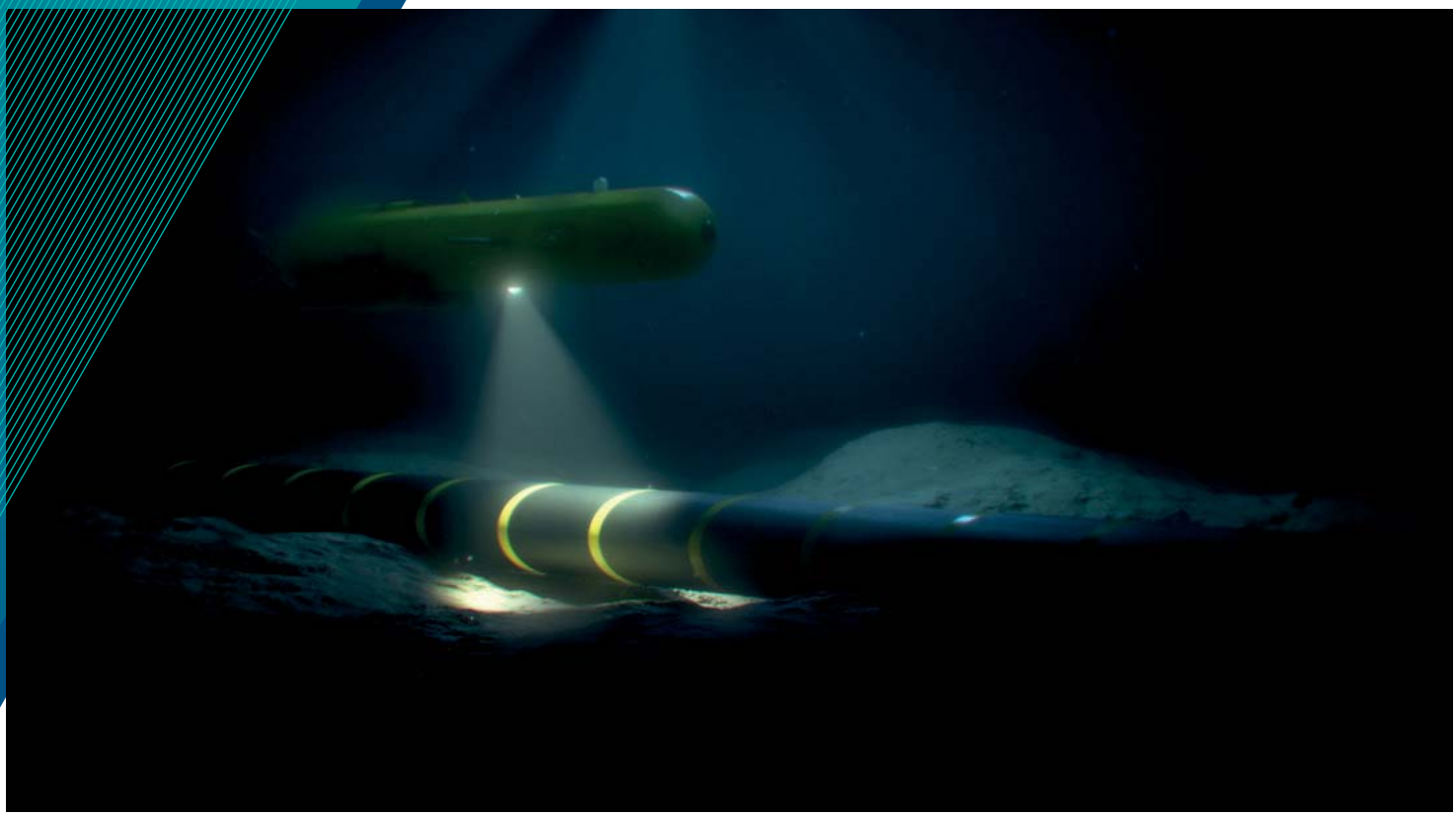
Nr. 495 / Dezember 2022
Analysen & Argumente

