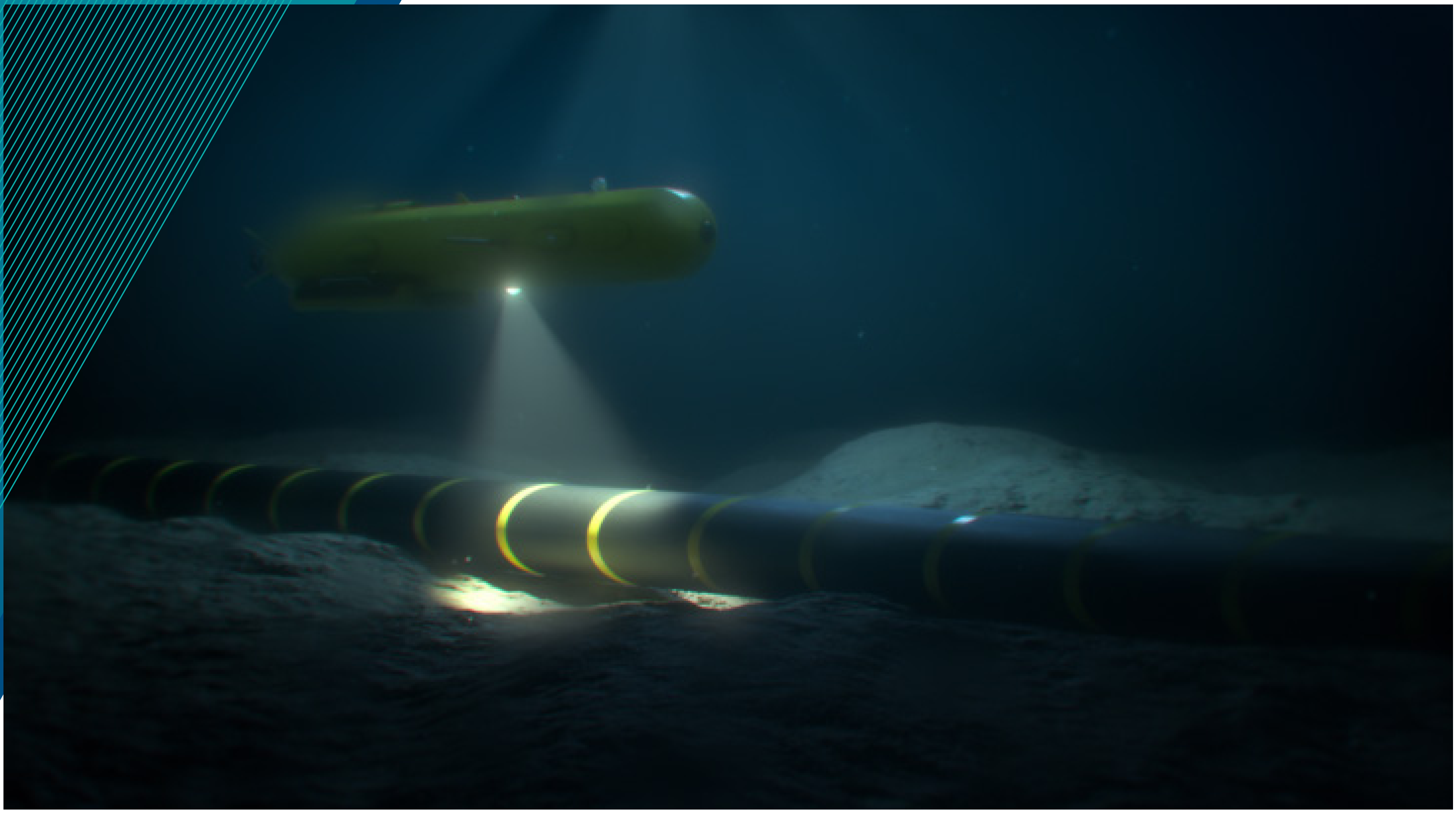
No 495 / January 2023

Facts & Findings

KONRAD ADENAUER STIFTUNG



Undersea cables as critical infrastructure and geopolitical power tool

Why undersea cables must be better protected

Ferdinand Alexander Gehringer

- Undersea cables are critical infrastructure and must be protected from sabotage and espionage.
- US Big Tech companies, the Russian Federation, and the People's Republic of China have recognised the geopolitical significance of the undersea cable infrastructure and either built up dependencies or, in the case of Russia, kept them to a minimum.
- For far too long, the European Union has underestimated the importance of this infrastructure and is only now beginning to take action.
- Physical and digital protection of undersea cables require equally strong consideration.
- Physical protection of the critical infrastructure in particular needs coordinated and skill-specific action.

