Maritime kritische Infrastrukturen: strategische Bedeutung und geeignete Schutzmaßnahmen

Voelsen, Daniel (Ed.)

SWP

SWP-Studie

Daniel Voelsen (Hg.)

Maritime kritische Infrastrukturen

Strategische Bedeutung und geeignete Schutzmaßnahmen

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

SWP-Studie 3
Februar 2024, Berlin

- Im maritimen Raum findet sich eine Vielzahl von Infrastrukturen, die von zentraler Bedeutung für die globalen Energiebeziehungen, das Netz des weltweiten Handels mit Nahrungs- und Düngemitteln und nicht zuletzt den Datenaustausch im Internet sind.
- Schon immer war das Meer Austragungsort geopolitischer Konflikte. Hinzu kommen nun hybride Bedrohungen, bei denen die Akteure die Weite des maritimen Raums nutzen, um im Verborgenen zu agieren.
- Zugleich werden maritime Infrastrukturen in Zukunft noch an Bedeutung gewinnen; so wird zu beobachten sein, welche neuen Infrastrukturen durch neuartige Nutzungen des maritimen Raums wie den Tiefseebergbau oder die Speicherung von Kohlenstoff entstehen.
- Einige maritime Infrastrukturen haben eine derart herausgehobene gesellschaftliche Bedeutung, dass sie als *kritische* Infrastrukturen verstanden und entsprechend besonders geschützt werden sollten. Zugleich gilt es, eine pauschale »Versicherheitlichung« des maritimen Raums zu vermeiden.
- Der hohe Grad der Vernetzung innerhalb Europas führt dazu, dass Infrastrukturen an der Küste eines Landes von besonderer Bedeutung für ganz Europa sein können. Darüber hinaus sind aufgrund der globalen Vernetzung aber auch maritime Infrastrukturen in weiter entfernten Regionen von kritischer Bedeutung für Europa.
- Um maritime Infrastrukturen zu schützen, sollte neben Ansätzen, die auf die Eigenheiten einzelner Einrichtungen oder Sektoren zielen, insbesondere auf Resilienz und Diversifizierung gesetzt werden. Wo dies nicht möglich und die Bedrohung durch staatliche Akteure groß ist, bedarf es ergänzender militärischer Schutzmaßnahmen.

SWP-Studie

Daniel Voelsen (Hg.)

Maritime kritische Infrastrukturen

Strategische Bedeutung und geeignete Schutzmaßnahmen

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 3
Februar 2024, Berlin

SWP-Studien unterliegen einem Verfahren der Begutachtung durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*, sie werden zudem einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/. SWP-Studien geben die Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6372
ISSN (Online) 2747-5115
DOI: 10.18449/2024S03

Inhalt

Maritime kritische Infrastrukturen. Strategische Bedeutung und geeignete Schutzmaßnahmen

Als Gesellschaft nutzen wir Tag für Tag eine Vielzahl von technischen und sozialen Infrastrukturen. Als »kritisch« gelten dabei jene Infrastrukturen, die von besonderer Bedeutung für die Funktionsfähigkeit und das Wohlergehen der Gesellschaft sind. Zum Schutz dieser kritischen Infrastrukturen existiert auf nationaler wie europäischer Ebene ein umfangreiches Regelwerk. In den letzten Jahren hat sich auch die Nato verstärkt den strategischen Herausforderungen zugewandt, die mit dem Schutz solcher Infrastrukturen verbunden sind.

Die Anschläge auf die Gasleitungen Nord Stream 1 und 2 im September 2022 haben allerdings eine dabei bislang in Deutschland wenig beachtete Dimension in den Vordergrund gerückt, nämlich kritische Infrastrukturen im maritimen Raum. Diese sind in mindestens drei Sektoren von besonderer Bedeutung: Energie, Nahrung und Kommunikation. Während jedoch die Diskussion über kritische Infrastrukturen auf dem Festland in Deutschland wie auch auf europäischer Ebene schon weit gediehen ist, steht eine vergleichbar systematische Diskussion über *maritime* kritische Infrastrukturen in Deutschland noch aus.

Zentrale Herausforderungen ergeben sich dabei aus den Eigenheiten des maritimen Raumes. Hierzu zählen dessen enorme Weite und entsprechend auch die geografische Ausdehnung der hier verbauten Infrastrukturen. Abhängig vom Wetter können sie zumindest zeitweise selbst mit modernem Gerät nur schwer zugänglich sein, erst recht, wenn sie sich in großer Tiefe befinden. Darüber hinaus ist der maritime Raum völkerrechtlich durch eine Ausdifferenzierung staatlicher Privilegien und Verantwortlichkeiten in den verschiedenen Meereszonen geprägt; viele maritime Infrastrukturen verlaufen entsprechend durch unterschiedliche Rechtsräume.

Diese Charakteristika des maritimen Raums treffen nun auf eine veränderte Bedrohungslage: Schon immer war das Meer Austragungsort geopolitischer Konflikte. In letzter Zeit ist jedoch zu beobachten, wie neben die offen zur Schau getragene staatliche Präsenz auf und unter dem Wasser der Einsatz hybrider Mittel tritt: So wird die Weite der Meere genutzt, um im Verbor-

genen und noch unterhalb der Schwelle eines offen gewaltsamen Konfliktes zu agieren. Dabei rücken auch maritime Infrastrukturen in den Blick, die privat betrieben werden und in Friedenszeiten primär zivilen Zwecken dienen. Die noch immer nicht aufgeklärte Sprengung der Nord-Stream-Pipelines ist hierfür ein eindrückliches Beispiel.

Aus dieser veränderten Bedrohungslage erwächst ein Klärungsbedarf, der aktuell zu intensiven Debatten auf nationaler Ebene, im Rahmen der EU und auch unter den Partnern in der Nato führt. Die grundlegenden Fragen dabei lauten: Wie lässt sich die strategische Bedeutung maritimer kritischer Infrastrukturen fassen? Und was ist dementsprechend ein angemessenes Verständnis von deren Sicherheit?

Was die bisherige Diskussion über kritische Infrastrukturen in jedem Fall deutlich macht, ist die Notwendigkeit einer Fokussierung bzw. Priorisierung. Es wäre schlichtweg nicht möglich, alle maritimen Infrastrukturen vor gezielten Angriffen zu schützen, und es wäre auch nicht nötig. Die Frage ist vielmehr, welche maritimen Infrastrukturen von besonderer Bedeutung sind und folglich eines besonderen Schutzes bedürfen.

Die vorliegende Studie geht dieser Frage in einem Dreischritt nach: Den Anfang macht eine Klärung der völkerrechtlichen Rahmenbedingungen. Auf diese folgt eine Analyse von drei zentralen Sektoren: Energie, Nahrung und Kommunikation. Im Lichte der Spezifika dieser drei Sektoren wird jeweils untersucht, welche maritimen Infrastrukturen hier aus deutscher und europäischer Sicht als kritisch zu verstehen sind. So entsteht ein differenziertes Bild der Bedrohungslage bzw. des Schutzbedarfs. Die darauffolgenden Beiträge legen dar, welche Möglichkeiten es gibt, auf diesen Schutzbedarf mit zivilen und militärischen Maßnahmen zu reagieren. Im Fokus stehen dabei die Europäische Union, die Nato und nicht zuletzt auch die deutschen Streitkräfte.

