Centrum für Europäische Politik
FREIBURG | BERLIN

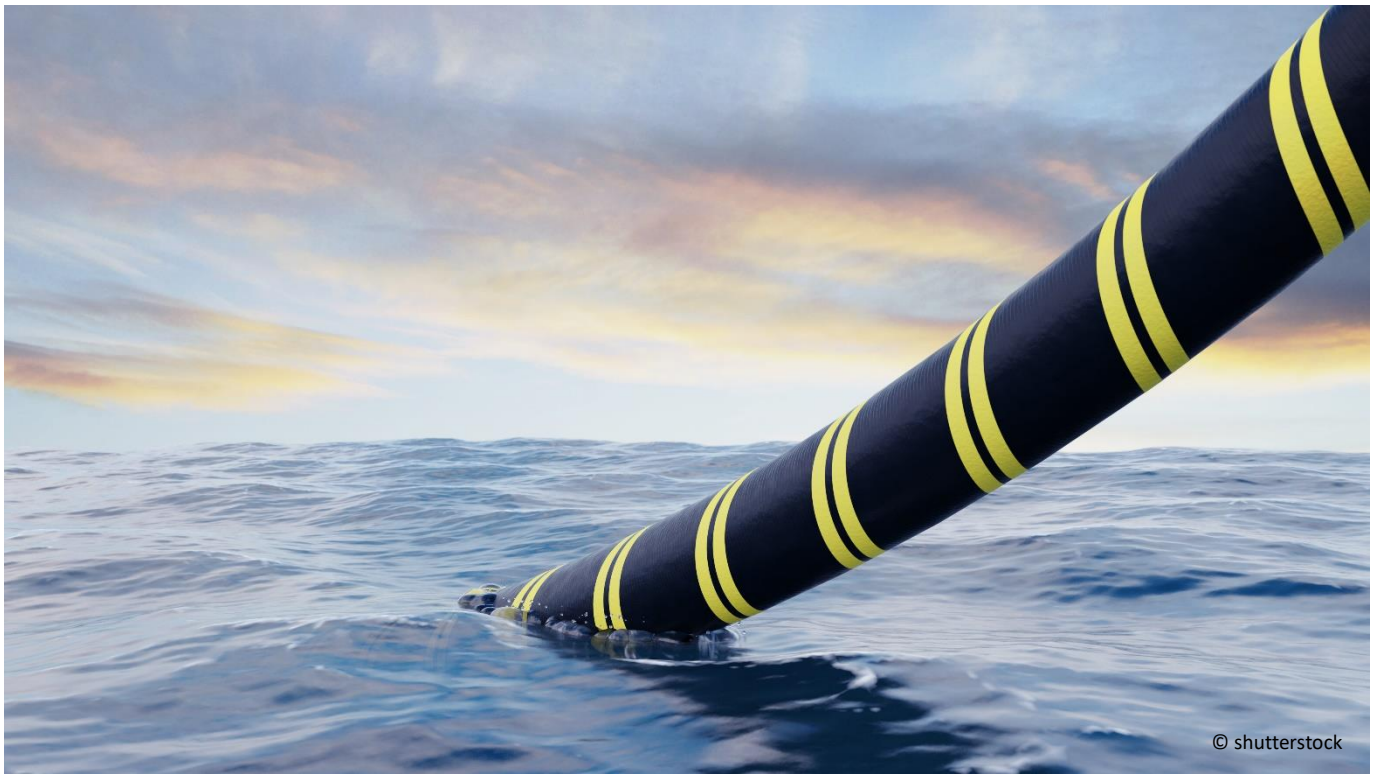
cepAdhoc

Nr. 13 | 2022 21. Oktober 2022

Europas verwundbares Rückgrat

Warum die EU digitale kritische Infrastruktur besser schützen muss

Anselm Küsters



Die jüngsten Anschläge auf Gas-Pipelines und Bahn-Kabel dokumentieren die Verletzlichkeit kritischer Infrastruktur. Bemühungen, das digitale Rückgrat Europas zu schützen, kommen zu spät kommt und sind nicht ausreichend. Das Centrum für Europäische Politik (cep) fordert deshalb eine europäische Clean Cable-Kampagne. Zudem sollen Knotenpunkte militärisch überwacht und bestehende Initiativen beschleunigt werden.

- Europas Abhängigkeit von nicht-europäischen datenführenden Tiefseekabeln stellt ein sicherheitspolitisches Risiko dar. Diese **Verwundbarkeit** kennen Experten schon lange. Weniger bekannt ist, dass nicht alle militärische Datenflüsse auf Satelliten ausgelagert werden können, etwa die Steuerung von Drohnen in Echtzeit.
- Gleichwohl **mangelt es an konkreten und schnellen europäischen Maßnahmen**, um resiliente Netze, eine widerstandsfähige Backbone-Infrastruktur und sichere Unterseekabel zu gewährleisten. Die EU sollte künftig eine **wesentliche Koordinierungsrolle** übernehmen, um den Schutz digitaler Infrastruktur zu verbessern.
- Das cep fordert ein europäisches **Clean Cable-Investitionsprogramm** und **sofortigen militärischen Schutz.** Dies soll sicherstellen, dass kritische Unterseekabel nicht angezapft oder sabotiert werden. Zusätzlich sind eine **raschere Umsetzung bestehender Kommissionspläne** zu kritischer Infrastruktur und Sattelitenkommunikation sowie eine **konsequente Verschlüsselung** notwendig, um sensible Datenflüsse besser zu schützen.

