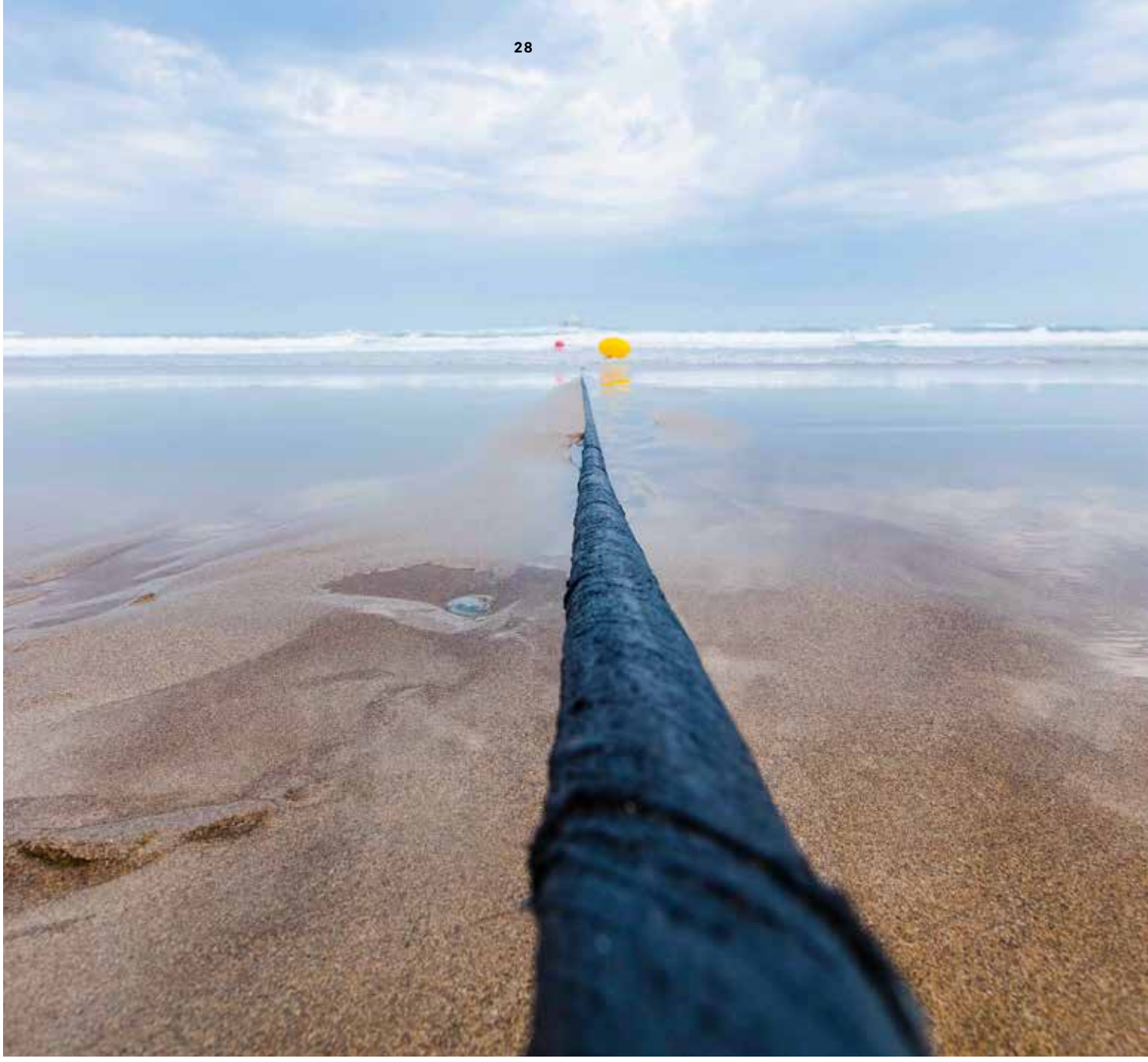


Das Marea-Seekabel, das von Facebook und Microsoft finanziert wurde, überträgt seit 2018 Daten zwischen Europa über Spanien in die USA.