KONRAD ADENAUER STIFTUNG



Unterseekabel als Kritische Infrastruktur und geopolitisches Machtinstrument

Warum Unterseekabel besser geschützt werden müssen

Ferdinand Alexander Gehringer

- Unterseekabel sind Kritische Infrastruktur und müssen besonders vor Sabotage und Spionage geschützt werden.
- Die US-amerikanischen Big-Tech-Unternehmen, die Russische Föderation und die Volksrepublik China haben die geopolitische Bedeutung der Unterseekabelinfrastruktur erkannt und Abhängigkeiten aufgebaut beziehungsweise im Falle Russlands gering gehalten.
- Die Europäische Union hat die Bedeutung der Infrastruktur viel zu lange unterschätzt und wird nur langsam tätig.
- Der physische und digitale Schutz der Unterseekabel muss zusammengedacht werden.
- Besonders der physische Schutz der Kritischen Infrastruktur bedarf eines koordinierten und fähigkeitsspezifischen Handelns.

Inhaltsverzeichnis

Daten werden größtenteils durch die Ozeane über Unterseekabel transportiert. Tagtäglich werden Finanztransaktionen in Höhe von mehr als zehn Billionen US-Dollar über die Kabelinfrastruktur abgewickelt.[1] Circa 95 Prozent des internationalen Datenverkehrs verläuft durch die Kabelinfrastruktur unter Wasser, bevor sie über Landungspunkte[2] an Land weiter verteilt werden.[3] Schätzungen gehen davon aus, dass sich die Datenmenge, die beispielsweise durch den Atlantik verläuft, alle zwei Jahre verdoppelt.[4] Die Tendenz ist weiter steigend. Die digitale Transformation mit täglich steigenden Zahlen neuer Internetnutzerinnen und -nutzer und neuen digitalen Prozessen (wie Cloudangebote, Streamingdienste, soziale Medien, etc.) macht es möglich.

Unterseekabel sind Kritische Infrastruktur und derzeit alternativlos für Datenübertragungen

Die Kritische Infrastruktur unter Wasser muss besonders geschützt werden.

Im Jahr 2022 werden 530 Unterseekabel aktiv genutzt oder befinden sich in der Planung. Das Kabelnetz in den Tiefen der Meere beläuft sich derzeit auf eine Gesamtlänge von mindestens 1,3 Millionen Kilometer.[5] Die in der Regel armdicken Kabel, vorwiegend aus feinen Glasfasern (früher aus Kupferdraht) bestehend, bilden damit ein weltweites Netz und eine Handelsroute für Daten aller Art, die durch Lichtimpulse übertragen werden.

Die interkontinentale Übertragung großer Datenmengen in kürzester Zeit mittels Unterseekabel ist aktuell alternativlos. Zwar findet Datenübertragung auch über Satelliten statt, jedoch nur da, wo es terrestrisch nicht möglich und der Bau einer Kabelinfrastruktur ausgeschlossen ist. Die höhere Paketlaufzeit durch die größere Distanz zu den Satelliten, höhere Kosten und größere Störanfälligkeiten der Satellitenübertragung sprechen – derzeit noch – gegen eine Alternativnutzung.[6] Der Schutz der Unterseekabelinfrastruktur zur Gewährleistung der Datenübertragung ist daher auch in der Zukunft unerlässlich.

Bedrohungsszenarien wie Sabotage und Spionage nehmen weiter zu

Daten- und Kommunikationsspionage an Unterseekabeln gibt es bereits seit Jahren.

Die Bedrohungen für die Kritische Infrastruktur unterhalb der Wasseroberfläche sind vielfältig. Seebeben, Wirbelstürme oder das Freischwemmen der Kabel sind realistische Szenarien, denen natürliche Erscheinungen zugrunde liegen und die auch nur schwerlich – durch eine Verstärkung der Ummantelung – verhindert werden können. So führte ein Seebeben vor der Küste Taiwans 2006 zu einem Kabelbruch und unter anderem dazu, dass Banken und Wert-

papierhäuser in der Region zeitweise vom internationalen Handel abgeschnitten waren.[7] Die häufigsten Ursachen für Beschädigungen an Unterseekabeln kommen jedoch aus der Fischerei (38 Prozent) und der Schifffahrt. In der Vergangenheit wurden zahlreiche Kabel durch Anker (25 Prozent) großer Schiffe zerstört.[8]