Für das Verständnis der strategischen Bedeutung maritimer Infrastrukturen bedarf es eines kontinentaleuropäischen Blicks. Da die Staaten Europas gerade in den hier untersuchten Sektoren so eng miteinander verknüpft sind, lässt sich die Bedeutung einzelner Infrastrukturen oftmals nur erkennen, wenn sie als Elemente europaweit vernetzter Strukturen verstanden werden. Dies gilt aufgrund der geografischen Lage und der im Vergleich kurzen eigenen Küstenlinie insbesondere für Deutschland. Neben fixen physischen Infrastrukturen können dabei auch Seewege oder Schiffe den Charakter von Infrastrukturen erlangen und sollten entsprechend Teil der Diskussion sein. Nicht zuletzt sind, strategisch vorausschauend, bereits jetzt zukünftige Infrastrukturen in den Blick zu nehmen, die zum Beispiel im Bereich von CO_2-Transport- und Speicherungsanlagen oder beim Abbau von Rohstoffen am Meeresgrund entstehen könnten. Für die deutsche Außen- und Sicherheitspolitik ergeben sich daraus drei zentrale Empfehlungen:

- Die Förderung der Diversität und Resilienz von Infrastrukturen ist das effektivste Mittel, um den sich abzeichnenden Bedrohungen zu begegnen. Letztlich zielt dies darauf ab, maritime kritische Infrastrukturen weniger kritisch werden zu lassen. Gerade hier ist eine gesamteuropäische Vorgehensweise notwendig.
- Wo sich die Kritikalität nicht auf diese Weise reduzieren lässt, kann ergänzender militärischer Schutz vor gezielten Angriffen notwendig sein. Im Wesentlichen zielt dieser auf verbesserte Aufklärung und Abschreckung ab. Neben dem Schutz einzelner Anlagen bei konkreten Hinweisen auf Bedrohungen erscheint es sinnvoll, den kontinuierlichen Schutz auf jene Orte an den Küsten Europas zu konzentrieren, an denen mehrere kritische Infrastrukturen zusammenkommen.
- Auch jenseits der europäischen Gewässer finden sich maritime kritische Infrastrukturen, die als Teil globaler Netzwerke von herausgehobener Bedeutung auch für Europa sind, etwa in der Straße von Malakka. Wenngleich hier die direkten Handlungsmöglichkeiten deutlich eingeschränkter sind, liegt es im Interesse Europas, Formen der internationalen Kooperation zu finden, die zum Schutz dieser weiter entfernten Infrastrukturen beitragen. Dies kann von strategischen Dialogen über verstärkten Informationsaustausch bis hin zu gemeinsamen militärischen Maßnahmen reichen. Auszuloten ist zudem, welche Möglichkeiten es gibt, im Rahmen der Entwicklungszusammenarbeit die Sicherheit der maritimen kritischen Infrastruktur von Partnerländern zu erhöhen.

Göran Swistek / Daniel Voelsen

Einleitung

Als Gesellschaft sind wir auf eine Vielzahl von technischen und sozialen Infrastrukturen angewiesen. In der Regel werden diese für so selbstverständlich gehalten, dass sie kaum Aufmerksamkeit erlangen. Seit einigen Jahren gibt es jedoch eine zunehmend intensiv geführte Debatte über die Sicherheit sogenannter kritischer Infrastrukturen. Ein Grund dafür ist wohl der Schreck später Erkenntnis. Von wissenschaftlichen Untersuchungen bis in den Bereich der Unterhaltungsliteratur gab es in den letzten Jahren Warnungen davor, welch weitreichende wirtschaftliche und soziale Folgen zum Beispiel schon ein begrenzter Ausfall der Stromversorgung nach sich ziehen würde. Besondere Aufmerksamkeit haben dabei die Risiken von Cyberangriffen auf vernetzte Infrastrukturen erfahren, was auch erklären dürfte, warum gerade der IT-Sicherheit im Rahmen der bisherigen Vorgaben zum Schutz kritischer Infrastrukturen eine herausgehobene Bedeutung zukommt. Und mehr noch: Während die Bedeutung von Infrastrukturen in einer immer umfassender von Technologie abhängigen Gesellschaft wächst, wurden seit dem Ende des Kalten Krieges die Investitionen in Sicherungsmaßnahmen und Redundanzen zurückgefahren. Öffentlich sichtbar wurde dies etwa durch das kolossale Scheitern des bundesweiten Warntags 2020. Nicht nur versagten damals die digitalen Warnsysteme, vielerorts waren auch Sirenen als analoge Rückfalloption entweder schon lange außer Betrieb genommen worden — oder sie funktionierten schlichtweg nicht.[1]

Hinzu kommt eine neue Bedrohungswahrnehmung, die sich durch den Angriff Russlands auf die Ukraine im Februar 2022 noch verschärft hat. Lange Zeit lag der Fokus der politischen Debatte auf den Gefahren, die von terroristischen Gruppierungen ausgehen. Schon seit einigen Jahren lässt sich jedoch beobachten, dass die Betreiber kritischer Infrastrukturen zum Ziel primär kommerziell motivierter Cyberangriffe werden, sogenannter »Ransomware«-Attacken.[2] Inzwischen sind es aber verstärkt auch wieder Staaten, die in diesem Bereich agieren. Mit Sorge wird etwa beobachtet, dass Russland in der Ukraine ganz gezielt zivile Infrastrukturen angreift. Und entsprechend geschockt reagierte die politische Öffentlichkeit in Deutschland, als im September 2022 die Gasleitungen Nord Stream 1 und 2 durch Sprengungen beschädigt wurden. Nimmt man den europäischen Kontinent in Gänze in den Blick, so fällt auf, dass es in den letzten Jahren eine ganze Reihe verdächtiger Vorfälle gegeben hat, die zur signifikanten Zerstörung oder zumindest zu erheblichen Beeinträchtigungen von Infrastrukturen geführt haben (siehe Abbildung). Die jüngsten Angriffe der Huthi-Milizen auf Handelsschiffe im Roten Meer verdeutlichen besonders drastisch, wie es zu signifikanten Einschränkungen von Seewegen als Teil der maritimen Infrastruktur kommen kann, die zwar geografisch weiter entfernt, für Europa aber dennoch von kritischer Bedeutung sind.

Vor diesem Hintergrund wächst das Bewusstsein für die Bedeutung maritimer kritischer Infrastrukturen, insbesondere in den Bereichen Energieversorgung, Handel mit Nahrungsmitteln sowie globale Kommunikationsnetze. Neben fest installierten Strukturen, wie zum Beispiel Offshore-Windparks, Unterseekabeln oder auch Häfen, geht es dabei auch um Containerschiffe, schwimmende Terminals und eben zentrale Seewege.

Während die Diskussion über kritische Infrastrukturen auf dem Festland in Deutschland wie auch auf europäischer Ebene schon weit gediehen ist, steht eine vergleichbar systematische Debatte über maritime kritische Infrastrukturen in Deutschland noch aus. Dies mag unter anderem der Geografie geschuldet

1 »Bundesweiter Warntag ›fehlgeschlagen‹«, *Tagesschau.de*, 10.9.2020, <https://www.tagesschau.de/inland/warntag-115.html> (eingesehen am 4.9.2023).