Verletzliche Adern am Meeresgrund

Foto: Mark Maljan / Microsoft; Illustration: AdobeStock

Die Datenadern der Menschheit liegen tief in den Ozeanen – und sind verletzlich. Die Sabotage von Unterseekabeln nimmt zu. Während andere Länder die Bedeutung der kritischen Infrastruktur auf dem Grund der Meere erkannt haben, hält sich Deutschland mit proaktiven Schutzmaßnahmen zurück. Die Zeit arbeitet für China.

VON FERDINAND GEHRINGER

Ein autonomes Unterwassergefährt inspiziert ein Datenkabel auf dem Meeresgrund (Illustration).

Im Oktober 2022 meldete das französische Telekommunikationsunternehmen Free Störungen in der Datenübertragung nach Asien, in die USA und in Europa. Das Glasfasernetz wurde an mehreren Stellen zeitgleich durchtrennt. Wie sich infolge der polizeilichen Ermittlungen herausstellte, handelte es sich um einen Sabotageakt. Unter anderem war ein Unterseekabel in Marseille betroffen. Die Stadt ist einer der großen und wichtigen Knotenpunkte in Europa, viele Unterseekabel kommen dort zusammen.

Rund 95 Prozent des internationalen Datenverkehrs verlaufen durch die Kabelinfrastruktur unter Wasser. Das weltweite Kabelnetz umfasst eine Gesamtlänge von etwa 1,3 Millionen Kilometern. Das längste Unterseekabel verbindet Singapur und die Vereinigten Staaten und ist 20.000 Kilometer lang. Über die Landungspunkte werden die Daten von den Unterseekabeln dann auf dem Land weiter verteilt. Schätzungen zufolge verdoppelt sich das Datenvolumen, das durch die Unterseekabel im Transatlantik transportiert wird, alle zwei Jahre. In Deutschland gibt es vier Landungspunkte: Sylt, Rostock, Markgrafenheide und Puttgarden.

Derzeit werden 530 Unterseekabel für die Übertragung von Daten genutzt oder befinden sich in der Planungsphase. Unterseekabel sind für die Datenübertragung unverzichtbar. Daten werden zwar auch über Satelliten vor allem dorthin übertragen, wo der Bau einer Kabelinfrastruktur nur schwer möglich ist. Das führt zu höheren Kosten, einer längeren Übertragungsdauer und einer größeren Störanfälligkeit. Am Ende ist die terrestrische Übertragung noch alternativlos. Das Massachusetts Institute of Technology hat errechnet, dass ein einziges Faserpaar in einem Unterseekabel mehr Signale übermitteln kann als viertausend Starlink-Satellitensysteme. Das Problem: Die Infrastruktur ist gemessen an ihrer Bedeutung als kritisch einzustufen.

Beschädigungen oder Kabelbrüche durch Seebeben, Wirbelstürme oder Freischwemmen sind keine Seltenheit. Diese Risiken lassen sich nur durch verstärkte Ummantelung der armdicken Kabel minimieren. Die häufigste Ursache für Schäden an der Infrastruktur stellt mit rund 38 Prozent der Fälle jedoch die Fischerei dar. So haben Netze und Anker in der Vergangenheit zahlreiche Kabel beschädigt.

Die Sabotageakte an den Gaspipelines von Nordstream I und II haben gezeigt, dass durch Sprengstoffdetonationen auch Kabel jederzeit zerstört werden können. Eine Sabotage durch Taucher, U-Boote, Unterwasserroboter oder -drohnen sind realistische Szenarien.