Doch das sind längst nicht die einzigen möglichen Einwirkungen. Die Vorkommnisse in diesem Sommer in der Ostsee rund um die Gaspipelines Nordstream I und II haben gezeigt, dass die Infrastruktur unter Wasser vor manipulierender Einwirkung nicht gefeit ist. So ist eine Zerstörung durch Sprengstoffdetonationen oder anderen gezielten Angriffen (durch U-Boote, Unterwasserroboter oder -drohnen) auch für Unterseekabel nicht auszuschließen.

Auch die Datenspionage stellt eine zusätzliche Form der Bedrohung dar und keinesfalls eine neuartige. So überwachte der amerikanische Geheimdienst während des Kalten Krieges in den 1980er Jahren im Rahmen der Operation Ivy Bells ein Unterseekabel der Sowjetunion. Durch Abhörvorrichtungen an den russischen Unterseekabeln erhielt die US-Marine kritische Informationen über die Aktivitäten, Prozesse und Technologien der sowjetischen Marine.[9]

Mit verhältnismäßig niedrigerem Aufwand verbunden ist der Zugang zum Datenverkehr über die Landungspunkte der Unterseekabel. So überwacht der britische Geheimdienst GCHQ an der zypriotischen Yeroskipos Submarine Cable Station den globalen Kommunikationsverkehr. Offiziell dient die Überwachung der Terrorismusbekämpfung. Die Enthüllungen von Edward Snowden rund um das Vorgehen der NSA von 2012 bis 2014, im Rahmen dessen europäische Spitzenpolitikerinnen und -politiker abgehört wurden, zeigen aber, dass dies oftmals nur ein Teil der Wahrheit ist. Der US-Geheimdienst nutzte damals unter anderem die Abhörstation Sandagergardan in Dänemark für die Überwachung. In Deutschland gibt es derzeit vier Landungspunkte (Sylt, Rostock, Markgrafenheide, Puttgarden), an denen insgesamt acht Kabel auf das Festland treffen.

Dateninfrastruktur ist Ziel der hybriden Kriegsführung

Ein Totalausfall des Datenverkehrs ist derzeit nicht realistisch. Die Beschädigung eines Kabels führt noch nicht zum Abbruch der Datenübertragung[10], sofern alternative Verbindungen innerhalb dieses Netzes vorhanden sind. Werden einzelne Kabelverbindungen zerstört, „suchen" sich die Daten zunächst einen anderen funktionsfähigen Weg durch die Kabelinfrastruktur (Redundanzen), sodass es lediglich zu Verzögerungen kommen kann. Dabei steigt jedoch das Risiko einer Überlastung des Netzes.

Theoretisch ist zwar ein physischer Angriff auf mehrere Unterseekabel zeitgleich möglich, bedarf aber neben dem Wissen um die exakten Kabelverläufe weitreichender Vorbereitungen und eines großen Ressourcenaufwandes. Da die Kabelverläufe und Orte der Landungspunkte frei einsehbar, im Internet abrufbar und auf Seekarten eingezeichnet sind, kann die Kritische Infrastruktur unter Wasser für moderne Konfliktszenarien allerdings genutzt werden. Die Akteure kombinieren im Rahmen der hybriden Bedrohungen klassische Militäreinsätze, wirtschaftlichen Druck, Angriffe auf Kritische Infrastruktur, Cyberangriffe und Desinformation in (sozialen) Medien. Angriffe auf Unterseekabel können daher Gegenstand von Abschreckungsstrategien und Prozessverzögerungstaktiken werden.

Russland und die USA verfügen über militärisches Gerät zur Zerstörung und China baut die Entwicklung aus

Ein militärisches Wettrüsten zwischen den USA und China ist zu beobachten.