#KAS4 SECURITY

www.kas.de

Table of Contents

For the most part, data is transported across the oceans via undersea cables. Finance transactions totalling over 10 billion US dollars are completed via these cables on a daily basis.[1] Around 95 per cent of international data transfer runs through this underwater cable infrastructure before being distributed further overland at various landing points.[2,3] Estimates suggest the amount of data running through the Atlantic, for instance, doubles in volume every two years.[4] And the trend is rising. Digital transformation, with increasing numbers of new internet users every day and new digital processes (like cloud products, streaming services, social media, etc.) is driving this trend.

Undersea cables are critical infrastructure as there is no current alternative for data transmission

In 2022, a total of 530 undersea cables were actively being used or planned. The cable network deep beneath the oceans now extends to a total length of more than 1.3 million kilometres.[5] The generally arm-thick cables now primarily made out of fibreglass (rather than copper wire as in the past), constitute a worldwide network and a trading route for all kinds of data conveyed by light impulses.

Special protection must be provided for critical underwater infrastructure.

There is currently no alternative to rapid intercontinental transmission of large volumes of data via undersea cable. Some data transmission does occur via satellite, but only where no terrestrial options exist and construction of cable infrastructure is out of the question. The higher packet runtimes necessitated by longer distances to satellites, higher costs and greater susceptibility to failure of satellite transmission – at this point – all count against reliance on this method as an alternative.[6] This is why protection of undersea cable infrastructure is essential to ensure ongoing data transmission in the future.

Risk scenarios like sabotage and espionage are on the rise

There are many different kinds of threats to critical underwater infrastructure. Undersea earthquakes, tornados or dislodged cables are realistic scenarios due to natural causes and can only be prevented with difficulty – by strengthening the cable sheath. For instance, a sea quake off the coast of Taiwan in 2006 led to a cable break and, amongst other consequences, left banks and investment firms in the region cut off for a time from international

Data and communications espionage has been an issue for years.

trade.[7] The most common causes of damage to undersea cables, however, stem from fishery activity (38 per cent) and shipping traffic. Many cables (25 per cent) have been destroyed in the past by the anchors of large vessels.[8]

But these are by no means the only potential threats. Events this summer surrounding the gas pipelines of Nordstream I and II in the Baltic Sea have shown that underwater infrastructure is not immune to manipulative forces. Destruction by explosive devices or other targeted attacks on undersea cables (by submarines, underwater robots, or drones) cannot be ruled out either.

Data espionage is an additional threat and by no means a new phenomenon. The US Secret Service, for instance, monitored the undersea cable of the Soviet Union during the Cold War of the 1980s as part of its “Operation Ivy Bells”. Bugging devices used on Russian undersea cables provided US marines with critical information about the activities, processes, and technologies of the Soviet navy.[9]

Access to data transfer via the landing points of undersea cables is possible with minimal outlay. For instance, the British secret service GCHQ monitors global communication traffic via the Cypriot “Yeroskipos Submarine Cable Station”. Officially, such surveillance is conducted for counter-terrorism purposes. The revelations of Edward Snowden about the activities of the NSA from 2012 to 2014, where top European politicians were bugged, indicate, however, that the full truth is not always disclosed. The US Secret Service, for instance, intercepted communications via its Sandagergardan surveillance station in Denmark during that period. There are currently four landing points in Germany (Sylt, Rostock, Markgrafenheide, Puttgarden), where a total of eight cables meet the mainland.