Dass der Datenverkehr durch Beschädigungen oder Sabotage vollständig ausfällt, ist allerdings in den seltensten Fällen möglich. Ist ein Kabel nicht mehr funktionsfähig, führt es noch nicht zum Abbruch der Datenübertragung, sofern alternative Verbindungen bestehen. Daten „suchen“ sich andere mögliche Wege durch die Infrastruktur. Eher kommt es stattdessen zu Verzögerungen in der Übertragung. Doch es kann auch anders kommen. Im Inselstaat Tonga im Südpazifik kam 2019 das gesellschaftliche und wirtschaftliche Leben zum Erliegen, nachdem die Internetverbindung für zwölf Tage unterbrochen war. Der Inselstaat ist nämlich nur über ein einziges Unterseekabel mit dem globalen Datenverkehr verbunden. ▸

Verschiebung im Markt

Aus deutscher und europäischer Sicht sind die physischen Einwirkungsmöglichkeiten jedoch nur ein Aspekt der Bedrohungsanalyse. Während früher große Konsortien aus Telekommunikationsbetreibern in die Kabelinfrastruktur investierten und einseitige Abhängigkeiten weniger ausgeprägt waren, zeichnet sich heute eine andere Tendenz ab. Die Telekommunikationsunternehmen können sich den Bau und die Instandhaltung nicht mehr leisten. Stattdessen drängen große Tech-Unternehmen auf den Markt. Alphabet, Meta, Amazon, Apple und Huawei investieren enorm in die Infrastruktur. Der Marktanteil der US-Tech-Konzerne könnte bis 2027 auf 80 Prozent anwachsen. Chinesischen Herstellern von Bauteilen für Infrastruktur sowie Projektinvestoren aus China werden hingegen bis 2030 nahezu 20 Prozent der gesamten Marktanteile vorausgesagt. Hengtong Optic-Electric gehört als chinesischer Hersteller zu den größten Glasfaserproduzenten der Welt. Bei allen seit 2019 geplanten Unterseekabelinfrastrukturprojekten liegt der Anteil Chinas bereits bei 24 Prozent.

Als Teil der „Digitalen Seidenstraße“ erstreckt sich das PEACE-Projekt (Pakistan & East Africa Connecting Europe) der Volksrepublik China über Pakistan, das Horn von Afrika durch den Suezkanal bis nach Westeuropa. Landungspunkt des Projektes, das Chinas Datenübertragung nach Afrika und Europa unabhängig von anderen Unternehmen oder geopolitischen Akteuren machen soll, ist wiederum Marseille. Europa ist vom Markt ausgeschlossen und macht sich dadurch fast vollumfänglich abhängig. Lediglich die Unternehmen Nokia und Orange zeigen noch Ambitionen für Investitionen im Bereich der Kabelinfrastruktur. So verbuchte Nokia 2022 einen Marktzuwachs von 1,2 Milliarden Euro auf dem Markt der Unterseekabelinfrastruktur.

Brasilien beispielsweise hat diese Entwicklungen erkannt und mit Ella-Link im Juni 2021 ein Unterseekabel von Brasilien nach Portugal verlegt, um sich ebenfalls geopolitisch unabhängiger zu positionieren. Russland ist über Finnland, Georgien und Japan mit dem internationalen Datenkabelnetz verbunden.