Militärisch können Unterseekabel jederzeit zur Zielscheibe werden. So verfügt die Seekriegsflotte der Russischen Föderation über zwei nuklear betriebene U-Boote. Sie können als Mutterschiffe für kleinere U-Boote zu Spionage- und Sabotagezwecken für die Kriegsführung am Meeresboden (Seabed Warfare) zum Einsatz kommen. Neben dem Bergen von abgestürzten Flugzeugen und dem Installieren von Abhörsensoren ist das nuklearbetriebene U-Boot „Losharik" auch für das Manipulieren oder den Beschuss von Unterseekabeln geeignet.[11]

Außerdem ist das Forschungsschiff „Yantar", das von der Abteilung für Tiefseeforschung im russischen Verteidigungsministerium betrieben wird, mit zwei unbemannten U-Booten ausgestattet, die bis zu 6.000 Meter in die Tiefe gehen können und über hydraulische Greifarme verfügen. In Kombination mit Unterwasserrobotern oder -drohnen ließe sich nicht nur Aufklärung damit betreiben, sondern ebenfalls die Kabelinfrastruktur unter Wasser in wenig bis schlecht überwachten Gebieten (beispielsweise im Atlantik) zerstören. Die US-Marine entwickelt derweil im Rahmen des Projektes Cognitive Lethal Autonomous Weapons Systems (CLAWS) autonome Unterwasserwaffensysteme. Die bewaffneten „Roboter-U-Boote" sollen durch künstliche Intelligenz gesteuert werden und potenziell ohne ausdrückliche menschliche Kontrolle Handlungen – darunter auch die Erzeugung kinetischer Effekte (Zerstörung von Gegenständen) – ausführen können.

Ihnen gleich tut es die Volksrepublik China. Bereits vor drei Jahren hat China sein erstes unbemanntes Unterwasserfahrzeug (UUV) „HSU001" vorgestellt.[12] Zugleich erklärte die Volksrepublik, sich in den kommenden Jahren vor allem mittels hochtechnologisierter UUVs und künstlicher Intelligenz den eigens ausgemachten militärischen Defiziten im Bereich der Unterwasserkriegsführung annehmen zu wollen.

Big Tech und China haben bald die Datenkontrolle

Europa wird bald vollumfänglich abhängig von Dateninfrastruktur der US-Tech-Konzerne und China sein.

Doch Einwirkungsoptionen bieten sich auch auf einer anderen Ebene. Während die Unterseekabel früher noch vermehrt von Konsortien bestehend aus Telekommunikationsbetreibern (vor allem Orange, British Telecom, Alcatel, Norddeutsche Seekabelwerke) geplant, gebaut und betrieben wurden, dringen nun die großen Tech-Konzerne (Alphabet, Meta, Amazon, Apple, Huawei) auf den Markt. Für die Telekommunikationsunternehmen sind die Kosten für den Bau und die Instandhaltung mittlerweile zu hoch. Mit dem Ziel, die Bandbreite zunächst für eigene Angebote auszubauen, investieren die Tech-Konzerne hingegen beständig in neue Kabelnetze oder ersetzen alte durch schnellere, leistungsfähigere Leitungen.[13] So erhöhen vor allem Alphabet und Amazon die Bandbreite für das eigene Cloudangebot und die Versorgung ihrer Rechenzentren. Prognosen zufolge könnte der Eigentumsanteil der Tech-Konzerne aus den USA an der Infrastruktur bis 2027 auf 80 Prozent anwachsen.

Alphabet hat mit den Leitungen „Curie", „Dunant", „Equitano" und „Grace Cooper" vier Unterseekabel in der Hand. Zudem plant das Unternehmen gemeinsam mit Meta zwei weitere Unterseekabel, „Echo" und „Bifrost", die 2023 beziehungsweise 2024 fertiggestellt werden sollen.[14]

Aber auch die Volksrepublik China dringt auf den Markt. So hat China mit chinesischen Telekomkonzernen 2017 ein eigenes Unterseekabel gebaut, das Südostasien, den Mittleren und Nahen Osten mit Westeuropa verbindet.