Inhaltsverzeichnis

1 Das Rückgrat der digitalen Welt ist in Gefahr 3

2 Aktuelle EU-Initiativen und ihre Mängel..... 4

3 Lehren aus der Vergangenheit 6

4 Fazit und Forderungen..... 9

Abbildungsverzeichnis

Abb. 1: Die westliche Internet-Infrastruktur. 3

1 Das Rückgrat der digitalen Welt ist in Gefahr

Auf den ersten Blick sieht es aus wie das U-Bahn-Netz einer modernen Großstadt – aber es handelt sich um das weltweite Geflecht aus Ozean-Glasfaserkabeln, die das „Rückgrat“[1] des digitalen Datenverkehrs bilden (Abb. 1). Diese Kabel erlauben, dass Europäer reibungslos ihrer Arbeit am Computer nachgehen, Nachrichten konsumieren und mit ihren Bekannten in Kontakt bleiben können. Traditionell im Aufgabenbereich klassischer Telekommunikationsunternehmen angesiedelt, ist deren Verlegung mittlerweile auch in den Fokus von ausländischen Digitalvorreitern wie Google oder Huawei sowie von Militär- und Sicherheitsexperten gerückt.[2] Was passiert, wenn diese kritische digitale Infrastruktur wegbricht, kann man erahnen, wenn man „Inmitten der Nacht“ in die Hand nimmt. Der 2020 veröffentlichte Gesellschaftsroman von Rumaan Alam deutet die rasant um sich greifende Panik plastisch an, die sich aus dem Verlust von Internet- oder Handyempfang ergeben würde.[3] Die Ereignisse der letzten Wochen – von den Nord Stream Leaks bis zum Sabotage-Akt gegen die Deutsche Bahn – zeigen, dass ein solches Szenario nicht länger Fiktion bleiben muss.

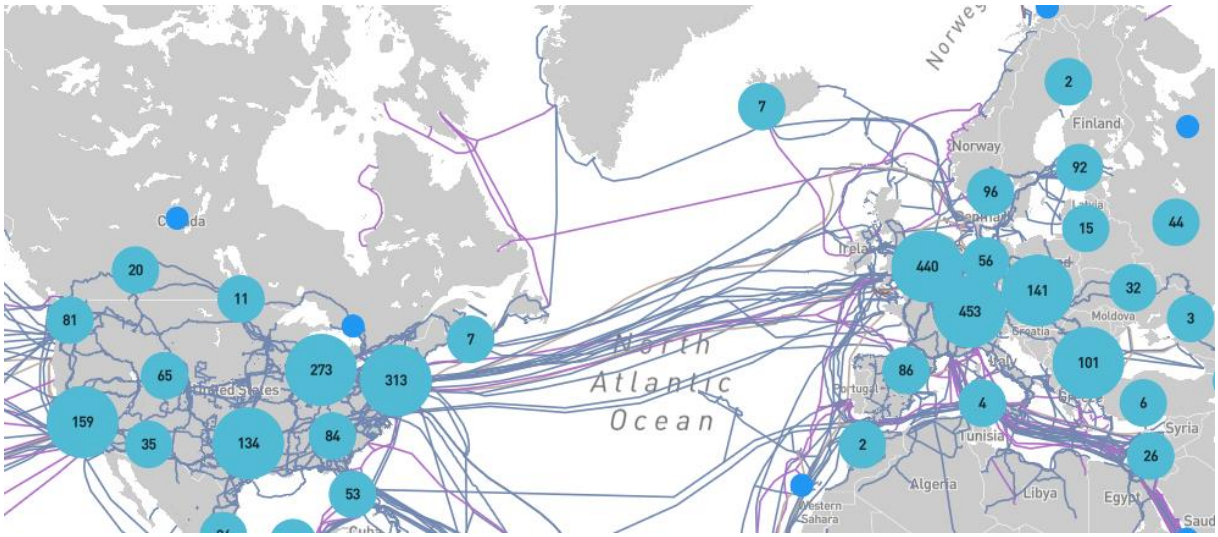


Abb. 1: Die westliche Internet-Infrastruktur.

Bemerkung: Rechenzentren als blaue Kreise abgebildet, Tiefseekabel als Linien (blau = aktiv; lila = Projekt). Quelle: Screenshot von Infrapedia mit eigener Datenauswahl (Stand: 13. Oktober 2022).

