states (approximately five) are capable of operating below 1000 meters and only the U.S., Russian and Chinese militaries reportedly have the equipment for depths between 3000 and 6000 meters.[45] For example, a weakness the French Government recognized in its 2022 seabed strategy was the need to develop UUVs that can operate at depths of 6000 meters, which a French military official described as 'the' strategic depth.[46] Russia has invested heavily in its undersea capabilities, resulting in the "most developed force for seabed warfare in the world" according to analysts.[47] Unlike other states, the Russian navy operates a fleet of submarines solely dedicated to seabed warfare.[48]

[41] Niels Fastrup, Henrik Moltke, and R. Querfeld, "Ny Afsløring: FE Masseindsamler Oplysninger Om Danskere Gennem Avanceret Spionsystem," *DR*, September 24, 2020, https://www.dr.dk/nyheder/indland/ny-afsloering-fe-masseindsamler-oplysninger-om-danskere-gennem-avanceret-spionsystem.

[42] Jamie Tarabay, "An Underwater Hack and the Digital Ripple Effects," *Bloomberg*, April 20, 2022, https://www.bloomberg.com/news/newsletters/2022-04-20/an-underwater-hack-and-the-digital-ripple-effects.

[43] James Stavridis, "China's Next Naval Target Is the Internet's Underwater Cables," *Bloomberg*, April 9, 2019, https://www.bloomberg.com/opinion/articles/2019-04-09/china-spying-the-internet-s-underwater-cables-are-next; For the U.S.-China confrontation on subsea cables, see: Jeremy Page, Kate O'keeffe, and Rob Taylor, "America's Undersea Battle with China for Control of the Global Internet Grid," *Wall Street Journal*, March 12, 2019, https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466.

[44] Bryan Clark, "The Emerging Era in Undersea Warfare" (CSBA, 2015), https://csbaonline.org/research/publications/undersea-warfare, 18; Andrew Reddie and Bethany Goldblum, "Unmanned Underwater Vehicle (UUV) Systems for Submarine Detection," *CSIS*, July 29, 2019, https://ontheradar.csis.org/issue-briefs/unmanned-underwater-vehicle-uuv-systems-for-submarine-detection-a-technology-primer/.

[45] James Kraska and Raul A. Pedrozo, *Disruptive Technology and the Law of Naval Warfare* (New York NY: Oxford University Press, 2022), 169; John Irish, "France to Dive Deeper for Undersea Security After Nord Stream Attacks," *Reuters*, October 11, 2022, https://www.reuters.com/world/europe/france-dive-deeper-undersea-security-after-nord-stream-attacks-2022-10-11/.

[46] Charlotte Le Breton and Hugo Decis, "France's Deep Dive into Seabed Warfare," *IISS*, February 25, 2022, https://www.iiss.org/blogs/military-balance/2022/02/frances-deep-dive-into-seabed-warfare; Irish, "France to dive deeper for undersea security after Nord Stream attacks."

[47] Kathleen H. Hicks and Andrew Metrick, "Contested Seas: Maritime Domain Awareness in Northern Europe" (CSIS, 2018), https://www.csis.org/programs/international-security-program/global-threats-and-regional-stability/contested-seas, 7.

[48] The U.S. submarine *Jimmy Carter* is a multi-purpose platform, not just a spy submarine. H. I. Sutton, "Russia's Growing Secret Submarine Fleet Key to Moscow's Undersea Future," *USNI News*, November 30, 2021, https://news.usni.org/2021/11/30/russia-growing-secret-submarine-fleet-key-to-moscows-undersea-future.