Das neueste Projekt der Volksrepublik China nennt sich PEACE (Pakistan East Africa Connecting Europe), ist Teil der „digitalen Seidenstraße" und seit August diesen Jahres in Betrieb.[15] Mit einem 15.000 Kilometer langen Unterseekabel wird Pakistan über das Horn von Afrika, durch das Rote Meer und den Suezkanal mit Westeuropa (Landungspunkt: Marseille) verbunden. Zugleich stellt das Projekt eine Verbindung nach Ostafrika (Somalia und über die Africa-1 auch nach Kenia) her.[16]

Mit einer Datenübertragungsrate von 96 Terabyte pro Sekunde ermöglicht es die Übertragung von so vielen Daten pro Sekunde, um 90.000 Stunden Netflix zu streamen.[17] Neben den wirtschaftlichen Beweggründen für den Bau könnte diese Struktur die bestehende chinesische Militärbase in Dschibuti mit künftigen militärischen Stützpunkten der Volksrepublik China in Südasien (Pakistan) oder im Golf verbinden. Die Volksrepublik kokettiert bereits seit Längerem mit dem Ausbau der eigenen militärischen Stützpunkte weltweit. Eine Ausweitung des PEACE-Projektes auf Singapur über die Malediven wurde bereits angekündigt.

Zudem sind chinesische Unternehmen bereits heute Zulieferer für Bauteile der Infrastruktur. Mit dem chinesischen Unternehmen Hengtong Optic-Electric gehört ein chinesischer Hersteller zu den größten Glasfaserherstellern der Welt.[18]

Russland hingegen hält seine Abhängigkeit gering, verfügt auf seinem Territorium nicht über wichtige Knotenpunkte und ist nur über vier internationale Unterseekabel (Verbindung mit Finnland, Georgien und zwei mit Japan) an das globale Datenverkehrsnetz angebunden.[19] Über diese überschaubare Anzahl an Verknüpfungen behält sich die Russische Föderation zumindest die Möglichkeit der Kontrolle der eigenen Landungspunkte und des Datenverkehrs vor.

Eine ähnliche Tendenz, sich der möglichen ausländischen Einflussnahme zu entziehen, lässt sich in Brasilien beobachten. Vergangenes Jahr im Juni wurde „EllaLink", mit einer Datenübertragungsrate von 100 Terabyte pro Sekunde, in Betrieb genommen: Ein Unterseekabel, das Brasilien und Lateinamerika mit Europa (Portugal) verbindet. Gebaut wurde es nach Angaben der brasilianischen Regierung, um die Neutralität des Datenverkehrs zu sichern und sich einer möglichen Überwachung durch US-Geheimdienste beziehungsweise der Datenkontrolle durch die US-Tech-Konzerne zu entziehen.[20]

Geopolitischer Wettlauf ist nicht zu übersehen

Die geopolitische Bedeutung von Unterseekabeln haben die Großmächte längst erkannt. Wer die Kabelinfrastruktur kontrolliert, kann unter Umständen den Informationsfluss erfassen oder gar beeinflussen. 2020 verhinderten die US-Behörden den Bau einer Direktleitung zwischen den USA und Hongkong.[21]

Die USA sind sich den drohenden Abhängigkeiten von China bewusst.

Vor fünf Jahren beabsichtigten damals noch Google und Facebook mit einer Tochtergesellschaft der China Soft Power Holdings zusammenzuarbeiten, um Los Angeles und Hongkong mit einem Hochkapazitätsunterseekabel zu verbinden. Das Pacific Light Cable Network sollte 12.800 Kilometer lang sein und den Pazifischen Ozean unterqueren. Mit etwa 120 Terabyte pro Sekunde sollte die Verbindung 80 Millionen hochauflösende Videokonferenzen gleichzeitig zwischen Los Angeles und Hongkong ermöglichen.[22]

Die US-Behörden blockierten das Vorhaben und begründeten die Ablehnung damit, dass Hongkong als Landungspunkt auf chinesischem Territorium die nationale Sicherheit der USA gefährdet und Millionen von sensiblen personenbezogenen Daten von US-Bürgerinnen und

US-Bürgern einer chinesischen Überwachung preisgegeben werden könnten. Das andere Teilstück zwischen den USA, den Philippinen und Taiwan wurde hingegen in Betrieb genommen.