2 Matthias Schulze, *Ransomware. Technische, nationale und multilaterale Gegenmaßnahmen*, Berlin: Stiftung Wissenschaft und Politik, August 2021 (SWP-Aktuell 56/2021), doi: 10.18449/2021A56.

Großbritanniens Konzept für den Schutz maritimer kritischer Infrastrukturen

Häfen, Schiffe, marine Energie-Infrastrukturen wie Öl- und Gaspipelines sowie Unterseekabel gelten in Großbritannien als kritische Infrastrukturen. Eine zentrale Rolle bei ihrem Schutz kommt dem Centre for the Protection of National Infrastructure zu, das Risikoeinschätzungen vornimmt und sowohl Regierung als auch Industrie berät. In den letzten Jahren legte die Regierung einen besonderen Fokus auf maritime Sicherheit. Die National Strategy for Maritime Security 2022 betont die Verbesserung des Schutzes maritimer Infrastrukturen infolge der Network and Information Systems Regulations 2018 und sieht eine Überprüfung der Regulierung zum Schutz von Unterseekabeln vor.[a] Im Oktober 2023 wurde mit *Proteus* das erste Multi-Role Ocean Surveillance Ship (MROSS) der Marine in Dienst gestellt. Ein weiteres Schiff ist in Planung.[b]

a UK Secretary of State for Transport, *National Strategy for Maritime Security*, London, August 2022, <https://s3.documentcloud.org/documents/22136535/national-strategy-for-maritime-security-web-version.pdf> (eingesehen am 14.6.2023).
b Peter Felstead, »UK's First Multi-Role Ocean Surveillance Ship Enters Service«, in: *European Security & Defence*, 11.10.2023, <https://euro-sd.com/2023/10/news/34540/first-mross-enters-service/> (eingesehen am 11.1.2024).

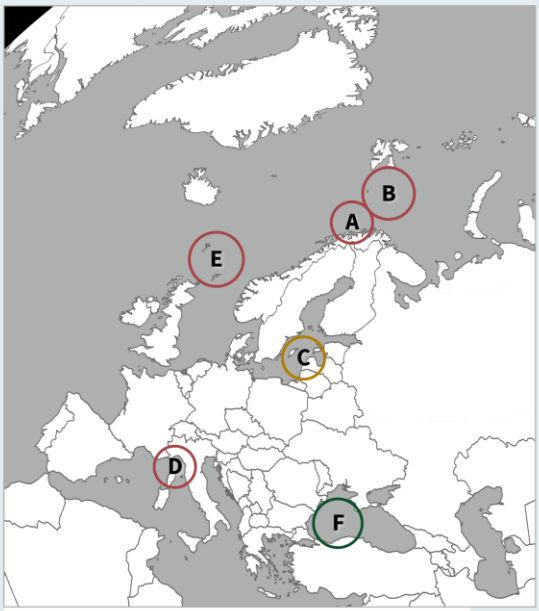
sein: Inselstaaten wie Großbritannien,[3] Japan[4] oder Australien,[5] aber auch Staaten mit langen Küstenlinien wie Finnland,[6] Spanien[7] oder auch die USA[8] haben zum Teil schon vor Jahrzehnten Strategien zum Schutz explizit maritimer kritischer Infrastrukturen umgesetzt und entsprechende Vorkehrungen getroffen.

Mit dem Anschlag auf die Nord-Stream-Pipelines hat diese Diskussion nun auch Deutschland erreicht. Um sie ergebnisorientiert führen zu können, gilt es zwei zentrale Fragen zu beantworten: Wie lässt sich die strategische Bedeutung maritimer kritischer Infrastrukturen fassen? Und was ist dementsprechend ein angemessenes Verständnis von deren Sicherheit?

3 Großbritannien hat in den letzten Jahren Sicherheitsmaßnahmen für kritische Infrastrukturen im maritimen Raum ausgeweitet. Siehe zum Beispiel: UK Department for Transport, *Maritime 2050, Navigating the Future*, London, Januar 2019, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872194/Maritime_2050_Report.pdf> (eingesehen am 14.6.2023); UK Secretary of State for Transport, *National Strategy for Maritime Security*, London, August 2022, <https://s3.documentcloud.org/documents/22136535/national-strategy-for-maritime-security-web-version.pdf> (eingesehen am 14.6.2023).
4 Japan veröffentlicht seit 2013 alle fünf Jahre einen Basic Plan on Ocean Policy: Japan Cabinet Office, »Ocean Policy«, Tokio 2023, <https://www8.cao.go.jp/ocean/english/index_e.html> (eingesehen am 14.6.2023). Maritime Sicherheit ist zentraler Teil der Sicherheitsstrategie. Japanese Government, *National Security Strategy of Japan*, Tokio, Dezember 2022, <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nsse.pdf> (eingesehen am 14.6.2023).
5 Australien legt seit Jahrzehnten einen besonderen Fokus auf den maritimen Raum. Aktuelle Vorhaben sind die Umsetzung der Civil Maritime Security Strategy 2021 und Reformen der Regulierung kritischer Infrastrukturen. Australian Home Affairs Department, *Australian Government Civil Maritime Security Strategy*, Canberra 2021, <https://www.homeaffairs.gov.au/nat-security/files/australian-government-civil-maritime-security-strategy.pdf> (eingesehen am 14.6.2023); Australian Cyber and Infrastructure Security Centre, *Aviation and Maritime Critical Infrastructure Reforms*, Canberra 2022, <https://www.cisc.gov.au/legislative-information-and-reforms/aviation-and-maritime-transport-security/aviation-maritime-critical-infrastructure-reforms> (eingesehen am 14.6.2023).
6 Finnlands nationale Risikoeinschätzung 2023 klassifizierte unter anderem Unterseekabel und maritime Transportinfrastrukturen als kritisch für die nationale Versorgungssicherheit. Finland's Ministry of the Interior, *National Risk Assessment 2023*, Helsinki 2023, <https://julkaisut.valtioneuvosto.fi/handle/10024/164629> (eingesehen am 14.6.2023).
7 Die Nationale Sicherheitsstrategie Spaniens verweist auf die Relevanz maritimer kritischer Infrastrukturen wie Unterseekabel, Pipelines und Häfen. Spanische Regierung, *National Security Strategy 2021. A Shared Project*, Madrid 2021, <https://www.dsn.gob.es/es/file/7272/download?token=miLM79u6> (eingesehen am 14.6.2023).
8 Die USA verfügen über zahlreiche Regelungen und Maßnahmen zum Schutz maritimer kritischer Infrastrukturen, darunter auch im Bereich Cybersecurity. Siehe US Department of Homeland Security, *The Maritime Infrastructure Recovery Plan*, Washington, D.C., April 2006, <https://www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf> (eingesehen am 14.6.2023); United States White House Office, *National Maritime Cybersecurity Plan to the National Strategy for Maritime Security*, Washington, D.C., Dezember 2020, <https://www.hsdl.org/c/abstract/?docid=848704> (eingesehen am 14.6.2023).

Abbildung

Ausgewählte Zwischenfälle 2021/22, die maritime Infrastruktur zerstört oder beeinträchtigt haben



Vorfälle in der Region Europa / Nordatlantik, die zu einer substanziellen Zerstörung / Einschränkung von Infrastrukturen geführt haben und deren Urheber unbekannt sind.