Entsprechende Meldungen von gerissenen Kabeln tauchten in den letzten Tagen vermehrt auf und stoßen durch die geopolitischen Spannungen mit Russland auf erhöhte Sensibilität. So wurden in der Nacht zum 19. Oktober französische Glasfaserkabel in der Nähe von Marseille an mindestens drei Stellen gezielt durchtrennt.[4] Das unterbrach den internationalen Informationsfluss, da Marseille eine wichtige Datendrehscheibe ist. Am Tag darauf wurde bekannt, dass zwei Unterseekabel nördlich von Schottland gleichzeitig beschädigt sind – mit der Folge, dass die Bewohner der Shetlandinseln nicht auf das Internet zugreifen oder Notanrufe per Mobilfunk absetzen konnten.[5]

---

1 Boie, J. / Frederik Obermaier, F. (2013), Rückgrat des weltweiten Datenverkehrs, SZ 4.8.2013, https://www.sueddeutsche.de/digital/infrastruktur-des-internets-rueckgrat-des-weltweiten-datenverkehrs-1.1737792.

2 Hummel, T. / Karon, J. (2022), Das Geschäft mit Tiefseekabeln, SWR2 16.6.2022.

3 Alam, R. (2022), Inmitten der Nacht, btb Verlag: Deutsche Erstausgabe 18.10.2021.

4 Ermert, M. (2022), Frankreich: Anschlag auf Glasfaserkabel, Heise Online 20.10.2022, https://www.heise.de/news/Frankreich-Anschlag-auf-Glasfaserkabel-bremst-internationalen-Datenverkehr-aus-7315563.html.

5 Holland, M. (2022), Zwei Unterseekabel beschädigt, Heise online 20.10.2011, https://www.heise.de/news/Zwei-Unterseekabel-beschaedigt-Shetlandinseln-vom-Internet-abgeschnitten-7315534.html.

Prinzipiell ist das Reißen von Seekabeln und insbesondere an Land verlegter Kabel durchaus keine Seltenheit, ohne dass dafür geopolitische Hintergründe vorliegen oder daraus schwerwiegende Folgen resultieren. Die Agentur der Europäischen Union (EU) für Cybersicherheit gibt einen jährlichen Bericht über größere Vorfälle im Bereich der Telekommunikationssicherheit heraus, der für das vergangene Jahr 168 Vorfälle listet, die von nationalen Behörden aus 26 EU-Mitgliedstaaten und 2 EFTA-Ländern eingereicht wurden. Die meisten dieser Risse in der digitalen Infrastruktur gehen auf menschliche Unfälle wie Bauarbeiten, natürliche Phänomene wie Feuer oder andere zufällige Externalitäten zurück und haben lediglich lokale Auswirkungen, d.h. sie betreffen nur einige tausende Internetnutzer.[6] Gerade einmal 5 Prozent der Vorfälle wurden als böswillige Handlungen klassifiziert, das entspricht 73 Vorfällen im Laufe von über 11 Jahren.[7] Allerdings gibt es Hinweise darauf, dass die Datenlage unvollständig ist[8] und der sich gerade rasant ändernde geopolitische Kontext zu einer neuen Sicherheitsbewertung von strategischen Kabeln führen wird.

Die Debatte ist in den letzten Tagen mit voller Wucht auf deutscher und europapolitischer Ebene angekommen. Es gibt Befürchtungen von Bundestagsabgeordneten, dass Russland auch Angriffe auf deutsche kritische Infrastruktur plant.[9] Schon bei ihrem informellen Treffen des Europäischen Rates am 7. Oktober 2022 erörterten die Staats- und Regierungschefs der EU, neben den drängenden Fragen der Energiepreiskrise und der Unterstützung der Ukraine, den Schutz kritischer Infrastrukturen.[10] Frankreichs Präsident Macron forderte hierbei eine gemeinsame europäische Strategie. Auch die Bekämpfung von russischen oder iranischen Cyberangriffen, so Macron, mache ein starkes europäisches Vorgehen unerlässlich. Drei Tage später verkündete EU-Kommissionspräsidentin Ursula von der Leyen beim Digitalgipfel in Tallinn, dass die EU mehr in vertrauenswürdige Konnektivität investieren wolle.[11] Folgen diesen Worten auch Taten zum Schutz des digitalen Datenverkehrs auf dem Kontinent? Und falls ja, kommen diese noch rechtzeitig?

2 Aktuelle EU-Initiativen und ihre Mängel

Da weit über 95 Prozent des weltweiten Datenverkehrs durch die Meere verläuft, geht die wohl gravierendste Gefahr für Europas digitale Infrastruktur von einer Sabotage bestimmter Tiefseekabel aus. Hier rächt sich jetzt Europas weitgehende Abhängigkeit von ausländischen Anbietern. In ihrer Talliner Grundsatzrede erwähnte von der Leyen das transatlantische EllaLink-Kabel, das Europa mit Lateinamerika verbindet, und lobte das neue Glasfaserkabel, das im Rahmen der Global Gateway Strategie der EU unter dem Schwarzen Meer verlegt wird. Global Gateway ist die vor rund einem Jahr ausgerufene europäische Antwort auf die chinesische Belt and Road Initiative und verspricht bis zu 300 Milliarden Euro an Investitionen, um Europa krisenfester zu machen – unter anderem durch eine stärkere und

---

6 ENISA (2022), Telecom Security Incidents 2021. Annual Report, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021, S. 13.

7 ENISA (2022), Telecom Security Incidents 2021. Annual Report, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021, S. 22.