Die Volksrepublik China sieht offenbar auch ein mögliches Angriffsszenario auf Taiwan über Unterseekabel. Auf einer chinesischen Plattform wurden mögliche strategische Ziele, zu denen auch der Zugriff auf die Halbleiterindustrie Taiwans über die Unterseekabelinfrastruktur gehörte, entdeckt. Wie realistisch und ernsthaft diese Überlegungen in Regierungskreisen sind, lässt sich jedoch nicht seriös bewerten.

Schnelle Leitungen entscheiden über die Datensouveränität

Zukünftig wird es – sofern die Staaten keinen Kontrollverlust hinnehmen wollen – immer entscheidender, von wem und mit welchen Bauelementen die Kabel gebaut werden, um die Einflusspotenziale anderer Staaten so gering wie möglich zu halten.

Mit schnelleren Leitungen können mehr Daten kontrolliert werden.

Auch könnte das Rennen um die größte Datenübertragungsrate perspektivisch noch mehr in den Vordergrund rücken. Wer schnellere Leitungen baut, die Datenübertragungsrate und tatsächliche Kapazität erhöht, kann in kürzerer Zeit mehr Daten durch seine Unterseekabel leiten und so den Datenfluss beeinträchtigen. Daten suchen sich immer den schnelleren Weg, ganz gleich, ob dieser über Landungspunkte in China, den USA oder Russland reicht.

Die Infrastruktur überwachen und verschlüsselt Daten übertragen

Physischer und digitaler Schutz müssen zusammengedacht werden.

Angesichts der zu beobachtenden Entwicklung ist die Unterseekabelinfrastruktur als Kritische Infrastruktur besonders zu schützen – ganz im Sinne eines All-Gefahren-Ansatzes. In diesem Zusammenhang werden alle Arten von Gefahren (zum Beispiel Naturgefahren, technologische Gefahren, problematische Abhängigkeiten etc.) mitgedacht. Für Unterseekabel bedeutet das: Durch vollumfängliche Lagebilder mithilfe von Satellitenaufzeichnungen und Unterwasserüberwachung sowie Patrouillen können schädigende Einwirkungen, Manipulationsversuche oder Spionageeingriffe frühzeitig verhindert oder die Angreifer erkannt und zugeordnet (Attribution) werden. Landungspunkte sollten hierbei einer besonderen Beobachtung unterstellt werden. Darüber hinaus könnten Angriffe mit Unterwasserrobotern oder Unterwasserdrohnen notfalls auch abgewehrt werden. Dazu müssten zahlreiche internationale (Einzel-)Initiativen besser abgestimmt und koordiniert werden. Frankreich hat im Februar bereits eine Strategie für den Unterwasserkrieg publik gemacht.[23] Teil dieser ist es, die Unterwasserfähigkeiten der französischen Marine auf bis zu 6.000 Meter Tiefe zu erweitern, gerade ausreichend, um die durchschnittliche Tiefe der Ozeane zu erreichen.[24] Im März gab die britische Marine bekannt, dass ab 2024 das Schiff „Mulit Role Ocean Surveillance Ship“ die Überwachung des britischen und Teile der internationalen Gewässer übernehmen soll, ausgestattet mit einem ferngesteuerten Tauchboot und verschiedenen Sensoren. Die Telecom Italia Sparkle kündigte im Sommer 2022 an, mit der italienischen Marine bei der Aufklärung und Überwachung in den Gebieten rund um die Kabel von Sparkle zusammenzuarbeiten.[25] Die Bundesregierung ist bisher untätig geblieben, auch eine europäische Institution, die für den Schutz und die Überwachung zuständig ist, gibt es bisher noch nicht.[26] Die Europäische Union hat jedoch im Juni 2022 die Studie *Security threats to undersea communications cables and infrastructure – consequences for the EU*[27], die sich mit dem Schutzbedürfnis der Unterseekabel befasst, veröffentlicht. Die Europäische Kommission hat die Errichtung einer Koordinierungsgruppe für die Widerstandsfähigkeit von Kabeln vorgeschlagen. Denkbar wäre auch der Aufbau einer Anti-Submarine-Warfare (ASW) im NATO-Verbund zum Schutz der Kritischen Infrastruktur. Das Joint Force