	Datum	Kurzbeschreibung des Vorfalls
A	April 2021	Großflächige Zerstörung von **Untersee-Datenkabeln** und damit verbundenen Sensoren des norwegischen Instituts für Meeresforschung
B	07.01.2022	Durchtrennung des Haupt-**Untersee-Datenkabels** zwischen dem norwegischen Festland und der Insel Spitzbergen, das unter anderem der Anbindung der Satellitenkommunikationsstation SvalSat dient
C	26.09.2022	Sprengung von drei Strängen der Gas**pipelines** Nord Stream 1 und 2
D	19.10.2022	Durchtrennung von drei **Untersee-Datenkabeln** vor Marseille
E	Oktober 2022	Durchtrennung von zwei **Untersee-Datenkabeln** innerhalb einer Woche zwischen den Färöer-Inseln und den Shetland-Inseln
F	seit März 2022	Störung der **Seewege** durch Seeminen, die vor der ukrainischen Schwarzmeerküste verlegt wurden und durch Strömung bis in den Bosporus treiben

Quellen:
zu **A** www.newsinenglish.no
zu **B** https://thebarentsobserver.com
zu **D** https://apnews.com | https://trust.zscaler.com/zscloud.net
zu **E** www.highnorthnews.com
zu **F** www.euronews.com | www.reuters.com | www.tradewindsnews.com

Quellen:
Zu **A**: <https://www.newsinenglish.no/2021/11/07/surveillance-cables-mysteriously-cut/>
Zu **B**: <https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption>
Zu **D**: <https://en.overclocking.com/in-a-few-hours-3-underwater-internet-cables-damaged-in-the-south-of-france/>
Zu **E**: <https://www.highnorthnews.com/en/fiber-optic-submarine-cable-near-faroe-and-shetland-islands-damaged-mediterranean-cables-also-cut>
Zu **F**: <https://www.euronews.com/2022/08/11/ukraine-war-drifting-mines-pose-deadly-threat-in-black-sea-waters>
<https://www.reuters.com/world/europe/ukraine-warns-mines-drifting-along-black-sea-coast-due-storm-2023-02-14/>
<https://www.tradewindsnews.com/bulkers/russian-navy-issues-mine-warning-for-parts-of-the-black-sea/2-1-1486727>

Wann sind Infrastrukturen »kritisch«?

Um diese Frage beantworten zu können, bedarf es zunächst einer Klärung des Begriffs »Infrastruktur«. Bei genauerer Betrachtung erweist er sich nämlich als vieldeutig. Die Frage nach der Kritikalität von Infrastrukturen, also dem Grad bzw. Ausmaß ihrer besonderen Bedeutung, führt zudem unweigerlich zu politischen Urteilen über die gesellschaftliche Bedeutung einzelner Infrastrukturen. Es überrascht insofern nicht, dass diesbezüglich auch in der reichhaltigen wissenschaftlichen Literatur zum Thema kein Konsens herrscht. Im Bewusstsein darum, dass es sich hierbei um einen politisch umkämpften Begriff handelt, nimmt unsere Analyse als Ausgangspunkt daher den aktuellen politischen Diskurs. So definiert etwa die European Critical Infrastructures Directive von 2008 »kritische Infrastruktur« als

> »die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen

> Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten«.[9]

Ähnliche Formulierungen finden sich bis heute in den einschlägigen Dokumenten der EU, zuletzt etwa in der überarbeiteten Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS-2-Richtlinie) vom Dezember 2022.[10]

In deutschen Gesetzestexten, beispielsweise dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI), findet sich ein ganz ähnliches Verständnis kritischer Infrastrukturen.[11] Sie gelten demnach als »kritisch«, wenn bzw. weil ihr Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe sowie eine Gefährdung der öffentlichen Sicherheit zur Folge hätte.

Auch die bisherige Diskussion um das KRITIS-Dachgesetz, in dem die verschiedenen nationalen Bemühungen zum Schutz kritischer Infrastrukturen unter einem »Dach« zusammengeführt werden sollen, weist in diese Richtung. Den von der Bundesregierung hierzu veröffentlichten Eckpunkten ist zu entnehmen, dass die grundsätzliche Definition kritischer Infrastrukturen beibehalten, die teilweise unklaren Regelungen jedoch angepasst, Überschneidungen minimiert und insbesondere die Ausformulierung der Schutzverantwortlichkeiten deutlich herausgestellt werden sollen.[12]

Genau betrachtet bietet dieses Verständnis kritischer Infrastrukturen aber für sich genommen noch keine trennscharfen Kriterien. Um praktische Wirksamkeit entfalten zu können, wird es daher auf EU-Ebene wie auf der Ebene nationaler Gesetzgebung ergänzt durch stark ausdifferenzierte Listen von Sektoren, Anlagen und Betreibern konkreter Einrichtungen, denen damit eine besondere, eben »kritische« Bedeutung zugewiesen wird. So wurde zuletzt im Frühjahr 2023 eine neue Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) erlassen.[13]

Für die Zwecke dieser Analyse nehmen wir die gesetzlich auf europäischer wie nationaler Ebene verankerte und spezifizierte Definition kritischer Infrastrukturen zum Ausgangspunkt, behalten uns aber vor, darüber hinauszugehen und zu untersuchen, ob auch Einrichtungen im maritimen Raum, die gesetzlich bisher nicht als kritisch definiert wurden, eine so herausgehobene Bedeutung aufweisen, dass sie als kritisch betrachtet werden sollten — zum Beispiel strategisch besonders bedeutsame Seewege.[14]

Darüber hinaus gilt es noch einmal genauer zu hinterfragen, *für wen* eine Einrichtung von kritischer Bedeutung ist. Auch hier zeigt sich der politische Charakter der Diskussion: Soll es »nur« um deutsche und europäische Interessen gehen, oder sollte eine Infrastruktur auch dann als kritisch gelten, wenn sie Teil globaler Kooperationsbeziehungen ist und folglich auch die Interessen von Staaten und Gesellschaften jenseits Europas berührt?

Schließlich gehört zum Verständnis von kritischen Infrastrukturen, dass diese in besonderer Weise zu schützen sind. Um zu beurteilen, ob eine Einrichtung als kritische Infrastruktur verstanden werden sollte, bedarf es daher auch einer Analyse der potentiellen Gefährdungen. Für eine Vielzahl kritischer Infrastrukturen, auch solcher im maritimen Bereich, gehen die meisten Gefährdungen von technischen Defekten, Unfällen oder natürlichen Ereignissen wie Unwettern aus. Neben diesen nicht intendierten, deshalb aber in ihren Auswirkungen nicht weniger bedeutsamen Störfaktoren liegt ein besonderer Fokus dieser Ana-

9 Europäisches Parlament/Rat der Europäischen Union, *Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern*, Brüssel, 8.12.2008, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008L0114> (eingesehen am 4.9.2023).

10 Europäisches Parlament/Rat der Europäischen Union, *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*, Brüssel, 14.12.2022, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555> (eingesehen am 11.1.2024).

11 Bundesamt für Justiz, *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)*, 14.8.2009, § 2, <https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html> (eingesehen am 4.9.2023).

12 Bundesministerium des Innern, *Eckpunkte für das KRITIS-Dachgesetz*, <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2022/eckpunkte-kritis.pdf?__blob=publicationFile&v=1> (eingesehen am 4.9.2023).