8 Ermert, M. (2022), Missing Link: Angriffe auf Backbones, Heise Online 29.05.2022, https://www.heise.de/hintergrund/Missing-Link-Informationsgesellschaft-Wie-sicher-sind-die-Glasfaserkabel-7123783.html?seite=all.

9 Z.B. Roderich Kiesewetter, zitiert in: „Wir sind viel zu passiv.“, Welt Video-Interview 12.10.2022, https://www.welt.de/politik/ausland/video241552891/Ukraine-Roderich-Kiesewetter-zu-den-Angriffen-auf-kritische-Infrastruktur.html.

10 Anghel, Z. (2022), Outcome of the European Political Community and European Council meetings in Prague on 6-7 October 2022, EPRS 11.10.2022, https://epthinktank.eu/2022/10/11/outcome-of-the-european-political-community-and-european-council-meetings-in-prague-on-6-7-october-2022/.

11 Von der Leyen, U. / Kallas, K. (2022), Ein entscheidender Moment der Wahrheit, Gastbeitrag t-online 8.10.2022, https://www.t-online.de/nachrichten/ausland/eu/id_100063020/neue-eu-strategie-diese-lehren-koennen-wir-aus-dem-ukraine-krieg-ziehen.html.

diversifizierte digitale Vernetzung. Zudem gibt es anonyme Hinweise darauf, dass die Kommission ein 14.000 Kilometer langes Glasfaserkabel mitfinanzieren möchte, das Skandinavien und Irland über die Arktis mit Japan verbinden würde.[12] Die geplanten Investitionen sind zu begrüßen, da sie die Abhängigkeit von terrestrischen Kabeln, die Russland durchqueren, verringern. Außerdem bilden sie eine Alternative zur Volksrepublik China, die mit ihrem 12.000 Kilometer langen, zwischen Europa und Asien verlaufenden Unterseekabel „Peace“ und ihrer 5G-Technologie mittlerweile kräftig beim Ausbau der hiesigen Digitalinfrastruktur mitmischt – um letztlich Daten europäischer Bürger abzuhören und Verhandlungsmacht zu gewinnen, so die Befürchtung.[13] Zusätzliche europäische Kabel schützen nicht nur vor Abhängigkeiten und Datenklau, sondern erhöhen durch Diversifizierung auch die Resilienz der digitalen kritischen Infrastruktur Europas.

Allerdings ist bislang nur ein kleiner Anteil der Global Gateway Strategie für die Verbesserung dieser Situation angedacht: Die von der Kommission am 12. Oktober veröffentlichte Aufforderung zur Einreichung von Vorschlägen im Rahmen der „Connecting Europe“ Fazilität beziffert 277 Millionen Euro für sichere, schnelle und hochleistungsfähige Netze, Backbone-Infrastrukturen und Unterseekabel.[14] Das ist zu wenig. Zudem läuft die Bewerbungsfrist weit in das kommende Jahr hinein, bis zum 23. Februar 2023. Insgesamt zeigt eine vom Unterausschuss für Sicherheit und Verteidigung des EU-Parlaments in Auftrag gegebene Durchsicht relevanter EU-Strategien, dass Kabel- und andere Meeres-Infrastrukturen zwar öfter genannt werden, es jedoch kaum konkrete Maßnahmen gibt, um tatsächlichen Schutz zeitnah zu erzeugen.[15] Es bräuchte daher ein schlagkräftiges Instrumentarium analog zur 5G Cybersecurity Toolbox der Kommission, die aufbauend auf einer EU-weit koordinierten Risikobewertung strategische und technische Schlüsselmaßnahmen für die Kommission und/oder die Mitgliedstaaten entwickelt hat. Auf Unionsebene handelt es sich dabei konkret z.B. um eine verstärkte Überprüfung ausländischer Direktinvestitionen, handelspolitische Schutzinstrumente, eine rigorose Anwendung des Wettbewerbsrechts sowie die Koordinierung von Normierungen, sicherheitspolitischen Zielen und Zertifikaten. Allerdings zeigt die bislang schleppende Implementierung dieser Toolbox, wie langwierig ein Umbau digitaler Infrastrukturen trotz detaillierter Pläne und Rechtsrahmen sein kann.[16]

Mehr Geld und Handlungsspielraum wäre theoretisch verfügbar, wenn datenintensive Plattformen zur Finanzierung der digitalen Netze verpflichtet würden, so wie in der aktuellen Debatte um das künftige Abrechnungsmodell der EU-Telekommunikationsinfrastruktur vorgeschlagen wurde.[17] Auch wenn aus ordnungspolitischer Perspektive grundlegende Probleme mit einem solchen „Sender Party Pays“-Modell bestehen, ist schon heute Fakt, dass eine zunehmende Anzahl der rund 500 weltweit liegenden Tiefseekabel von Big Tech-Konzernen finanziert werden, während die wichtigsten Beteiligungen der

---

[12] Bertuzzi, L. (2022), EU visiert arktisches Internetkabel zur Verbindung Europas mit Asien an, Euractiv 14.10.2022, https://www.euractiv.de/section/innovation/news/eu-erwaegt-arktisches-internetkabel-zur-verbindung-europas-mit-asien/.

[13] Anonym (2022), Die Infrastruktur des Internets, LeitzCloud 6.1.2022, https://leitz-cloud.com/internetkabel.