Data infrastructure as the target of hybrid warfare

A total outage of all data traffic is not a realistic prospect at this time. Damage to one cable will not lead to a total breakdown in data transmission,[10] provided alternative options within the network are available. When individual cable connections are destroyed, the data will “search” for another functioning route through the cable infrastructure (redundancies), which may lead to a delay in data reaching its target. But the risk of overloading the network increases when this happens.

Theoretically a simultaneous physical attack on several undersea cables is possible, but as well as knowing the exact location of the cable route, this would require extensive preparation and a huge amount of resources. However, since the cable course and location of landing points is freely available for all to see (downloadable via the internet and marked on marine maps), critical undersea infrastructure can be leveraged during modern conflict scenarios. As part of a hybrid harassment strategy, aggressors will typically combine classic military operations with economic pressure, attacks on critical infrastructure, cyberattacks, and disinformation via (social) media. Attacks on undersea cables can therefore form part of an intimidation strategy and an overall process of delaying tactics.

Russia and the USA have destructive military equipment and China is expanding its capabilities

Military arms race between the US and China.

Undersea cables may become a military target at any time. For instance, the naval war fleet of the Russian Federation has two nuclear-powered submarines. They can be used as the motherships of smaller U-boats for espionage and sabotage purposes as part of the process of conducting seabed warfare. Apart from recovering crashed aircraft and installing wire-tapping sensors, the nuclear-powered U-boat “Losharik” is also suitable for manipulation or shelling of undersea cables.[11]

Furthermore, the “Yantar“ research ship run by the Department of Deep Sea Research within the Russian Defence Ministry is equipped with two unmanned U-boats that can penetrate to a depth of 6,000 metres below sea and are fitted with hydraulic tentacles. When combined with underwater robots or drones, they can be used not just for reconnaissance missions but are also capable of destroying underwater cable infrastructure in insufficiently or poorly monitored areas (like parts of the Atlantic). The US navy, as part of its “Cognitive Lethal Autonomous Weapons Systems” (CLAWS) project, is currently developing autonomous underwater weapon systems. The armed “robotic U-boats” are designed to be controlled by artificial intelligence and could potentially act without any human supervision – including the performance of kinetic effects (destruction of objects).

The People’s Republic of China is going down the same track. Three years ago, China unveiled its first unmanned underwater vehicle (UUV) “HSU001”.[12] At the same time, the People’s Republic announced that in the ensuing years it would focus on using high-tech UUVs and artificial intelligence to address the military deficits it had identified in its own underwater warfare capability.

Big Tech and China will soon have data control

Europe will soon be entirely dependent on data infrastructure from US tech companies and China.

Other ways of exerting influence also exist in other areas. While in the past undersea cables were primarily planned, built, and operated by consortiums consisting of telecommunication companies, such as Orange, British Telecom, Alcatell and Norddeutsche Seekabelwerke, Big Tech companies like Alphabet, Meta, Amazon, Apple, and Huawei are now converging on the market. For telecommunication companies, the cost of building and maintaining such infrastructure has become too high. Big Tech companies on the other hand, are constantly investing in new cable networks or replacing old systems with faster, more high-performing cables as part of their goal to expand their bandwidth, initially to support their own products and services.[13] For instance, Alphabet and Amazon, in particular, are increasing the bandwidth for their own cloud services and to support their huge data centres. Forecasts indicate that by 2027, tech giants in the US will own as much as 80 per cent of the infrastructure themselves.

Alphabet currently owns four undersea cables, in the form of “Curie”, “Dunant”, “Equitano”, and “Grace Cooper”. The same company in conjunction with Meta is also planning two further undersea cables, “Echo” and “Bifrost”, due to be finished in 2023 and 2024 respectively.[14]

But the People’s Republic of China has well and truly entered the market, too, building its own undersea cable with Chinese telecom companies in 2017 to connect South East Asia and both the Middle and Far East with Western Europe.