13 »Dritte Verordnung zur Änderung der BSI-Kritisverordnung«, in: *Bundesgesetzblatt I*, (1.3.2023) 53, <https://www.recht.bund.de/bgbl/1/2023/53/VO.html> (eingesehen am 4.9.2023).

14 Vgl. dazu den Beitrag von Bettina Rudloff in dieser Studie, S. 37ff.

lyse auf Handlungen, die darauf abzielen, die Funktionsfähigkeit kritischer Infrastruktur zu beeinträchtigen oder gänzlich zu zerstören — also auf absichtsvoller politischer Sabotage.

Die strategische Bedeutung des maritimen Raums

Wie schon angedeutet, rücken in diesem Zusammenhang maritime Infrastrukturen erst seit einigen Jahren in den Blick. Prominent hervorgehoben wurden sie in der Nationalen Sicherheitsstrategie, wo es nun heißt: »Für die Versorgungs- und Wirtschaftssicherheit Deutschlands hat dabei die maritime Dimension, über und unter Wasser, eine besondere Bedeutung.«[15] Zwar ist das Thema damit gesetzt, die strategische Debatte darüber steht aber noch aus.

In jedem Fall ist der maritime Raum schon länger zu einem politisch instabilen und damit auch (wieder) unsicheren Ort geworden. Seine Destabilisierung reicht durchaus über das unmittelbare Geschehen auf und unter dem Wasser hinaus und wirkt sich so auch auf Regionen aus, die auf den ersten Blick weit von den Meeren und Ozeanen entfernt sind.

Unterschiedliche Faktoren tragen zu dieser Destabilisierung bei.[16] Einige gehen auf unbewusste oder zumindest nicht bewusst gesteuerte Handlungen zurück (u. a. die Auswirkungen des Klimawandels), andere hingegen lassen sich unmittelbar auf das Handeln und die Interessen staatlicher wie nichtstaatlicher Akteure zurückführen (u. a. Territorialstreitigkeiten, Zugang zu Ressourcen oder die Abhängigkeit von lebenswichtigen kritischen Infrastrukturen).

Nichtstaatliche Akteure, etwa terroristische Gruppierungen und kriminelle Vereinigungen, nutzen seit jeher den maritimen Raum. Rückblickend hat insbesondere Terrorismus den Schutz kritischer Infrastrukturen, auch auf See, notwendig gemacht. Aufgrund seiner strategischen Weite und Tiefe wie auch der Möglichkeiten zum verdeckten Einsatz ist der maritime Raum derzeit aber vor allem im Fokus von zwischenstaatlichen Rivalitäten, die vielfach als Großmachtkonflikte gedeutet werden. Diese entfalten sich in vier Handlungsdimensionen mit Relevanz für das maritime Umfeld: einer weltordnungspolitischen, einer wirtschaftlichen, einer militärischen und schließlich einer technologischen Dimension.

Dimensionen globaler Großmachtrivalitäten

Weltordnungspolitisch geht es hier um die Geltung der bestehenden internationalen Rechtsnormen für die Beziehungen zwischen den Staaten. Dies zeigt sich etwa in territorialen Streitigkeiten und damit verbunden in der Frage nach dem Zugang zu maritimen Räumen, zu Seeverbindungslinien und Ressourcen oder nach der Kontrolle über diese. Das Internationale Seerecht und seine Regelungen zur Klärung von Territorialstreitigkeiten sowie zur Nutzung des maritimen Raums im Verständnis der freien Schifffahrt (Freedom of Navigation) werden dabei teils offen infrage gestellt.

Bei der *wirtschaftlichen* Dimension stehen Ressourcen und Seeverbindungslinien im Zentrum der Konflikte, insbesondere mit Blick auf globale Lieferketten, auf die weltweite Nahrungsversorgung, aber auch auf das Agieren von Seestreitkräften zur Kontrolle dieser Seewege. Die See gewinnt zugleich als Standort und als rares Gut für Energiegewinnung und entsalztes Trinkwasser immer mehr an Relevanz.

Die *militärische* Dimension wird augenscheinlich geprägt durch umfangreiche Flottenrüstungsprogramme von Staaten wie China, Russland und den USA und damit verbundene Machtansprüche. Wer Großmacht sein will, so die dahinterstehende Logik, braucht Seemacht, und Seemacht setzt wiederum den Zugang zu Seeverbindungslinien und Häfen voraus.[17] Damit steigt die Gefahr einer Zuspitzung von Konflikten im maritimen Raum, erst recht dann, wenn andere kon-

15 Bundesregierung, *Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie*, Berlin, 14.6.2023, S. 25, <https://www.bmvg.de/resource/blob/5636374/38287252c5442b786ac5d0036ebb237b/nationale-sicherheitsstrategie-data.pdf> (eingesehen am 4.9.2023).

16 Göran Swistek/Michael Paul, *Geopolitik im Ostseeraum*, Berlin: Stiftung Wissenschaft und Politik, Januar 2023 (SWP-Aktuell 6/2023), doi: 10.18449/2023A06. Herausgearbeitet wurden hier die Bereiche des geopolitischen Wettbewerbs mit einer einhergehenden Militarisierung, ungelöste Territorialstreitigkeiten, illegale transnationale Aktivitäten, der Zugang und die Nutzung von Ressourcen, die Auswirkungen des Klimawandels, die Fragilität lebenswichtiger Seeverbindungslinien sowie die Abhängigkeit von lebenswichtiger kritischer Infrastruktur als destabilisierende Faktoren im maritimen Umfeld.

17 Raymond Aron, *Frieden und Krieg. Eine Theorie der Staatenwelt*, Frankfurt a. M. 1963.

ventionelle, militärische Fähigkeiten an Durchsetzungsfähigkeit und Überraschungsmoment verlieren.

Die *technologische* Dimension schließlich vereint verschiedene Aspekte. So ist der maritime Raum ein wichtiger Ort der Entwicklung und Erprobung neuer Technologien: von kabelloser Unterwasserkommunikation und Datenübertragung über Klimatechnologien wie die Speicherung von CO_2 und neuen autonomen Transport- sowie Fortbewegungsmöglichkeiten bis hin zur Erprobung von »Hyperwaffen« mit theoretisch apokalyptischen Konsequenzen. Zugleich finden sich im maritimen Raum aber auch zahlreiche bereits existierende Technologien, die von vitaler Bedeutung für die Stabilität von Staaten und Gesellschaften sind, wie zum Beispiel Untersee-Datenkabel oder Stromtrassen.

Sabotage, Spionage und hybride Angriffe

Vor dem Hintergrund der sich verschärfenden Großmachtrivalitäten, aber auch bereits mit Blick auf wiederholte Versuche nichtstaatlicher Akteure, sich den maritimen Raum für terroristische Aktivitäten zunutze zu machen, verschwimmen die Grenzen zwischen innerer und äußerer Sicherheit zusehends. Gleichzeitig kommen Aspekte hinzu, die bislang eher selten aus einem explizit sicherheitspolitischen oder militärischen Blickwinkel betrachtet wurden. Dazu zählen unter anderem Fragen der Energiesicherheit, der Schutz der Handels- und Wirtschaftsstandorte, transnationale Kriminalität, Sabotage oder die zielgerichtete Beeinflussung von Gesellschaften im Informations- und Cyberraum.