[14] https://digital-strategy.ec.europa.eu/de/news/launch-new-calls-proposals-budget-eu277-million-support-investments-digital-connectivity (Abruf: 18.10.2022).

[15] Sawall, A. (2022), Europäische Seekabel sollen militärisch geschützt werden, Golem.de 30.9.2022, https://www.golem.de/news/europaparlament-europaeische-seekabel-sollen-militaerisch-geschuetzt-werden-2209-168655.html.

[16] NIS Cooperation Group (2020), Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. Für die weiteren Fortschritte seit Publikation dieses Berichtes, siehe: https://5gobservatory.eu/5g-cybersecurity-toolbox-implementation/ (Abruf: 18.10.2022).

[17] Bertuzzi, L. (2022), Telekommunikation: Experten sprechen sich gegen Kostenbeteiligung großer Plattformen aus, Euractiv 12.10.2022, https://www.euractiv.de/section/innovation/news/telekommunikation-experten-sprechen-sich-gegen-kostenbeteiligung-grosser-plattformen-aus/.

Deutschen Telekom auf die Jahrtausendwende zurückgehen.[18] Das Beispiel Afrikas zeigt, dass die Einbindung von marktmächtigen Akteuren wie Google oder Microsoft zwar zu schnellen Verbesserungen der Infrastruktur, aber ebenso zu drohenden Abhängigkeiten führt. Der entsprechende Vorschlag der Kommission zum Abrechnungsmodell der EU-Telekommunikationsinfrastruktur ist jedenfalls nicht im Arbeitsprogramm für 2023 gelistet; lediglich eine Konsultation zum Thema ist für Anfang des nächsten Jahres vorgesehen. Hierbei sollten dann nicht nur die möglichen Auswirkungen auf Innovation und Wettbewerb – wie aktuell geplant – studiert werden, sondern vorrangig sicherheitspolitische Aspekte.

Neben der Global Gateway Strategie einigten sich Rat und Europäisches Parlament prinzipiell auf eine Richtlinie über die Resilienz kritischer Einrichtungen, die auf einen bereits 2020 vorgeschlagenen Kommissionsentwurf zurückgeht.[19] Diese strebt an, die Anfälligkeit kritischer Einrichtungen, unter anderem in den Bereichen Informationstechnik und Telekommunikation, zu verringern.[20] Dieser Vorschlag komplementiert die Kommissionsvorschläge für eine Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS 2), die die Betreiber von Internet-Knoten explizit auflistet, und die Verordnung über die Betriebsstabilität digitaler Systeme (DORA), die die IT-Sicherheit von Finanzunternehmen in Krisen stärken soll.[21] Alle drei neuen Rechtsakte müssen erst noch von den Mitgliedstaaten koordiniert umgesetzt werden. Wie von EU-Innenkommissarin Ylva Johansson am 18. Oktober gefordert,[22] müssen die Vorbereitungsarbeiten, auch auf Seiten der Mitgliedsstaaten, beschleunigt werden, um diese neuen Regeln schnellstmöglich anwenden zu können.

Zu berücksichtigen ist, dass die Kompetenzen der EU in der Sicherheitspolitik eng umrissen sind und das Subsidiaritätsprinzip auch hier seinen Wert hat. So weiß ein Mitgliedsstaat potenziell besser als die supranationale Kommission, welche Kabel am besten wie zu schützen sind. Gleichzeitig sind kritische digitale Infrastrukturen in Europa oft eng vernetzt, sodass die gegenseitige Abhängigkeit eine besondere Rolle der EU bei grenzüberschreitenden Einrichtungen und deren Schutz durchaus begründet. Insgesamt verdeutlicht die Übersicht, dass die Initiativen der EU dennoch deutlich zu spät kommen und suggeriert, dass man lange Zeit zu naiv war.

3 Lehren aus der Vergangenheit

Prinzipiell ist Europas digitale Verwundbarkeit schon seit vielen Jahren bekannt. Die Idee, Kabel abzuhören, geht auf den Kalten Krieg zurück und schon während des Ersten Weltkrieges wurden Seekabel gezielt gestört.[23] Im Jahr 2015 vermeldeten US-Militärkreise, dass russische U-Boote und Schiffe vermehrt in der Nähe von Unterseekabeln aktiv seien und äußerten die Befürchtung, Russland könne die

[18] Vgl. die Auswertung von TeleGeography-Daten in: Kirsch, S. (2018), Google und Co koppeln sich ab, WirtschaftsWoche 8.2.2018, https://www.wiwo.de/technologie/digitale-welt/tiefseekabel-google-und-co-koppeln-sich-ab/20916398.html.

[19] Kommission (2020), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen, COM(2020) 829 final, Brüssel, den 16.12.2020.

[20] Internet-Unterseekabel werden nicht spezifisch genannt, da Kabel keine kritischen Einrichtungen per se sein können.