The latest project of the People's Republic of China with the acronym "PEACE" (Pakistan East Africa Connecting Europe) forms part of the "Digital Silk Road" and has been operating since August of this year.[15] With a 15,000-kilometre-long undersea cable, Pakistan is now connected via the Horn of Africa, Red Sea, and Suez Canal to Western Europe (with Marseille as the landing point). At the same time, the project is also building a connection to East Africa (Somalia via Africa-1 to Kenya).[16]

With data transmission rates of 96 terabytes per second, it enables transmission of as much data per second as the amount required to stream 90,000 hours of Netflix.[17] As well as the economic reasons for constructing this cable, the infrastructure could connect the existing Chinese military base in Djibouti with future military strongholds of the People's Republic of China in South Asia (Pakistan) or the Gulf. For a long time now, the People's Republic has been toying with the idea of expanding its own military bases worldwide. Its intention to extend the "PEACE" project to include Singapore via the Maldives has already been announced.

More significantly, Chinese companies already supply the components of this infrastructure. In fact, a Chinese company by the name of Hengtong Optic-Electric is one of the biggest fibreglass manufacturers in the world.[18] Russia on the other hand keeps its dependency to a minimum, does not have key junctions on its own territory, and is only linked to the global data transmission network via four international undersea cables (one connection each to Finland and Georgia and two with Japan).[19] This manageable number of connections enables the Russian Federation to at least retain the possibility of controlling its own landing points and data traffic.

A similar tendency to evade potential foreign influence is discernible in Brazil. In June of last year "EllaLink", an undersea cable linking Brazil and Latin America to Europe (Portugal), was commissioned with a data transmission rate of 100 terabytes per second. It was built, according to the Brazilian government, in order to safeguard the neutrality of data traffic and avoid potential surveillance by the US Secret Service or data control by big US Tech companies.[20]

The geopolitical race cannot be ignored

The great powers have long recognised the geopolitical significance of underwater cables. Whoever controls the cable infrastructure can potentially track or even influence the flow of information. In 2020, US authorities warned against the construction of a direct cable between the US and Hong Kong.[21]

The US are aware of the risk of becoming dependent on China.

Five years ago, Google and Facebook were still intending to work with a subsidiary company of China Soft Power Holdings to link Los Angeles and Hong Kong via a high-capacity underwater cable. The Pacific Light Cable Network would be 12,800 kilometres long and cross under the Pacific Ocean. At a rate of about 120 terabytes per second, the link would enable transmissions of 80 million simultaneous, high-resolution video conferences between Los Angeles and Hong Kong.[22]

US authorities blocked the plan, justifying their rejection of it on the grounds that having Hong Kong as a landing point on Chinese territory would endanger the national security of the US, and millions of sensitive personal data of US citizens could potentially be intercepted by Chinese surveillance. The other section of the project between the US, the Philippines, and Taiwan, on the other hand, went ahead and is now operating.

The People's Republic of China obviously anticipates a potential attack scenario on Taiwan via underwater cable. Some proposed strategic goals were discovered on a Chinese platform, including access to the semiconductor industry of Taiwan via the underwater cable infrastructure. How realistic and serious such suggestions are within government circles is impossible to ascertain for sure.

High-speed cables determine data sovereignty

In the future – unless the US is prepared to accept some loss of control – who builds which components of the cable will be crucial to keeping the potential for interference by other nations as low as possible. The race for the highest data transmission rate is also likely to become increasingly important. Whoever builds the faster cables, thereby increasing the data transmission rate and actual capacity, will be able to transmit more data via their underwater cables and thus influence the flow of data. Data is always looking for the fastest possible route, irrespective of whether it runs via landing points in China, the US, or Russia.

Monitoring the infrastructure and transmitting encoded data

Physical and digital protection must be designed in tandem.

In view of this noticeable trend, underwater cables, as critical infrastructure, require particular protection – and demand an all-risk approach. In this context, all kinds of risks (e.g., natural hazards, technological threats, problematic dependencies, etc.) need to be taken into consideration. For underwater cables, this means using satellite images and underwater monitoring to produce comprehensive locational imagery, along with patrols to prevent any dangerous incursions, manipulation attempts, or espionage attacks, so that any attackers can be identified and attributed. Particular attention must be devoted to the landing points involved. If necessary, attacks could also be repelled by underwater robots or underwater drones. In order for this to be effective, (individual) international initiatives need to be better coordinated as part of a concerted approach.