Bezogen auf maritime kritische Infrastrukturen lassen sich insbesondere drei Arten sicherheitsrelevanter Aktivitäten unterscheiden: Spionage, Sabotage und psychologische Beeinflussung von Gesellschaften.

Spionageaktivitäten im maritimen Raum können unterschiedliche Ziele verfolgen: Zum einen kann das Abgreifen von Daten an den Unterseekabeln der politischen oder wirtschaftlichen Informationsgewinnung dienen.[18] Zum anderen können Spionageaktivitäten aber auch dazu dienen, maritime Infrastrukturen auszuspähen, um deren Verwundbarkeit zu ergründen und entsprechende Pläne zu ihrer Zerstörung im Konfliktfall zu erarbeiten.

Die bewusste Herbeiführung von Störungen, die Sabotage, dient dann der konkreten Schädigung und Schwächung des davon betroffenen Staates. Jede Form der Manipulation an kritischer Infrastruktur, auch eine, die gar keine tatsächliche Störung verursacht, kann wiederum — als Teil gezielter psychologischer Beeinflussung — bereits Angst und Verunsicherung in der betroffenen Gesellschaft hervorrufen und damit die politische Stabilität schwächen.

Darüber hinaus ist eine zunehmende Verlagerung von Aktivitäten in den sogenannten »hybriden« Bereich zu beobachten. Solche Maßnahmen und die dabei eingesetzten Mittel liegen unterhalb der Schwelle eines bewaffneten Angriffs und lassen sich nur schwer einem bestimmten staatlichen oder nichtstaatlichen Akteur zuschreiben. Attraktiv ist ein derartiges hybrides Vorgehen vor allem für Staaten, die einen offenen Bruch mit internationalem Recht vermeiden wollen.

Was nun den Schutz maritimer kritischer Infrastrukturen angeht, so kommen hier spezifische Eigenheiten des Raums zum Tragen.[19] Beispielsweise ist das maritime Umfeld geprägt von einem hohen Grad an rechtlicher Komplexität[20] und umfasst zudem Bereiche ungenauer, kaum ausdifferenzierter oder sich überlagernder Regelungen. Hinzu kommt, dass sich der maritime Raum aufgrund seiner Geografie besonders für verdecktes Agieren eignet. Der Schutz kritischer Infrastrukturen wird zusätzlich dadurch erschwert, dass diese oftmals eine hohe Flächenausprägung bzw. Ausdehnung aufweisen, wie etwa im Fall von Windparks, Pipelines oder Unterseekabeln. Schließlich werden diese Infrastrukturen überwiegend privatwirtschaftlich betrieben und sind aufgrund ihrer räumlichen Dimensionen nur schwer lückenlos zu überwachen, ob nun durch die privaten Betreiber selbst oder durch staatliche Sicherheitsorgane.

Die Struktur der Studie

Die vorliegende Studie soll einen Beitrag zur strategischen Debatte über maritime kritische Infrastrukturen leisten. Leitend sind dabei die schon oben genannten Fragen: Wie lässt sich die strategische Bedeutung maritimer kritischer Infrastrukturen fassen? Und was ist dementsprechend ein angemesse-

18 Vgl. hierzu den Beitrag von Daniel Voelsen in dieser Studie, S. 48ff.

19 Vgl. Christian Bueger/Tobias Liebetrau, »Critical Maritime Infrastructure Protection: What's the Trouble?«, in: *Marine Policy*, 155 (2023), S. 2f.

20 Vgl. den Beitrag von Christian Schaller in dieser Studie, S. 14ff.

nes Verständnis von deren Sicherheit? Die verschiedenen Beiträge der Studie setzen einen je eigenen Fokus, ergeben aber im Zusammenspiel unsere Antwort auf die Leitfragen.

Den Anfang macht ein Beitrag von *Christian Schaller*, in dem die zentralen völkerrechtlichen Rahmenbedingungen erläutert werden. Insbesondere wird hier dargestellt, welche Rechte Staaten in den verschiedenen Zonen des maritimen Raumes in Bezug auf kritische Infrastrukturen haben, von den Küstengebieten über die ausschließliche Wirtschaftszone bis zur Hohen See. Der Beitrag geht auch darauf ein, welche rechtlichen Grundlagen das Völkerrecht mit Blick auf den Schutz dieser Infrastrukturen einräumt.

Die folgenden drei Beiträge nehmen zentrale Sektoren in den Blick: Energie, Ernährung, Kommunikation. Die Analyse folgt hier über die Sektoren hinweg einer gemeinsamen Systematik: Erstens wird identifiziert, welche maritimen Infrastrukturen überhaupt eine besondere, sprich »kritische« Bedeutung haben. Eine solche Priorisierung ist notwendig, weil maritime Infrastrukturen über weite Flächen verteilt sind und weil ihre Zahl kontinuierlich zunimmt. Zweitens wird geklärt, welchen Gefahren diese Infrastrukturen konkret ausgesetzt sind. Drittens prüfen die Beiträge, welche Maßnahmen zum Schutz vor diesen Gefahren wirksam und mit vertretbarem Aufwand umsetzbar sind.

Für den Bereich der Energieversorgung zeichnet *Jacopo Maria Pepe* in seinem Beitrag nach, wie sich infolge des Kriegs gegen die Ukraine, aber auch perspektivisch mit Blick auf die wachsende Bedeutung von Wasserstoff die globalen Energiebeziehungen verschieben. Einige maritime Energieinfrastrukturen erweisen sich in diesem Zusammenhang als besonders kritisch: Kurzfristig betrifft das die Gaspipelines Europipe 1 und 2, die Deutschland mit Norwegen verbinden; mittelfristig ist damit zu rechnen, dass sich der Fokus auf den Schutz globaler Lieferketten für Flüssigerdgas (Liquid Natural Gas, LNG) verschiebt — und dabei insbesondere auf Seewege und Containerschiffe sowie auf Offshore-Windparks, Stromanbindungsleitungen und Interkonnektoren, also internationale Verbindungsleitungen, in der Nordsee.

Bettina Rudloff nimmt in ihrem Beitrag jene globalen Handelsströme in den Blick, die Grundlage der Nahrungsversorgung in Europa wie auch in anderen Teilen der Welt sind. Zentrale Infrastrukturen sind in diesem Fall Häfen, Seewege sowie erneut Containerschiffe. Auch hier werden einzelne Bereiche von Infrastrukturen identifiziert, die aufgrund ihrer besonderen Bedeutung als kritisch einzustufen sind; dazu zählen Meerengen wie die Straße von Gibraltar oder die Straße von Malakka, aber auch einzelne Häfen wie Dover oder die Schwarzmeerhäfen der Ukraine.

Mit Blick auf die globalen Kommunikationsnetze untersucht schließlich *Daniel Voelsen*, welche Unterseekabel und Anlandepunkte als besonders kritische Infrastrukturen verstanden werden sollten. Hier zeigt sich, dass die Analyse letztlich eine kontinentaleuropäische Perspektive verlangt. Während ein einzelnes Datenkabel für sich genommen nicht kritisch ist, kommt einigen Orten an der europäischen Küste — von der Südwestküste Englands bis nach Marseille — eine besonders kritische Bedeutung zu, weil sich dort etwa zentrale Kabelverbindungen in die USA oder nach Asien verdichten.