Within the Russian armed forces, analysts associate seabed warfare with the Main Directorate for Deep Sea Research (GUGI), possibly the submarine intelligence service. Separate from the other military branches, GUGI reports directly to the Ministry of Defense.[49] GUGI operates a number of surface vessels, submarines and deep submergence vehicles (DSVs) crewed by elite 'hydronauts', who are reportedly among the top earners in the Russian military.[50] GUGI's best-known ship is the *Yantar*, (officially) an oceanographic research ship that entered service in 2015 and triggered initial reports about potential cable cutting during her journey to the U.S. in 2015.[51] The ship carries two crewed DSVs capable of diving up to 6000 meters, which is sufficient to access 97% of the world's seabeds.[52] They are equipped with robotic arms to manipulate items on the seafloor. The Russian Federal Assembly's newspaper noted that the *Yantar* is equipped with "deep-sea-tracking" devices and equipment "for connecting to top-secret communication cables".[53] U.S. officials believe that *Yantar's* DSVs are capable of cutting cables.[54] *Yantar* itself is equipped with thrusters that allow her to hover in position to operate remote-operated vehicles.[55] She has hovered above submarine cables for example in the Mediterranean in 2016 and off the Irish coast in 2021 – sometimes with her AIS (Automated Identification System) switched off.[56] *Yantar* could be trying to map the exact location of some cables for future operations, which might tie in with other Russian activities: in 2019, Russian agents travelled to Ireland to determine the location of subsea cables and to assess whether they could be tapped, according to sources in the Irish security services.[57] There has been no evidence that *Yantar* has manipulated any cable and its exact missions remain unknown.[58]

Even fewer details are available about GUGI's submarine force. In 2016, the nuclear-powered BS-64 Podmoskovye submarine entered service – for the second time.[59] Between 1986 and 1999, the submarine, then the K-64, served as a ballistic missile submarine in the Soviet Union, then in the Russian navy.[60] In 1999, she was sent to a construction yard, where over the course of 16 years she was

[49] Michael Kofman, "Fire Aboard as-31 Losharik: Brief Overview," *Russia Military Analysis (Blog)*, July 3, 2019, https://russianmilitaryanalysis.wordpress.com/2019/07/03/fire-aboard-as-31-losharik-brief-overview/.

[50] Kathleen H. Hicks et al., "Undersea Warfare in Northern Europe" (CSIS, 2016), https://www.csis.org/analysis/undersea-warfare-northern-europe, 12.

[51] Sanger and Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort."

[52] "Stratégie Ministérielle De Maîtrise Des Fonds Marins" (Ministère des Armées, 2022), https://www.defense.gouv.fr/actualites/armees-se-dotent-dune-strategie-ministerielle-maitrise-fonds-marins, 34.

[53] Alexander Andreev, "Корабль Спецназначения &laquo;Янтарь&raquo; Вошёл В Средиземное Море [Special Purpose Ship "Yantar" Entered the Mediterranean Sea]," *Parlamentskaya Gazeta*, October 8, 2017, https://www.pnp.ru/politics/korabl-specnaznacheniya-yantar-voshyol-v-sredizemnoe-more.html.

[54] Bill Gertz, "U.S. Shadowing Russian Ship in Atlantic Near Nuclear Submarine Areas," *Washington Free Beacon*, September 3, 2015, https://freebeacon.com/national-security/u-s-shadowing-russian-ship-in-atlantic-near-nuclear-submarine-areas/; Sanger and Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort."

[55] H. I. Sutton, "Russian Ship Loitering Near Undersea Cables," *Covert Shores (Blog)*, September 13, 2017, http://www.hisutton.com/Yantar.html.

[56] H. I. Sutton, "Suspected Internet Cable Spy Ship Operating in Americas for over a Month," *Forbes*, December 1, 2019, https://www.forbes.com/sites/hisutton/2019/12/01/suspected-internet-cable-spy-ship-operating-in-americas/?sh=72f6c0d032ae.

[57] John Mooney, "Russian Agents Plunge to New Ocean Depths in Ireland to Crack Transatlantic Cables," *The Sunday Times*, February 16, 2020, https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz.

[58] Yantar for example also helped locate Russian fighter jets that crashed in the Mediterranean 2016 and was involved in the search for the Argentine submarine ARA San Juan in 2017.

[59] *TASS, "*Атомная Субмарина "Подмосковье" Передана ВМФ России После Модернизации [The Nuclear Submarine "Podmoskovje" Was Handed over to the Russian Navy After Modernization]," December 26, 2016, https://tass.ru/armiya-i-opk/3907698.