[21] Eckhardt, P. (2022), NIS-2-Richtlinie, cepAdhoc 13.09.2022, https://www.cep.eu/eu-themen/details/cep/nis-2-richtlinie-neue-eu-vorgaben-zur-cybersicherheit-cepadhoc.html; Anzini, M. / Eckhardt, P. (2022), Digitale Betriebsstabilität von Finanzunternehmen, cepAnalyse 14.06.2021, https://www.cep.eu/eu-themen/details/cep/digitale-betriebsstabilitaet-von-finanzunternehmen-cepanalyse-zu-com2020-595.html.

[22] Kommission (2022), Kommission ruft Mitgliedstaaten zu besserem Schutz kritischer Infrastrukturen auf, Pressemitteilung 18.10.2022, https://germany.representation.ec.europa.eu/news/kommission-ruft-mitgliedstaaten-zu-besserem-schutz-kritischer-infrastrukturen-auf-2022-10-18_de.

[23] Grunert, F. (2012), Drohnen und SWIFT unter Wasser – Die Relevant von Unterseekabeln, sicherheitspolitik-blog 6.11.2012, https://d-nb.info/1063995795/34.

Kabel durchtrennen, um verfeindete Nationen vom Internet abzuschneiden.[24] Zwei Jahre zuvor zeigten die Enthüllungen des NSA-Whistleblowers Edward Snowden, dass auch die US-Geheimdienste – neben Kooperationen mit Betreibern und dem Hacken von Systemen – die weltweiten Glasfaserleitungen direkt anzapfen können.[25] Und schon 2010 hatte Wikileaks eine geheime Liste wichtiger Infrastrukturen veröffentlicht, die aus Sicht der USA vor Terrorangriffen geschützt werden müssten und dabei die ostfriesische Stadt Norden sowie Sylt, wo bis heute die wichtigen Unterseekabel SEA-ME-WE 3 beziehungsweise AC-1 ankommen, explizit nannte.[26] Aktuell gibt es sechzehn Unterseekabel, die Irland berühren und deren Unterbrechung den europäischen Internetverkehr für mehrere Stunden oder sogar Tage kritisch treffen würde.[27]

Russland hat bereits seit einigen Jahren die Möglichkeit, diese kritische digitale Infrastruktur jederzeit zu beeinträchtigen. Deutsche Geheimdienstexperten sprechen nun offen aus, dass die russische Armee über Unterseeboote und Einheiten verfügt, „deren originäre Aufgabe es ist, Kommunikation über Unterseekabel auszuforschen, Leitungen zu manipulieren und gegebenenfalls auch irreparabel zu schädigen."[28] Gemeint ist wohl das russische Schiff Yantar, dass regelmäßig seine genaue Reiseroute durch Deaktivieren des Tracking-Signals verschleiert und über zwei U-Boote verfügen soll, die auf das Anzapfen und Durchtrennen von Tiefsee-Glasfaserkabeln ausgerichtet sind.[29] Wenig überraschend wurde der Ausfall des wichtigen Glasfaserkabels zwischen dem arktischen Archipel und dem norwegischen Festland Ende letzten Jahres auf russische Spionage zurückgeführt,[30] auch wenn eine sichere Schlussfolgerung (bislang) nicht gezogen werden kann. Experten des Atlantic Council, einer US-Denkfabrik, warnten schon kurz vor dem Ukraine-Krieg, dass das russische Militär zukünftig eines der europäischen Unterseekabel angreifen sowie Einrichtungen von Internetdienstanbietern und Internetaustauschpunkten physisch beschädigen oder von der Stromversorgung abtrennen könnte.[31]

Selbst wenn es der EU gelingen sollte, ausreichend eigene Kabel und andere kritische Digital-Infrastruktur schnell zu verlegen, um Redundanz und damit Resilienz zu schaffen, bleibt deren Schutz eine schwierige Angelegenheit. Zwar bemühen sich die Netzbetreiber bereits enorm darum, ihre Glasfaserstrecken und Kabelstationen durch eine spezifische Gestaltung der Kabel und Schächte und den Einsatz spezialisierter Sensorik und Monitoring widerstandsfähiger zu machen.[32] Doch ein umfassender Schutz insbesondere von Tiefseekabeln, so Experten, würde enorme Investitionen in die Überwachung, U-

---

[24] Gruber, A. (2015), Wenn die Tiefseekabel reißen, SZ 26.10.2015, https://www.sueddeutsche.de/digital/datenverbindungen-im-meer-wenn-die-tiefseekabel-reissen-1.2708619.

[25] Meister, A. (2013), Glasfaserkabel und Spionage-U-Boote, Netzpolitik.org 20.6.2013, https://netzpolitik.org/2013/glasfaserkabel-und-spionage-u-boote-wie-die-nsa-die-nervenzentren-der-internet-kommunikation-anzapft/.

[26] DPA (2010), Wikileaks veröffentlicht Liste potenzieller Terrorziele, Stern 6.12.2010, https://www.stern.de/politik/ausland/enthuellungsplattform-wikileaks-veroeffentlicht-liste-potenzieller-terrorziele-3873034.html. Das Dokument ist hier einsehbar: https://wikileaks.org/plusd/cables/09STATE15113_a.html (Abruf: 18.10.2022).

[27] Sherman, J. (2022), Cord-cutting, Russian style, Atlantic Council 31.1.2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/.