Im Anschluss an die Analyse zentraler Sektoren widmen sich die folgenden zwei Beiträge noch einmal vertieft den Möglichkeiten zum Schutz maritimer kritischer Infrastrukturen.

Der Beitrag von *Göran Swistek* geht der Frage nach, welche militärischen Schutzmaßnahmen denkbar sind. Dabei macht er unter anderem deutlich, dass die Möglichkeiten der Bundeswehr zum Schutz ziviler Infrastrukturen in Friedenszeiten rechtlich eingeschränkt sind und dass im Übrigen die dafür benötigten operativen Fähigkeiten nur in begrenztem Maße zur Verfügung stehen. *Raphael Bossong* ergänzt diesen Teil der Analyse, indem er in seinem Beitrag die Möglichkeiten der EU im Bereich ziviler Schutzmaßnahmen auslotet.

Das Schlusskapitel führt die Analysen der einzelnen Beiträge zusammen, liefert einen Ausblick auf die mittel- bis langfristige Entwicklung und formuliert auf dieser Grundlage übergreifende Handlungsempfehlungen.

Christian Schaller

Völkerrechtliche Grundlagen des Schutzes maritimer kritischer Infrastruktur

Die Errichtung und der Betrieb maritimer kritischer Infrastruktur sind zu einem gewissen Grad durch das Seevölkerrecht reguliert. Bislang existieren jedoch nur wenige Regelungen, die speziell die Sicherheit und den Schutz solcher Infrastruktur in den Blick nehmen. Unabhängig davon setzt das allgemeine Völkerrecht einen Rahmen, innerhalb dessen Staaten auf konkrete Bedrohungen reagieren und sich etwa gegen Sabotageakte wehren können.

Seevölkerrecht

Das Seevölkerrecht ist größtenteils im Seerechtsübereinkommen der Vereinten Nationen von 1982 (SRÜ)[1] kodifiziert, das in vielen Vorschriften Gewohnheitsrecht widerspiegelt. Das SRÜ regelt unter anderem die Errichtung künstlicher Inseln sowie von Anlagen und Bauwerken im Meer. Außerdem enthält es Vorgaben für das Verlegen unterseeischer Kabel und Rohrleitungen.

Innere Gewässer und Häfen

Die inneren Gewässer eines Staates sind von dessen Küstenmeer durch die Basislinie getrennt.[2] Im Normalfall handelt es sich hierbei um die Niedrigwasserlinie entlang der Küste.[3] Häfen, die ein Staat an seiner Küste errichtet, befinden sich im seerechtlichen Sinne in den inneren Gewässern.[4]

Innere Gewässer unterfallen der Gebietshoheit des Staates. Das SRÜ schränkt die Handlungsfreiheit des Staates dort nicht ein. Wichtig ist dies zum Beispiel für den Schutz schwimmender Flüssigerdgasterminals, die in den inneren Gewässern vertäut sind, sowie für die Absicherung der Anlandestationen unterseeischer Kabel und Rohrleitungen.

Jeder Staat kann festlegen, unter welchen Voraussetzungen fremde Schiffe in seine inneren Gewässer und Häfen einlaufen dürfen. Entsprechende Rechte werden meist durch bilaterale oder multilaterale Übereinkünfte begründet. Dem allgemeinen Seevölkerrecht entspringt jedoch kein generelles Recht zum Anlaufen fremder Häfen.[5] Aus Sicherheitsgründen kann ein Staat sogar seine internationalen Handelshäfen schließen.[6]

Mit dem Einlaufen in innere Gewässer und Häfen begeben sich fremde Schiffe unter die vollständige Hoheitsgewalt des jeweiligen Küstenstaates. Kriegsschiffe und sonstige Staatsschiffe, die nicht Handelszwecken dienen, sind zwar an die Gesetze des Küstenstaates gebunden, durch Immunität aber vor dem Zugriff seiner Behörden geschützt. Der Aufforderung durch den Küstenstaat, die inneren Gewässer zu verlassen, müssen sie gleichwohl Folge leisten.

Küstenmeer

Als Küstenmeer wird der Meeresstreifen bezeichnet, der mit einer Ausdehnung von bis zu 12 Seemeilen unmittelbar an das Landgebiet und die inneren Ge-

1 *UN Convention on the Law of the Sea*, 10.12.1982, United Nations Treaty Series (UNTS), Bd. 1833 (1994), S. 3.

2 Art. 8 Abs. 1 SRÜ. Vgl. zu den Begriffen Küstenmeer, Basislinie etc. die Abbildung im Beitrag von Göran Swistek, S. 67.

3 Art. 5 SRÜ.

4 Art. 11 i.V.m. Art. 5 SRÜ.

5 Robin Churchill/Vaughan Lowe/Amy Sander, *The Law of the Sea*, 4. Aufl., Manchester 2022, S. 112ff; Yoshifumi Tanaka, *The International Law of the Sea*, 3. Aufl., Cambridge 2019, S. 98f. Hafenzugangsrechte bestehen in Fällen von Seenot, zumindest soweit das Leben von Menschen bedroht ist, sowie unter bestimmten Voraussetzungen für Binnenstaaten bei der Ausübung der Transitfreiheit (Art. 125 Abs. 1 SRÜ).

6 Auch zur Durchsetzung anderer gewichtiger Interessen wird dies für zulässig erachtet. Dazu Churchill/Lowe/Sander, *The Law of the Sea* [wie Fn 5], S. 113f.

wässer anschließt.[7] Das Küstenmeer, der dazugehörige Meeresboden und Untergrund sowie der darüber befindliche Luftraum sind Teil des Staatsgebiets.[8] Die Errichtung und der Betrieb kritischer Infrastruktur im Küstenmeer sowie die Genehmigung und Regulierung solcher Aktivitäten obliegen allein dem Küstenstaat. Dieser hat die vollständige Hoheitsgewalt über Anlagen und Bauwerke sowie über Kabel und Rohrleitungen, die sich in seinem Küstenmeer befinden.

Bei der Ausübung seiner Hoheitsbefugnisse muss der Küstenstaat jedoch beachten, dass die Schiffe anderer Staaten das Recht haben, sein Küstenmeer friedlich zu durchfahren.[9] Im Hinblick auf Bedrohungen, die von fremden Schiffen im Küstenmeer ausgehen, kommt dem Regelwerk über die friedliche Durchfahrt besondere Bedeutung zu. Eine Durchfahrt ist demnach friedlich, solange sie nicht den Frieden, die Ordnung oder die Sicherheit des Küstenstaates beeinträchtigt.[10] Als Beeinträchtigung in diesem Sinne und damit als nichtfriedlich gilt die Durchfahrt eines fremden Schiffes unter anderem dann, wenn auf dem Schiff eine Handlung vorgenommen wird, »die auf die Störung eines Nachrichtenübermittlungssystems oder anderer Einrichtungen oder Anlagen des Küstenstaates gerichtet ist«.[11] Darunter fallen auch vorsätzliche Eingriffe in die Funktionsfähigkeit kritischer Infrastruktur. Außerdem führen Aktivitäten, die nicht unmittelbar mit der Durchfahrt zusammenhängen, grundsätzlich dazu, dass die Durchfahrt als nichtfriedlich gilt.[12] Um eine nichtfriedliche Durchfahrt zu unterbinden, darf der Küstenstaat die »erforderlichen« Maßnahmen ergreifen.[13] Welche Maßnahmen im Einzelfall zulässig sind, lässt das SRÜ offen. Das Spektrum reicht von einer Überprüfung des betreffenden Schiffes über die Aufforderung, nichtfriedliche Aktivitäten zu unterlassen oder das Küstenmeer zu verlassen, bis hin zur Anwendung von Zwang.[14] Unklar ist, ob und gegebenenfalls ab welcher Verdachtsstufe der Küstenstaat präventiv gegen Schiffe vorgehen darf.[15]