[60] Evgeny Saltykov, "В Сети Появилось Впечатляющее Видео Испытаний Атомной Подлодки Спецназначения "Подмосковье" [Impressive Video of Testing of Nuclear Submarine "Podmoskovie" Appeared on the Web]," *Vesti*, November 10, 2016, https://www.vesti.ru/article/1575428.

transformed into the BS-64 special-purpose submarine to be operated on behalf of GUGI.[61] Engineers replaced the K-64's missile tubes with a special compartment to enable the docking of small submarines.[62] On its back, the BS-64 can carry a deep-sea rescue vehicle (DSRV) capable of operating at depths of up to 700 meters. This DSRV could be used to rescue stricken submarine crews but is also equipped with manipulator arms that could interfere with objects on the seafloor.[63] Its distinguishing feature however, is the 70-meter-long nuclear-powered *Losharik* submarine that the BS-64 can carry under her hull.[64] The unarmed *Losharik* can dive to extreme depths – up to 6000 meters – with a crew of 25 hydronauts. Equipped with hydraulic arms and skids to sit on the seabed, she could place sensors, recover weapon systems or cut cables.[65] Besides the two small submarines, the BS-64 also features a hangar for the unarmed and deep-diving *Harpsichord* UUV. BS-64 appears to have become a host submarine, allowing its deep-diving submarines to operate much further from the shore. According to Russian media reports, her missions include deactivating U.S. wiretaps and submarine-tracking systems on the seabed, but little is known about her current missions.[66]

The BS-64 is not the only Russian submarine connected to GUGI's seabed operations. In July 2022, a possibly even stranger submarine entered service. Operated on behalf of GUGI, the 184-meter-long nuclear-powered *Belgorod* is the largest submarine in the world.[67] The submarine is similar to the BS-64 in both history and capabilities. Laid down in 1992 as a cruise-missile submarine, construction was suspended several times and she was close to being sold, before construction resumed and the *Belgorod* was finished as a 'special-mission' submarine.[68] Instead of cruise missiles, the *Belgorod* – like the BS-64 – can carry a DSRV on her back and a *Losharik*-type submarine under her hull as well as the *Harpsichord* UUV, broadly giving her the same range of missions as the BS-64. Unlike the BS-64, however, the *Belgorod* has also reportedly been modified to carry six of the nuclear-powered and nuclear-armed

[61] H. I. Sutton, "Russia's Unusual Mother Submarine for Spy Missions on the Sea Floor," *Covert Shores (Blog)*, November 19, 2021, http://www.hisutton.com/Russian-Spy-Submarine-BS-64.html; Anton Mardasov, "АПЛ «Подмосковье»: Подводный Разведчик Готовится К Охоте [Submarine "Podmoskovje": An Underwater Reconnaissance Submarine Prepares for the Hunt]," *Svobodnaya Pressa*, August 12, 2015, https://svpressa.ru/war21/article/129445/.

[62] Dmitry Yurov, "Оказались В Погружении: На Что Способны Российские Подводные Беспилотники [Turned Out to Be Submerged: What Russian Underwater Drones Can Do]," *Izvestia*, November 29, 2018, https://iz.ru/817694/dmitrii-iurov/okazalis-v-pogruzhenii-na-chto-sposobny-rossiiskie-podvodnye-bespilotniki; Thomas Nilsen, "Deep-Sea Sub Carrier on Test-Voyage in White Sea," *The Barents Observer*, October 23, 2016, https://thebarentsobserver.com/en/security/2016/10/deep-sea-sub-carrier-test-voyage-white-sea.

[63] DSRVs have historically been dual-use: the U.S. navy initiated its DSRV program both be able to rescue submariners but also to attain the capability to for example retrieve sunken Soviet missiles from the seafloor. Sontag and Drew, *Blind man's bluff*, 46–64; Norman Polmar and Kenneth J. Moore, *Cold War Submarines*: *The Design and Construction of U.S. And Soviet Submarines* (Washington D.C.: Potomac Books Inc., 2004), 207–8.