In February, France made its strategy for underwater warfare public.[23] Part of it is to extend the underwater capabilities of the French navy to a depth of 6,000 metres, which is just far enough to reach the average depth of the oceans.[24] In March, the British navy announced that from 2024 its Multi Role Ocean Surveillance Ship, equipped with a remote-controlled submersible and a range of different sensors, would undertake surveillance of British waters and sections of international waters. Telecom Italia Sparkle announced in the summer of 2022 that it would be working with the Italian navy on reconnaissance and surveillance in the areas surrounding its Sparkle cable.[25] The German government has so far taken no action; and no European institution responsible for protection and surveillance has been established to date.[26] In June 2022, the European Union did publish the study *Security threats to undersea communications cables and infrastructure – consequences for the EU*,[27] which addressed the need to protect underwater cables. The European Commission suggested the formation of a coordination group for cable defence purposes. It would also be conceivable to set up an Anti-Submarine-Warfare (ASW) group within the NATO alliance to protect such critical infrastructure. The Joint Force Command – Norfolk (JFC-NF) of NATO, formed in 2018 to protect transportation and communication channels, is only a start in the right direction.[28]

The German police and navy also need to boost their own capacity to protect this vital infrastructure. As well as police helicopters, this includes doubling the number of German naval U-boats from six to twelve, adding fleet service vessels (small espionage ships with electronic listening devices), autonomous underwater vehicles like the "Seekatze", and expanding the acoustic assessment system of the Bundeswehr (German armed forces). The Territorial Command Squad could be assigned a special role within its homeland protection function of safeguarding critical infrastructure in Germany. In addition, back-up solutions need to be found. For instance, satellite technology could be deployed to ensure that data transmission is still possible in an emergency. Furthermore, there are currently only three repair ships available for maintenance and repair work on the undersea cables in the Atlantic,[29] which is woefully inadequate.

Acoustic sensor systems (Distributed Acoustic Sensoring, DAS), attached to the cables have the ability to turn them into a type of microphone. The sensor elements enable interception of sounds and frequencies in the vicinity of the cables and thus give an indication of any unusual activity in the area. In regulatory terms, there is a need at the national level for special protection and maintenance obligations for the operators of cables and a clear allocation of skill-specific tasks and responsibilities. At the international level, underwater cable infrastructure does not have any protection under international law. The UN Maritime Law Convention does not prohibit the attack of underwater cables in conflict situations.

Moreover, consistent encoding of data and real-time communication has the ability to make espionage by other nations more difficult. In the future, dependence on foreign infrastructure must be taken into consideration more carefully than ever before. At the European level it would therefore be advisable for EU nations to invest in underwater cable infrastructure of their own and thus reduce their dependence on Big Tech or China. Otherwise the two major players in this field will in the future have a controlling influence on underwater cable infrastructure and gain full control of data transmission. In the first instance, countries need to recognise their degree of dependency and introduce strategic steps to reduce it and diversify their risk.[30]

[1] Wendorf, Marcia (2019): Sowohl die USA als auch Russland verfolgen die Unterwasserkabel der Welt, in: https://www.wissenschaft-x.com/both-the-us-and-russia-are-stalking-the-worlds-undersea-cables, 16 August 2019 [last accessed: 4.1.2023].

[2] Landing points are the points at which the cables reach the mainland.

[3] Gollmer, Philipp (2022). Russische U-Boote interessieren sich für das Nervensystem des Internets, in: Neue Zürcher Zeitung, https://www.nzz.ch/technologie/unterseekabel-verdaechtige-aktivitaeten-von-russischen-u-booten-ld.1678062, 28 April 2022 [last accessed: 13.12.2022].

[4] Rolofs, Oliver (2021): Krieg der Zukunft ein Krieg auch um die Untersee-Datenkabel, in: Neue Zürcher Zeitung, https://www.nzz.ch/meinung/krieg-der-zukunft-ein-krieg-auch-um-die-untersee-datenkabel-ld.1630916?reduced=true, 28 July 2021 [last accessed: 4.1.2023].

[5] Submarine Cable Frequently Asked Questions at https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [last accessed: 13.12.2022].