Command Norfolk (JFC-NF) der NATO, das 2018 für den Schutz der Transport- und Kommunikationswege über den Atlantik aufgestellt wurde, ist allenfalls ein Anfang.[28]

Auch die deutsche Polizei und Marine sollten zum Schutz der Infrastruktur die eigenen Kapazitäten aufstocken. Neben Polizeihubschraubern bedarf es einer Verdopplung der U-Boote der Bundeswehr von sechs auf zwölf, Flottendienstboote (kleine Spionageschiffe mit elektronischer Abhörfunktion), autonome Unterwasserfahrzeuge wie die „Seekatze" und den Ausbau des akustischen Auswertungssystems der Bundeswehr. Eine Sonderrolle könnte das Territoriale Führungskommando innerhalb des Auftrages Heimatschutz für den Schutz der Kritischen Infrastruktur in Deutschland zukommen. Zudem müssten Back-up-Lösungen geschaffen werden. So sollte Satellitentechnik für die Aufrechterhaltung einer Notdatenübertagung zum Einsatz kommen. Darüber hinaus gibt es derzeit nur drei Reparaturschiffe, die für Wartung und Reparatur der Unterseekabel im Atlantik zur Verfügung stehen[29] – bei Weitem nicht ausreichend. Akustische Sensorsysteme (Distributed Acoustic Sensoring DAS), die an den Kabeln angebracht werden, könnten diese zu einer Art Mikrofon machen. Die Sensorelemente ermöglichen die Erfassung von Geräuschen und Frequenzen in der Umgebung der Kabel und könnten so Hinweise auf ungewöhnliche Aktivitäten an diesen geben. Regulatorisch bedarf es auf nationaler Ebene besonderer Schutz- und Instandsetzungspflichten für die Betreiber und klarer fähigkeitsspezifischer Aufgabenverteilungen. International ist die Unterseekabelinfrastruktur bisher nicht völkerrechtlich geschützt. Das UN-Seerechtübereinkommen enthält kein Verbot, Unterseekabel im Konfliktfall anzugreifen.

Außerdem kann eine konsequente Verschlüsselung der Daten und der Echtzeit-Kommunikation die Spionage durch andere Staaten erschweren. Künftig gilt es, die Abhängigkeit von fremder Infrastruktur mehr denn je zu berücksichtigen. Auf europäischer Ebene wäre es daher ratsam, in eigene Unterseekabelinfrastruktur zu investieren und so die Abhängigkeit von Big Tech oder China zu verringern. Ansonsten werden beide zusammen künftig die Unterseekabelinfrastruktur beherrschen und so die Kontrolle über die Datenübertragung innehaben. Ein erster Schritt wäre, sich dieser Abhängigkeit bewusst zu werden und strategische Schritte für die Verringerung der Abhängigkeit und Diversifizierung des Risikos einzuleiten.[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, 16.08.2019 (zuletzt abgerufen am 13.12.2022).

2 Landungspunkte sind die Stellen, an denen die Kabel das Festland erreichen.

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, 28.04.2022 (zuletzt abgerufen am 13.12.2022).

4 Rolofs, Oliver (2021): Der Krieg der Zukunft wird auch ein Krieg um die Untersee-Datenkabel sein, in: Neue Zürcher Zeitung, https://www.nzz.ch/meinung/krieg-der-zukunft-ein-krieg-auch-um-die-untersee-datenkabel-ld.1630916?reduced=true, 28.07.2021 (zuletzt abgerufen am 13.12.2022).

5 Submarine Cable Frequently Asked Questions, in: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions (zuletzt abgerufen am 13.12.2022).

6 So haben Forscher des Massachusetts Institute of Technology errechnet, dass ein Faserpaar in einem Seekabel mehr Signale übermitteln kann als 4.000 Satelliten des Starlink-Systems.

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, 27.12.2006 (zuletzt abgerufen am 13.12.2022).

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

9 Blitz, Matt (2017): Secrets hunt 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, 30.03.2017 (zuletzt abgerufen am 13.12.2022).