[64] In 2019, a fire aboard the *Losharik* killed fourteen hydronauts and damaged the submarine. She is undergoing repairs and will likely return to service. *Belgorod* can also carry the older *Paltus* class submarines that are smaller but can fulfil similar roles and potentially the *Kashalot* submarine AS-15. For more information see: H. I. Sutton, "Russia's New Super Submarine, Belgorod (K-329)," *Covert Shores (Blog)*, June 29, 2021, http://www.hisutton.com/Belgorod-Class-Submarine.html; Bruce Jones, "Russia Readies Kashalot Submarine for Belgorod Role," *Janes*, April 1, 2021, https://www.janes.com/defence-news/news-detail/russia-readies-kashalot-submarine-for-belgorod-role; James Glanz and Thomas Nilsen, "The Deadly Losharik Submarine Fire and Russia's Secret Undersea Agenda," *New York Times*, April 20, 2020, https://www.nytimes.com/2020/04/20/world/europe/russian-submarine-fire-losharik.html.

[65] Kofman, "Fire aboard AS-31 Losharik: Brief Overview"; H. I. Sutton, "How Russian Spy Submarines Can Interfere with Undersea Internet Cables," *Forbes*, August 19, 2020, https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/?sh=3c38ed503b04.

[66] Mardasov, "АПЛ «Подмосковье»: подводный разведчик готовится к охоте [Submarine "Podmoskovje": an underwater reconnaissance submarine prepares for the hunt]"; Yurov, "Оказались в погружении: на что способны российские подводные беспилотники [Turned out to be submerged: what Russian underwater drones can do]."

[67] Sutton, "Russia's New Super Submarine, Belgorod (K-329)."

[68] *Izvestia, "*«Посейдон» В Лодке: Субмарину Готовят К Испытаниям Ядерных Роботов ("Poseidon" in a Boat: Submarine Being Prepared for Nuclear Robot Tests)," February 11, 2021, https://iz.ru/1123160/anton-lavrov-aleksei-ramm/poseidon-v-lodke-submarinu-gotoviat-k-ispytaniiam-iadernykh-robotov.

Poseidon torpedoes that are still under development.[69] Another mission associated with *Belgorod* is the installation of the (possibly nuclear-powered) underwater sonar tracking system 'Harmony' that the Russian military is reportedly building under the Arctic shelf.[70]

Consequently, few doubt that Russia has the capability to interfere with subsea cables, but questions remain about the exact nature of the Russian activity near undersea cables, which has reached unprecedented levels in 2017 according to the commander of NATO's submarine forces.[71] For one, the focus of GUGI's activities might lie on tracking enemy submarines rather than on internet cables. For example, according to sources in the Pentagon, *Yantar's* mission in her 2015 trip to the U.S. was to gather intelligence on underwater sensors and the Department of Defense's Information Network (DODIN).[72] A later story on the same journey which cited U.S. government sources made no mention of sensors or DODIN, referring instead to the threat to subsea internet cables.[73] Assuming that internet infrastructure were the target, how large is the threat?

Currently, 17 cables connect Europe to North America, accounting for 75% of Europe's interregional bandwidth. [74] Two more are set to be added in 2023 and 2024. It is unclear how many of these cables would need to be cut in order to overwhelm the built-in redundancy and disrupt or collapse transatlantic communication. [75] It seems that a carefully planned attack on several cables simultaneously would be necessary to achieve a significant impact. This would require Russia to locate the cables in the Atlantic, which are not mapped as precisely as cables near the shore, and carry out multiple attacks at different locations without being noticed. [76] Alternatively, a former deputy undersecretary of the US navy warned that the clustered cable landing stations near New Jersey and New York could be an easy target, since nearly all transatlantic cables come ashore there.[77] While cutting all transatlantic cables would cause severe disruptions to the global internet and affect neutral countries as well as Russia itself, most experts consider such an attack unlikely. However, Western warnings about the potential severity of a Russian attack have been stark, leading to questions about the potential impact of such an attack.[78]

[69] For information on Poseidon see:H. I. Sutton, "Poseidon Torpedo," *Covert Shores (Blog)*, February 22, 2019, http://www.hisutton.com/Poseidon_Torpedo.html; Felix Lemmer, "Poseidon," Security Tech Brief (Hertie School Centre for International Security, 2022), https://www.hertie-school.org/en/international-security/outreach/security-tech-brief.