[6] Researchers at Massachusetts Institute of Technology calculated that a pair of fibres in a sea cable can transmit more signals than 4,000 satellites of the Starlink system.

[7] Erdbeben bremst Internet in Ost-Asien, in: Der Spiegel, https://www.spiegel.de/wirtschaft/durchtrennte-tiefseekabel-erdbeben-bremst-internet-in-ost-asien-a-456687.html, 27 December 2006 [last accessed: 4.1.2023].

[8] Bueger, Christian (2021): Protecting hidden Infrastructure: the Security Politics of the global submarine data cable network, in: Contemporary Security Policy, pp. 1–18.

[9] Blitz, Matt (2017): Secrets haunt the still-classified Operation Ivy Bells, a daring Cold War wiretapping operation conducted 400 feet underwater, in: https://www.ussvirginiabase.org/files/How-Secret-Underwater-Wiretapping-Helped-End-the-Cold-War.pdf, 30 March 2017 [last accessed: 4.1.2023].

[10] This was different in the case of the South Pacific island group of Tonga. The only undersea communication cable broke during a massive volcano eruption and interrupted all transmission.

[11] Seidler, Christoph (2019): Havariertes russisches U-Boot. Die geheimnisvollen Missionen der „Loscharik", in: Der Spiegel, https://www.spiegel.de/wissenschaft/technik/loscharik-russisches-u-boot-wurde-wohl-fuer-spionage-genutzt-a-1275481.html, 2 July 2019 [last accessed: 4.1.2023].

[12] Goldstein, Lyle J. (2022): China's Underwater Unmanned Vehicles: How They'll Dominate Undersea Combat, in: https://nationalinterest.org/blog/reboot/chinas-underwater-unmanned-vehicles-how-theyll-dominate-undersea-combat-200098, 29 January 2022 [last accessed: 4.1.2023].

[13] Mauldin, Alan (2019): Are Content Providers the Biggest Investors in New Submarine Cables, in: https://blog.telegeography.com/are-content-providers-the-biggest-investors-in-new-submarine-cables, 20 June 2019 [last accessed: 4.1.2023].

[14] Savov, Vlad (2021): Google and Facebook's New Cable to link Japan and Southeast Asia, in: Bloomberg News, https://www.bloomberg.com/news/articles/2021-08-16/google-and-facebook-s-new-cable-to-link-japan-and-southeast-asia, 16 August 2021 [last accessed: 4.1.2023].

[15] Bechis, Francesco (2021): Undersea Cables: The Great Data Race Beneath the Ocean, in: Italian Institute for International Political Studies, https://www.ispionline.it/en/pubblicazione/undersea-cables-great-data-race-beneath-oceans-30651, 31 May 2021 [last accessed: 4.1.2023].

[16] Burdette, Lane (2021): Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy, in: Journal of Public & International Affairs, 5 May 2021.

[17] Dobberstein, Laura (2022): Construction starts on another Asia-Europe undersea cable, in: The Register, https://www.theregister.com/2022/02/21/singtel_cable/, 21 February 2022 [last accessed: 4.1.2023].

[18] Submarine cable systems Global Market Report 2022, in: https://finance.yahoo.com/news/submarine-cable-systems-global-market-112500419.html#:~:text=Major%20players%20in%20the%20submarine,Corporation%2C%20JDR%20Cable%20Systems%20Ltd.&text=%2C%20Huawei%20Marine%20Networks%20Co.%2C,Interconnect%20Systems%2C%20HENGTONG%20GROUP%20CO [last accessed: 4.1.2023].

[19] Submarine cable map: https://www.submarinecablemap.com [last accessed: 13.12.2022].

[20] Now interconnecting Brazil and Southern Europe: EllaLink and DE-CIX announce strategic partnership, in: Globenewswire.com, https://www.globenewswire.com/en/news-release/2022/03/09/2400134/0/en/Now-interconnecting-Brazil-and-Southern-Europe-EllaLink-and-DE-CIX-announce-strategic-partnership.html, 9 March 2022 [last accessed: 4.1.2023].