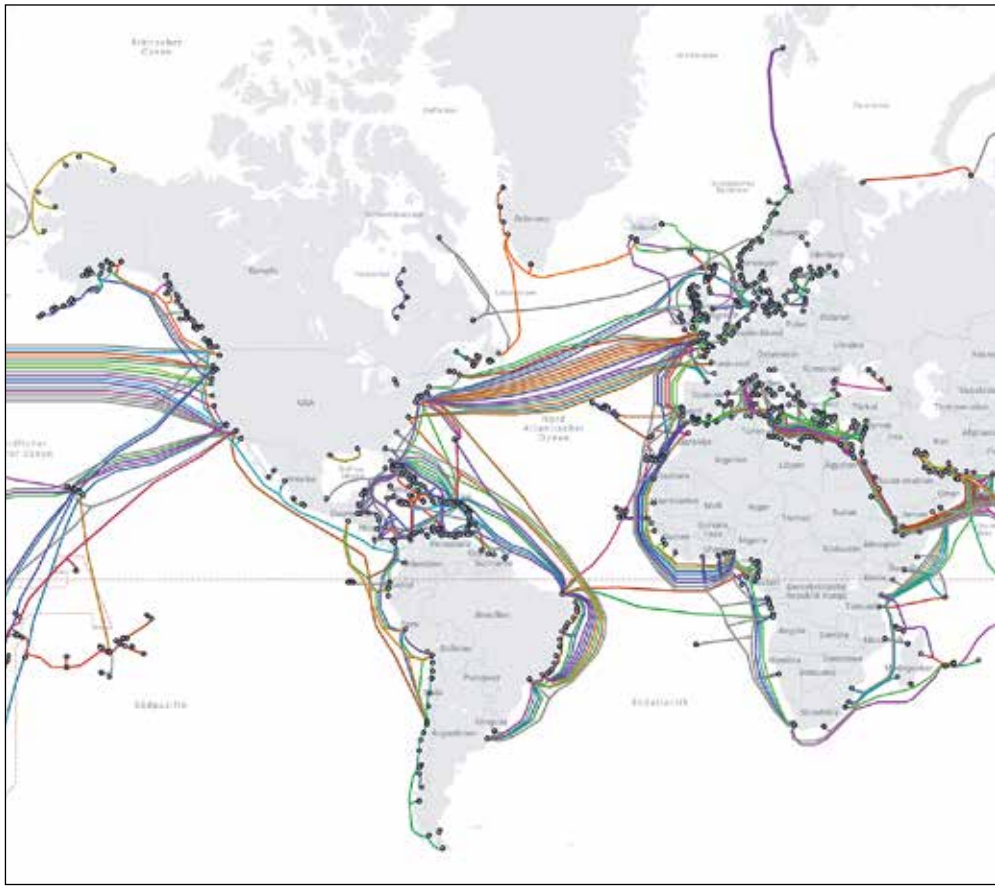
Bereits seit dem Kalten Krieg werden die Datenübertragungen an Unterseekabeln von Geheimdiensten überwacht. Der britische Geheimdienst GCHQ kontrolliert heutzutage den Kommunikationsverkehr beispielsweise auf Zypern – den offiziellen Angaben zufolge zur Terrorismusbekämpfung.

Die Dateninfrastruktur eignet sich auch als Ziel hybrider Kriegsführung. Innerhalb zwischenstaatlicher Beziehungen werden hierbei Machtinstrumente wie Cyberangriffe, Angriffe auf Kritische Infrastruktur, Desinformationskampagnen, Migration, wirtschaftlicher Druck oder einseitige Interdependenzen aufeinander abgestimmt zum Einsatz gebracht. Verwundbarkeiten eines Staates im gesellschaftlichen, wirtschaftlichen, politischen, militärischen oder technologischen Bereich sollen so ausgenutzt werden, um Unsicherheiten zu erzeugen oder Instabilität hervorzurufen.