[28] Zitiert nach: Sawall, A. (2022), Sicherheitspolitiker warnen vor Angriffen auf Seekabel, Golem.de 4.10.2022, https://www.golem.de/news/geheimdienst-sicherheitspolitiker-warnen-vor-angriffen-auf-seekabel-2210-168688.html.

[29] FutureZone, Russisches Spionageschiff in der Karibik unterwegs, 08.12.2019, https://futurezone.at/netzpolitik/russisches-spionageschiff-in-der-karibik-unterwegs/400697507

[30] Staalesen, A. (2022), 'Human activity' behind Svalbard cable disruption, The Barents Observer 11.2.2022, https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption.

[31] Sherman, J. (2022), Cord-cutting, Russian style, Atlantic Council 31.1.2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/.

[32] Ermert, M. (2022), Missing Link: Angriffe auf Backbones – Wie gut sind Glasfaserkabel geschützt?, Heise Online 29.05.2022, https://www.heise.de/hintergrund/Missing-Link-Informationsgesellschaft-Wie-sicher-sind-die-Glasfaserkabel-7123783.html?seite=all.

Boote und Fregatten erfordern.[33] Während Großbritannien mittlerweile ein zweites Kriegsschiff für den Schutz von Seekabeln in Auftrag gegeben hat,[34] verfügen die EU-Mitgliedsstaaten über keine derartigen Schiffe. Erst im Juni identifizierte eine interne Studie für das Europaparlament zahlreiche „sehr verwundbare" Stellen der europäischen Glasfaser-Seekabel und forderte militärischen Schutz.[35]

Neben dem physischen Schutz der Kabel ist deren Cybersicherheit ein zunehmend wichtiges Thema: Bei den im Zeitraum zwischen 2012 und 2021 bekannt gewordenen böswilligen Handlungen gegenüber europäischer Telekommunikationssicherheit handelte es sich nur bei rund einem Drittel um physische Schäden, wie beispielsweise durch Brandstiftung oder absichtliches Durchtrennen von Kabeln erzeugt, während 64% dieser Störungen auf sogenannte Denial-of-Service(DoS)-Angriffe zurückgeführt werden konnten.[36] Mit einem DoS-Angriff können nicht nur einzelne Websites, sondern ganze Netze zum Zusammenbruch gebracht werden, indem sie gezielt mit extrem vielen Anfragen bombardiert werden. Im Mai dieses Jahres hatte die Bundesregierung zugegeben, dass solche DoS-Angriffe auf deutsche Behörden und Ministerien durchgeführt worden seien, zu denen sich später die russische Hacker-Gruppe Killnet bekannte.[37] Allerdings ist zu betonen, dass sich im Rahmen des Ukraine-Krieges die anfangs befürchteten „Cyber-Pearl Harbor"-Bedrohungsszenarien bislang nicht erfüllt haben.[38]

Für besonders sensible Daten im militärischen Bereich ist die Satellitenkommunikation dem Kabeltransfer per Land oder See grundsätzlich vorzuziehen, doch auch hier lässt sich eine starke potentielle Verwundbarkeit feststellen. Vor einigen Tagen meldete der Abteilungsleiter Sicherheit des Bundeverbandes der deutschen Industrie, dass die europäische Satellitenkommunikation im Vergleich zu den Seekabeln sogar noch anfälliger für Angriffe sei.[39] Es ist daher zu begrüßen, dass das Europäische Parlament jüngst den Plan der Kommission für eine sichere Satellitenkommunikation gebilligt hat (der Trilog soll Ende Oktober stattfinden)[40] – aber die Zeit drängt, wie nicht zuletzt die Eskapaden um Elon Musks diskretionäre Entscheidungen über die Nutzung seines Satellitensystems Starlink durch das ukrainische Militär illustrieren. Doch selbst wenn man von den langen Vorbereitungszeiten für das Senden von Satelliten in den Orbit absieht, sind solche Systeme kein Allheilmittel. Schon seit den 1990er Jahren sind Fälle publik, in denen sich Kriminelle Zugang zur Satellitenkommunikation oder sogar deren Flugbahn verschaffen konnten. Zudem ist wenig bekannt, dass sich nicht alle militärisch relevanten Datenströme von Unterseekabeln auf Satellitenübertragung verschieben lassen, da z.B. die Steuerung

[33] Gsteiger, F. (2021), Tiefseekabel, SRF 15.8.2021, https://www.srf.ch/news/international/kuenftige-ziele-im-cyber-krieg-tiefseekabel-sehr-verletzlich-und-wie-geschaffen-fuer-sabotage.

[34] Anonym (2022), Protecting seabed infrastructure, Navy Lookout 3.10.2022, https://www.navylookout.com/protecting-seabed-infrastructure-uk-multi-role-ocean-surveillance-ship-to-be-in-service-by-2023/.

[35] Zitiert nach: Sawall, A. (2022), Sicherheitspolitiker warnen vor Angriffen auf Seekabel, Golem.de 4.10.2022, https://www.golem.de/news/geheimdienst-sicherheitspolitiker-warnen-vor-angriffen-auf-seekabel-2210-168688.html.

[36] ENISA (2022), Telecom Security Incidents 2021. Annual Report, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021, S. 22.