[21] US wants undersea data cable to skip Honk Kong, in: South China Morning Post, https://www.scmp.com/news/world/united-states-canada/article/3089495/us-wants-undersea-data-cable-skip-hong-kong, 18 June 2020 [last accessed: 4.1.2023].

[22] Leprince-Ringuet, Daphne (2020): Facebook and Google drop plans for underwater cable to Hong Kong after security warnings, in: https://www.zdnet.com/home-and-office/networking/facebook-and-google-drop-plans-for-underwater-cable-to-hong-kong-after-security-warnings/, 1 September 2020 [last accessed: 4.1.2023]

[23] Vavasseur, Xavier (2022): France Unveils New Seabed Warfare Strategy, in: Naval News, https://www.navalnews.com/naval-news/2022/02/france-unveils-new-seabed-warfare-strategy/, 16 February 2022 [last accessed: 4.1.2023].

24 Mackenzie, Christina (2022): At Euronaval, defense firms dive deep into seabed warfare platforms, in: https://breakingdefense.com/2022/10/at-euronaval-defense-firms-dive-deep-into-seabed-warfare-platforms/, 21 October 2022 [last accessed: 4.1.2023].

25 Sawall, Achim (2022): Europäische Seekabel sollen militärische geschützt werden, in: https://www.golem.de/news/europaparlament-europaeische-seekabel-sollen-militaerisch-geschuetzt-werden-2209-168655.html, 30 September 2022 [last accessed: 4.1.2023].

26 There are currently three EU agencies that are only responsible for the ocean surface (EMSA, EFCA and Frontex).

27 https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557 [last accessed: 13.12.2022].

28 Nato startet neues Atlantik-Kommando in USA, in: T-online.de, https://www.t-online.de/nachrichten/ausland/internationale-politik/id_88591246/zum-schutz-vor-russland-nato-startet-neues-atlantik-kommando-in-usa.html, 17 September 2020 [last accessed: 4.1.2023].

29 Jahn, Thomas/Holzki, Larissa (2022): Nach dem Angriff auf Nord Stream: Deutschland hat es jetzt eilig mit dem Schutz der maritimen Infrastruktur, in: https://www.tagesspiegel.de/wirtschaft/tiefsee-mikrophone-unbemannte-u-boote-nach-dem-angriff-auf-nord-stream-hat-deutschland-es-jetzt-eilig-mit-dem-schutz-der-maritimen-infrastruktur-8813647.html, 31 October 2022 [last accessed: 4.1.2023].

30 Voelsen, Daniel (2020): Die geopolitische Vereinnahmung des Digitalen, in: Internationale Politik 3/2020, pp. 20–25, https://internationalepolitik.de/system/files/article_pdfs/IPS-03-2020_Dig-EU_Voelsen.pdf [last accessed: 4.1.2023].

Imprint

The Author

Ferdinand Gehringer works for the Konrad-Adenauer-Stiftung e. V. in the International Politics and Security Department as a Policy Advisor on Cybersecurity. In the past he has worked for the foundation as a Policy Advisor on International Law and Rule of Law and as Coordinator of its Rule of Law Programmes. He studied law at the Johannes Gutenberg University in Mainz (Germany) and at the University of Valencia (Spain). Ferdinand Gehringer is an accredited lawyer and certified mediator.

Konrad-Adenauer-Stiftung e. V.

Ferdinand Alexander Gehringer
Cybersecurity
Analysis and Consulting
T +49 30 / 26 996-3460
ferdinand.gehringer@kas.de

Postal address: Konrad-Adenauer-Stiftung, 10907 Berlin

This publication of the Konrad-Adenauer-Stiftung e. V. is solely intended for information purposes. It may not be used by political parties or by election campaigners or supporters for the purpose of election advertising. This applies to federal, state and local elections as well as elections to the European Parliament.

Publisher: Konrad-Adenauer-Stiftung e. V., 2023, Berlin
Design: yellow too, Pasiek Horntrich GbR
Typesetting: Janine Höhle, Konrad-Adenauer-Stiftung e. V.

Produced with financial support from the German Federal Government.

ISBN 978-3-98574-130-4