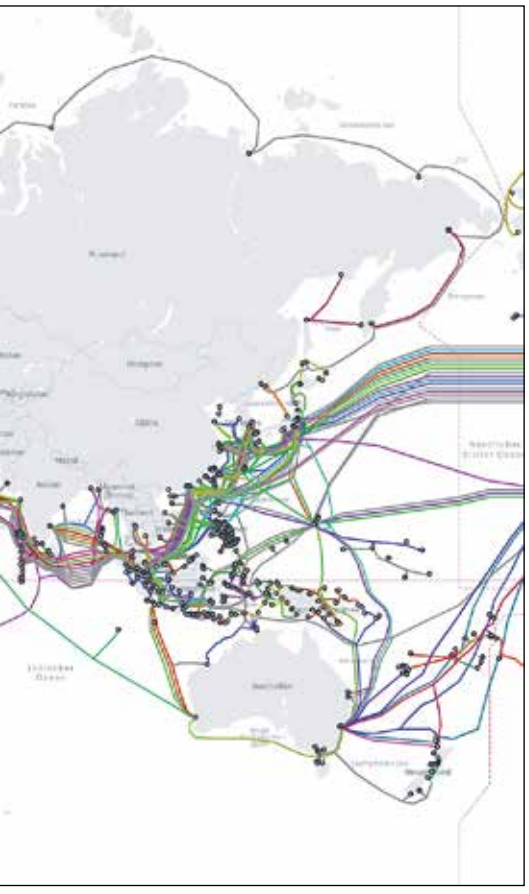
Da sich Daten immer auch andere, schnellere Wege suchen, hat derjenige, der die schnellste Datenübertragung anbieten kann, die Kontrolle über den Datenfluss. Kontrolle und Datensouveränität ist hierbei ein Stichwort: Die US-Behörden blockierten vor sechs Jahren ein Bauvorhaben von Google und Facebook mit China Soft Power Holdings mit dem Verweis auf die Gefährdung nationaler Sicherheitsinteressen. Mit dem Pacific Light Cable Network sollte eine Verbindung zwischen Hongkong und den USA gebaut werden. Dass personenbezogene Daten aus den USA auf chinesisches Festland treffen, war den USA zu risikoreich.

Russland hat mit Glavnoye Upravlenie Glubokovodsk Issledovanii (GUGI) eine Hauptabteilung für die Unterwasserforschung innerhalb des Marineführungsstabes im Verteidigungsministerium – offiziell rein zu Forschungszwecken. Die gut ausgestattete russische Flotte umfasst U-Boote und ozeanografische Vermessungsschiffe. So kann das Forschungsschiff „Yantar“ mit zwei unbemannten U-Booten ausgestattet werden, die durch Greifarme jederzeit zur Sabotage von Unterseekabeln oder Gaspipe-

Weltkarte der Datenkabel



lines in Tiefen bis zu 6000 Meter in der Lage sind. Das nuklear betriebene Mini U-Boot „Losharik“ ist für Manipulationen oder Beschuss der Unterwasserinfrastruktur ebenso einsetzbar wie das nukleare Torpedosystem „Poseidon“ oder das unbemannte Unterwasserfahrzeug „Harpsichord“. Letzten Sommer wurde mit der „Belgorod“ das größte U-Boot der Welt in Dienst gestellt und als ehemaliges Angriffs-U-Boot zum nuklearbetriebenen Mutterschiff für bis zu acht Unterwasserdrohnen umfunktioniert. Der Bootskörper dient als Dock für kleine und unbemannte Tauchfahrzeuge. Die US-Marine entwickelt im Rahmen des Projektes Cognitive Lethal Autonomous Weapons Systems (CLAWS) autonome Unterwasserwaffensysteme. Unterwasserroboter sollen künftig mit Hilfe von Künstlicher Intelligenz auch in den Tiefen der Ozeane Handlungen durchführen, die keinesfalls nur Reparaturarbeiten umfassen. Die Volkrepublik China hat 2019 sein erstes unbemanntes U-Boot, die „HSU001“ vorgestellt und kündigte ebenfalls Forschungsprojekte zum Einsatz Künstlicher Intelligenz in diesem Bereich an.



Quelle und Grafik: submarinecablemap.com / by TeleGeography under CC, Stand 08.03.23

Unterwasserüberwachung

Im November 2022 ließ das britische Verteidigungsministerium verlauten, dass es zwei MROS-Schiffe (Multi-Role Ocean Surveillance) beschaffen wird, um die Unterwasserinfrastruktur besser schützen zu können. Die MROS kann autonome Unterwasserfahrzeuge mitführen. Zudem gab die Royal Navy im Dezember 2022 bekannt, dass sie das unbewaffnete, batteriebetriebene U-Boot „Cetus“ beschaffen wird. Es kann tiefer tauchen als alle Boote der derzeitigen U-Boot-Flotte und in einem Einsatz bis zu 1.000 Meilen zurücklegen.