[37] Anonym (2022), Bundesregierung bestätigt Hacker-Angriffe, Tagesschau 9.5.2022, https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html.

[38] Schulze, M. (2022), Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022, Stiftung Wissenschaft und Politik 02.05.2022 (Ukraine-Analysen Nr. 267), S. 2-13.

[39] Sawall, A. (2022), Industrieverband hält Satellitennetz für verwundbarer, Golem.de 6.10.2022, https://www.golem.de/news/bdi-industriebverband-haelt-satellitennetz-fuer-verwundbarer-2210-168758.html.

[40] Kabelka, L. (2022), Grünes Licht für EU-Programm für sichere Konnektivität, Euractiv 13.10.2022, https://www.euractiv.de/section/innovation/news/parlamentarischer-hauptausschuss-genehmigt-eu-programm-fuer-sichere-konnektivitaet/.

von Drohnen eine Echtzeitübertragung und hohe Bandbreite voraussetzt.[41] Das ist mit Satellitenübertragung nicht gewährleistet, da diese noch eine zu hohe Latenz[42] aufweist.

Insgesamt zeigen diese Beispiele, dass der Schutz kritischer Kabel letztlich nicht von den teils privaten Betreibern alleine bewältigt werden kann, sondern im aktuellen geopolitischen Kontext als eine entscheidende hoheitliche Aufgabe der europäischen Mitgliedstaaten angesehen werden sollte, die nach koordinierten, raschen Investitionen verlangt. Auch wenn die EU über begrenze Kompetenzen in diesem Bereich verfügt, muss sie mit ihrer Koordinationsrolle und dem Bereitstellen von ausreichend Investitionskapital ein starkes Signal senden, da der Schutz der kritischen digitalen Infrastruktur nur für die EU als Ganzes gelingen kann. Die digitale Kette ist nur so stark wie ihr schwächstes Glied. Auch aus diesem Grund wäre eine engere Verzahnung mit US-Initiativen der letzten Jahre dringend geboten. Da ein absoluter physischer und digitaler Schutz der Daten-Infrastruktur kaum gewährleitet werden kann, ist schließlich eine konsequente Verschlüsselung aller relevanten Informationen unerlässlich.

4 Fazit und Forderungen

Auch wenn aktuelle EU-Initiativen die sicherheitspolitische Relevanz der digitalen Infrastruktur zwar zunehmend anerkennen, mangelt es an konkreten Maßnahmen, die rechtzeitig gestartet wurden, um Schutz zu gewährleisten. Die für die Global Gateway Strategie eingeplanten Mittel, die neben Digitalem auch Projekte in Klima und Energie, Verkehr, Gesundheit sowie Bildung und Forschung finanzieren möchten, müssen daher dringend auf den Schutz kritischer Digitalinfrastrukturen ausgerichtet werden und diese priorisieren. Angelehnt an die 2020 gestartete Aktion „Clean Cable“ der US-amerikanischen Regierung[43] würde ein europäisches Clean Cable Investitionsprogramm und sofortiger militärischer Schutz sicherstellen, dass kritische Unterseekabel, die den Kontinent mit dem Internet verbinden, nicht angezapft oder sabotiert werden können. Zusätzlich gilt es, die Verabschiedung und Umsetzung bestehender Kommissionspläne für kritische Infrastrukturen und eine sichere Satellitenkommunikation dramatisch zu beschleunigen sowie eine konsequente Verschlüsselung aller relevanten Daten durchzusetzen, um besonders sensible Daten besser zu schützen. Dafür ist die von der Kommission am 18. Oktober beanspruchte Koordinationsrolle unerlässlich. Denn ohne ein zügiges, entschlossenes und gemeinsames Handeln der Europäer droht, dass sich Rumaan Alams Dystopie allzu bald verwirklicht.

---

[41] Grunert, F. (2012), Drohnen und SWIFT unter Wasser – Die Relevant von Unterseekabeln, sicherheitspolitik-blog 6.11.2012, https://d-nb.info/1063995795/34.

[42] Latenz beschreibt in diesem Zusammenhang die Verzögerungszeit, die Datenpakete von der Quelle bis zum Ziel benötigen.

[43] Moss, S. (2020), US 'Clean Network' program seeks to build clouds, cables, and apps free of China, DCD 6.8.2020, https://www.datacenterdynamics.com/en/news/us-clean-network-program-seeks-build-clouds-cables-and-apps-free-china/.

Centrum für Europäische Politik
FREIBURG | BERLIN

Autor:

Dr. Anselm Küsters, LL.M., Fachbereichsleiter Digitalisierung und neue Technologien
kuesters@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin
Tel. + 49 761 38693-0

Das **Centrum für Europäische Politik** FREIBURG | BERLIN, das **Centre de Politique Européenne** PARIS, und das **Centro Politiche Europee** ROMA bilden das **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Das gemeinützige Centrum für Europäische Politik analysiert und bewertet die Politik der Europäischen Union unabhängig von Partikular- und parteipolitischen Interessen in grundsätzlich integrationsfreundlicher Ausrichtung und auf Basis der ordnungspolitischen Grundsätze einer freiheitlichen und marktwirtschaftlichen Ordnung.