[70] H. I. Sutton, "Analysis -Russia Seeks Submarine Advantage in Arctic," *Covert Shores (Blog)*, September 20, 2016, http://www.hisutton.com/Analysis%20-Russia%20seeks%20submarine%20advantage%20in%20Arctic.html; Alexei Ramm and Dmitry Boltenkov, "Мера Сил: Зачем России Нужна Самая Длинная В Мире Субмарина," *Izvestia*, February 13, 2021, https://iz.ru/1124101/dmitrii-boltenkov-aleksei-ramm/mera-sil-zachem-rossii-nuzhna-samaia-dlinnaia-v-mire-submarina.

[71] Michael Birnbaum, "Russian Submarines Are Prowling Around Vital Undersea Cables. It's Making NATO Nervous," *Washington Post*, December 23, 2017, http://wapo.st/2BCRwe0?tid=ss_tw.

[72] Gertz, "U.S. Shadowing Russian Ship in Atlantic Near Nuclear Submarine Areas."

[73] Steffan Watkins, "We Will Bury You (In Data) - Russian Navy Yantar Backgrounder and Summer 2016 Trip Report," *Vessel of Interest (Blog)*, November 3, 2018, https://www.vesselofinterest.com/2018/11/we-will-bury-you-in-data-russian-navy.html.

[74] Alan Mauldin, "Cutting Off Europe? A Look at How the Continent Connects to the World," *TeleGeography*, October 13, 2022, https://blog.telegeography.com/cutting-off-europe-a-look-at-how-the-continent-connects-to-the-world.

[75] A former technical director of France's DGSE foreign intelligence agency suggested at least 10 cut cables for a widespread internet blackout. Peter O'Brien, "France Tightens Subsea Cable Security Amid Growing Fear of Sabotage," *POLITICO*, October 13, 2022, https://www.politico.eu/article/france-tighten-subsea-cable-security-fear-sabotage-pipeline-gas-leak/.

[76] For an analysis of a potential attack, see: Christian Bueger, Tobias Liebetrau, and Jonas Franken, "Security threats to undersea communications cables and infrastructure" (European Parliament: Sub-committee on Security and Defence (SEDE), 2022), https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf, 27–35.

[77] Robert Martinage, "Under the Sea," *Foreign Affairs*, October 26, 2015, https://www.foreignaffairs.com/articles/commons/under-sea.

[78] Garret Hinck, "Evaluating the Russian Threat to Undersea Cables," *Lawfare*, March 5, 2018, https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

Instead of launching an all-out attack on subsea cables, which would likely only be plausible in the event of all-out war, Russia could target isolated areas with little redundancy in order to divert resources and keep its adversaries on their toes. In Europe, Iceland, the Faroe Islands, and the Azores are easier targets than the UK.[79] Outlying territories such as French Polynesia, the U.S. Northern Marianas or the Cayman Islands have almost no redundancy but are of little strategic importance. In any case, the UK's top military official warned in January 2022 that any overt attack would be considered an act of war.[80] Importantly, cable sabotage is relatively easy to conceal. Cables break regularly, and an expensive high-tech submersible is not always necessary; a fishing trawler "accidentally" anchoring in the wrong spot can do the job, and such incidents are common enough. In April 2021, for example, 4.3 km of cable (weighing about 9 tons) from a Norwegian ocean observatory disappeared off Svalbard. It was found six months later, 11 km out of position. While the cable was used for research purposes, Norwegian defense authorities filtered out "sensitive" data, including the position of submarines.[81] Using AIS data, a Norwegian broadcaster found that a Russian fishing trawler had crossed over the cable and sailed to where the cable was later found.[82] However, the police dropped their enquiry, which included interviews with Russian trawler crews, due to lack of evidence, leaving the incident unexplained.[83] This shows how difficult it is to prove sabotage and increases the danger of maritime hybrid warfare, which former NATO commander James Stavridis warned about in an influential 2017 think tank report on subsea cables written by Rishi Sunak.[84]

Ultimately, however, little is known about what role cable sabotage or tapping plays in Russian military strategy. Russian "research" ships might be mapping the precise location of subsea cables for future operations when they sail near cables. This would be expected behavior for such ships, according to a former British ambassador.[85] They might also be using unmarked ships as well. In 2021, the Irish coast guard discovered a Cape Verde-flagged vessel with its AIS switched off, which Irish defense forces suspected of launching a submersible near a subsea cable.[86] At any rate, the Russian military seems aware of what the West thinks their ships might be doing. When a cable fault disrupted the Shetland's internet access shortly after explosions damaged the Nord Stream pipelines, suspicion quickly fell on

[79] See for example Figure 4: Franken et al., "The digital divide in state vulnerability to submarine communications cable failure," 9.