10 Anders war dies hingegen bei der südpazifischen Inselgruppe Tonga. Das einzige Unterseekommunikationskabel ist bei einem massiven Vulkanausbruch gerissen und unterbrach die Übertragung vollständig.

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, 02.07.2019 (zuletzt abgerufen am 13.12.2022).

12 https://nationalinterest.org/blog/reboot/chinas-underwater-unmanned-vehicles-how-theyll-dominate-undersea-combat-200098 (zuletzt abgerufen am 13.12.2022).

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, 20.06.2019 (zuletzt abgerufen am 13.12.2022).

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, 16.08.2021 (zuletzt abgerufen am 13.12.2022).

15 Bechis, Francesco: 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, 31.05.2021 (zuletzt abgerufen am 13.12.2022).

16 Burdette, Lane (2021): Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy, in: Journal of Public & International Affairs, 05.05.2021.

17 Dobberstein, Laura (2022): Construction starts on another Asia-Europe undersea cable, in: The Register, https://www.theregister.com/2022/02/21/singtel_cable/, 21.02.2022, (zuletzt abgerufen am 13.12.2022).

18 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 (zuletzt abgerufen am 13.12.2022).

19 Submarine cable map – https://www.submarinecablemap.com/ (zuletzt abgerufen am 13.12.2022).

20 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, 09.03.2022 (zuletzt abgerufen am 13.12.2022).

21 https://www.scmp.com/news/world/united-states-canada/article/3089495/us-wants-undersea-data-cable-skip-hong-kong, 18.06.2020 (zuletzt abgerufen am 13.12.2022).

22 Leprince-Ringuet, Daphne (2020): Facebook and Google drop plans for underwater cable to Hong Kong after security warnings, in: www.zdnet.com, https://www.zdnet.com/home-and-office/networking/facebook-and-google-drop-plans-for-underwater-cable-to-hong-kong-after-security-warnings/, 01.09.2020 (zuletzt abgerufen am 13.12.2022).

23 https://www.navalnews.com/naval-news/2022/02/france-unveils-new-seabed-warfare-strategy/ (zuletzt abgerufen am 13.12.2022).

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. Oktober 2022 (zuletzt abgerufen am 13.12.2022).

25 https://www.golem.de/news/europaparlament-europaeische-seekabel-sollen-militaerisch-geschuetzt-werden-2209-168655.html (zuletzt abgerufen am 13.12.2022).

26 So gibt es gegenwärtig drei EU-Agenturen, die lediglich für die Meeresoberfläche zuständig sind (EMSA, EFCA und Frontex).

27 https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557 (zuletzt abgerufen am 13.12.2022).

28 https://www.t-online.de/nachrichten/ausland/internationale-politik/id_88591246/zum-schutz-vor-russland-nato-startet-neues-atlantik-kommando-in-usa.html (zuletzt abgerufen am 13.12.2022).

29 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 (zuletzt abgerufen am 13.12.2022).

30 Voelsen, Daniel (2020): Die geopolitische Vereinnahmung des Digitalen, in: Internationale Politik, 3/2020, S. 20–25, https://internationalepolitik.de/system/files/article_pdfs/IPS-03-2020_Dig-EU_Voelsen.pdf (zuletzt abgerufen am 13.12.2022).

Impressum

Der Autor

Ferdinand Gehringer arbeitet in der Abteilung Internationale Politik und Sicherheit als Referent für Cybersicherheit. Zuvor war er als Referent für Völkerrecht und Rechtsstaatsdialog sowie als Koordinator der Rechtsstaatsprogramme für die Konrad-Adenauer-Stiftung tätig. Er hat Rechtswissenschaften an der Johannes-Gutenberg-Universität Mainz und an der Universidad de Valencia studiert. Ferdinand Gehringer ist zugelassener Rechtsanwalt und zertifizierter Mediator.

Konrad-Adenauer-Stiftung e. V.

Ferdinand Alexander Gehringer
Cybersicherheit
Analyse und Beratung
T +49 30 / 26 996-3460
ferdinand.gehringer@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2022, Berlin
Gestaltung: yellow too, Pasiek Horntrich GbR
Satz: Janine Höhle, Konrad-Adenauer-Stiftung e. V.

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-126-7