Deutschland und Europa sollten zügig ihre Ressourcen ausbauen und vorhandene bündeln. Mithilfe von Satellitenaufzeichnungen und Unterwasserüberwachung sowie regelmäßigen Patrouillen auch unter Wasser kann ein europäisches Lagebild für die Kritische Infrastruktur erstellt werden. Schädigende Einwirkungen können frühzeitig verhindert oder Angreifer zumindest identifiziert werden. Die strategischen Bestrebungen einzelner Länder wie beispielsweise Frankreich, sollten in einer europaweiten Strategie zum Schutz und zur Verteidigung der Kritischen Infrastruktur unter Wasser aufgehen. Was für Unterseekabel gilt, gilt gleichermaßen für Stromkabelverbindungen und Gas- oder LNG-Pipelines. Die vorwiegend privaten Betreiber der Infrastruktur müssen vor Einwirkungen durch militärische Fähigkeiten unterstützt werden.

Die italienische Marine kooperiert mit dem italienischen Telekombetreiber. Dass in Deutschland die Polizei für den Schutz und die Überwachung in deutschen Hoheitsgewässern zuständig ist, entspricht nicht einer fähigkeitsspezifischen Zuständigkeitsverteilung. Ein Großteil der Infrastruktur verläuft nicht in deutschen Hoheitsgewässern, sondern in internationalen Gewässern oder Küstenmeeren von Drittstaaten, sodass eine einheitliche Zuständigkeit bei der Marine oder eine Sonderrolle des Territorialen Führungskommandos angemessen wäre.

Die NATO hat im vergangenen Januar eine Koordinierungszelle angekündigt, die unter Leitung von Generalleutnant Hans-Werner Wiermann Schwachstellen in der Infrastruktur identifizieren und gefährdete Pipelines und Unterseekabel besser überwachen und schützen soll. Damit Deutschland diese Koordinierungszelle auch unterstützen kann, müssen die Fähigkeiten der Marine ausgebaut werden. Die Zahl der U-Boote sollte verdoppelt werden. Neben einer Beschaffung der „Seekatze“ (unbemanntes kleines U-Boot) und Flottendienstbooten, müssen auch die akustischen Auswertungssysteme der Bundeswehr ausgebaut werden. Auch die Landungspunkte der Unterseekabel sind häufig nicht hinreichend geschützt sowie leicht zu orten, da sie oft wie Lagerhallen aussehen und der Verlauf der Kabel und Landungspunkte auf Karten einsehbar sind.

Auch die Unterseekabel selbst können für den Schutz und die Abwehr von Einwirkungen besser ausgestattet werden. Durch Sensoren und Infrarotkameras wären Eingriffe schneller erfassbar. Die Zahl der Reparaturschiffe gilt es zu erhöhen. Derzeit gibt es für den gesamten Atlantikbereich drei Reparaturschiffe.

Generell lassen sich Schäden an der Kritischen Infrastruktur und Beeinträchtigungen des Datenverkehrs nicht umfassend verhindern. Daher ist der Aufbau von Redundanzen wichtig. Mit Back-up-Datenübertragungsverbindungen und mit dem Aufbau der IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite) plant die EU ein schnelles und hochsicheres Satellitensystem bis 2027 für Datenübertragungen und Kommunikation.

Deutschland hält sich mit proaktiven Maßnahmen zum Schutz der Kritischen Infrastruktur noch vollständig zurück. Es bleibt abzuwarten, ob es einen weiteren Schockmoment, wie nach den Sabotageakten auf Nordstream I und II braucht, ehe eine sachgerechte Zuständigkeitsverteilung sowie Ausstattung vorangetrieben wird. ■

FERDINAND GEHRINGER ist Referent für Innere- und Cybersicherheit in der Abteilung Internationale Politik und Sicherheit der Konrad-Adenauer-Stiftung. Zugleich leitet er den Arbeitskreis Junge Außenpolitiker der Konrad-Adenauer-Stiftung e.V.