[80] Seibt, "Threat looms of Russian attack on undersea cables to shut down West's internet"; *The Guardian, "*UK Military Chief Warns of Russian Threat to Vital Undersea Cables," January 8, 2022, https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables.

[81] Nina Berglund, "Surveillance Cables Mysteriously Cut," *Norway's News in English*, November 7, 2021, https://www.newsinenglish.no/2021/11/07/surveillance-cables-mysteriously-cut/.

[82] Benjamin Fredriksen et al., "Kabelmysteriene," *NRK*, June 26, 2022, https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-for-brudd-1.16007084.

[83] See the Norwegian's police statement here: https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2022/06/30/henlegger-kabelbrudd/

[84] Rishi Sunak, "Undersea Cables" (Policy Exchange, 2017), https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/, 10.

[85] Birnbaum, "Russian submarines are prowling around vital undersea cables. It's making NATO nervous."

[86] John Mooney, "Navy Called in as Russians Suspected of Targeting Undersea Internet Cable," *The Sunday Times*, August 15, 2021, https://www.thetimes.co.uk/article/navy-called-in-as-russians-suspected-of-targeting-undersea-internet-cable-jztg8t6lx.

Russia.[87] While a UK-registered trawler appears to have been the cause, a Russian 'research' vessel changed course to pass the Shetlands a day after the cable fault.[88]

There are still uncertainties about the nature of the potential threat from Russia's activities near undersea cables. It is not clear if Russia is searching for submarines, sensors, pipelines, internet cables, or a combination of these. Do Western military officials expect a coordinated Russian attack on several subsea cables, crippling transatlantic communications (and thus affecting the global internet, not least Russia itself), although most experts think this unlikely? Similarly, it is unclear if officials believe that Russia is likely to engage in deep-sea cable tapping, despite the feasibility of such an operation being questionable and the more practical location for eavesdropping being on land. However, it is clear that Russia has invested heavily in its submarine force in recent years, with the navy receiving the largest share of the budget under the 2010 Russian 'State Armament Program'.[89] Submarine construction reached record levels in 2021, and several new submarines were commissioned in 2022, including the purpose-built *Belgorod*.[90] A new oceanographic research ship also completed sea trials at the end of 2022. While the focus of these activities is uncertain, it is clear that the Russian leadership values the capabilities that these advanced ships and submarines offer, and the potential threat to the West's underwater infrastructure must be taken seriously.

[87] Severin Carrell, "Shetland Loses Telephone and Internet Services After Subsea Cable Cut," *The Guardian*, October 20, 2022, https://www.theguardian.com/uk-news/2022/oct/20/shetland-loses-telephone-internet-services-subsea-cable-damaged.

[88] *Plenty of Ships (Blog), "*Russian Intelligence Ship Likely to Increase UK Tension Around Cable Cutting in the North Sea," October 21, 2022, https://plentyofships.blogspot.com/2022/10/russian-intelligence-ship-likely-to.html.

[89] See for example: "Chapter II: The Balance of Capabilities in the Subsurface Domain," *Whitehall Papers* 100, no. 1 (2022): 15–18, https://doi.org/10.1080/02681307.2022.2030966; This share declined in the 2027 'State Armament Program'. See: Richard Connolly and Mathieu Boulègue, *Russia's New State Armament Programme*: *Implications for the Russian Armed Forces and Military Capabilities to 2027,* Research paper (London: Chatham House, 2018), 20.

[90] Thomas Nilsen, "Russia's Nuclear Submarine Construction Reaches Post-Soviet High," *The Barents Observer*, January 6, 2022, https://thebarentsobserver.com/en/security/2022/01/bustling-sevmash-shipyard-enters-new-year-post-soviet-high-construction-peak.