Für Teile seines Küstenmeers kann der Küstenstaat die friedliche Durchfahrt fremder Schiffe vorübergehend aussetzen, sofern dies für seine Sicherheit unerlässlich ist,[16] etwa vor Militärhäfen.[17] In der Praxis kommt es immer wieder dazu, dass solche Sperrungen von längerer Dauer sind.[18] Zur Sicherung ziviler kritischer Infrastruktur kann eine räumlich und zeitlich begrenzte Suspendierung des Durchfahrtsrechts ebenfalls zulässig sein.[19] Fraglich ist, wie längerfristige Sperrungen zu beurteilen wären, die etwa dazu dienen könnten, Flüssigerdgasterminals zu schützen.

Ein Staat kann in seinem Küstenmeer Sicherheitszonen um gefährdete Objekte sowie entlang von Kabeln und Rohrleitungen einrichten.

Jedenfalls kann der Küstenstaat die friedliche Durchfahrt in Bezug auf bestimmte Angelegenheiten gesetzlich regeln. Seine Rechtsetzungsbefugnis erstreckt sich unter anderem auf den Schutz von Einrichtungen, Anlagen, Kabeln und Rohrleitungen.[20] Zu diesem Zweck kann ein Staat in seinem Küstenmeer Sicherheitszonen um gefährdete Objekte sowie entlang von Kabeln und Rohrleitungen einrichten und dort bestimmte Aktivitäten verbieten, etwa Ankern, Fischen oder Baggerarbeiten.[21] Zu den Staaten, die solche Zonen und Korridore eingerichtet haben, zählen unter anderem China, Indonesien, Japan und Singapur sowie Australien und Neusee-

7 Art. 2 Abs. 1 und Art. 3 SRÜ.
8 Art. 2 Abs. 2 SRÜ.
9 Art. 17 SRÜ.
10 Art. 19 Abs. 1 S. 1 SRÜ.
11 Art. 19 Abs. 2 lit. k SRÜ.
12 Art. 19 Abs. 2 lit. l SRÜ.
13 Art. 25 Abs. 1 SRÜ.
14 Siehe Richard A. Barnes, »Article 25«, in: Alexander Proelss (Hg.), *United Nations Convention on the Law of the Sea: A Commentary*, München/Oxford/Baden-Baden 2017, S. 222–226 (224f, Rn. 5ff).
15 Wolfgang Graf Vitzthum, »Maritimes Aquitorium und Anschlusszone«, in: Wolfgang Graf Vitzthum (Hg.), *Handbuch des Seerechts*, München 2006, S. 63–159 (124, dort Fn. 338).
16 Art. 25 Abs. 3 SRÜ.
17 Churchill/Lowe/Sander, *The Law of the Sea* [wie Fn. 5], S. 149.
18 Graf Vitzthum, »Maritimes Aquitorium und Anschlusszone« [wie Fn. 15], S. 125, Rn. 125.
19 Mikhail Kashubsky/Anthony Morrison, »Security of Offshore Oil and Gas Facilities: Exclusion Zones and Ship's Routeing«, in: *Australian Journal of Maritime and Ocean Affairs*, 5 (2013) 1, S. 1–10 (3).
20 Art. 21 Abs. 1 lit. b und lit. c SRÜ.
21 In Bezug auf Kabel siehe Tara Davenport, »Submarine Communications Cables and Law of the Sea: Problems in Law and Practice«, in: *Ocean Development & International Law*, 43 (2012) 3, S. 201–242 (217f).

land.[22] Für die Umsetzung derartiger Maßnahmen im Küstenmeer enthält das SRÜ keine Vorgaben. In der Literatur wird jedoch argumentiert, dass Sicherheitszonen einen Radius von mehr als 500 Metern um das jeweilige Objekt haben dürften, sofern die friedliche Durchfahrt durch das Küstenmeer hierdurch nicht behindert werde.[23] Eine weitere Option ist die Festlegung von Schifffahrtswegen und Verkehrstrennungslinien, wo es die Sicherheit der Schifffahrt erfordert,[24] etwa in Gebieten mit einer größeren Zahl von Einrichtungen und Anlagen.

Schiffe, die sich nicht auf der Durchfahrt[25] befinden, sondern im Küstenmeer hin und her fahren, unterliegen währenddessen in vollem Umfang der Hoheitsgewalt des Küstenstaates.[26] Dasselbe gilt für Schiffe, deren Durchfahrt als nichtfriedlich zu qualifizieren ist.[27] Eine Ausnahme besteht wiederum für Kriegsschiffe und sonstige Staatsschiffe, die nicht Handelszwecken dienen. Sie genießen Immunität.[28] Ein Kriegsschiff, das die Gesetze und sonstigen Vorschriften des Küstenstaates für die Durchfahrt auch nach Aufforderung nicht einhält, kann vom Küstenstaat aber gezwungen werden, das Küstenmeer sofort zu verlassen.[29] Obwohl das SRÜ dies nur in Bezug auf Kriegsschiffe regelt, wird generell argumentiert, dass ein solches Vorgehen auch gegenüber sonstigen Staatsschiffen, die nicht Handelszwecken dienen, zulässig ist.[30] Unterseebote und andere Unterwasserfahrzeuge, gleich ob militärisch oder zivil, müssen im Küstenmeer über Wasser fahren und ihre Flagge zeigen.[31]

Ausschließliche Wirtschaftszone und Festlandsockel

Bei der ausschließlichen Wirtschaftszone (AWZ) handelt es sich um ein Gebiet, das unmittelbar an die Territorialgewässer eines Küstenstaates grenzt. Diese Zone unterliegt nicht der Souveränität des Küstenstaates. Gleichwohl verfügt der Küstenstaat dort über souveräne Rechte zur Erforschung, Ausbeutung, Erhaltung und Bewirtschaftung der natürlichen Ressourcen der Gewässer, des Meeresbodens und seines Untergrunds. Hinzu kommen souveräne Rechte in Bezug auf andere Tätigkeiten, die der wirtschaftlichen Erforschung und Ausbeutung der Zone dienen, wie etwa die Energieerzeugung aus Wasser, Strömung und Wind. Außerdem haben Küstenstaaten in ihrer AWZ Hoheitsbefugnisse, die sich auf die Errichtung und Nutzung von künstlichen Inseln, Anlagen und Bauwerken, auf die wissenschaftliche Meeresforschung sowie auf den Schutz und die Bewahrung der Meeresumwelt beziehen.[32] In ihrer seewärtigen Ausdehnung darf sich die AWZ nicht weiter als 200 Seemeilen über die Basislinie hinaus erstrecken, von der aus auch die Breite des Küstenmeers gemessen wird.[33]

Der Festlandsockel umfasst als natürliche Verlängerung des Landgebiets den Meeresboden und den Untergrund jenseits des Küstenmeers bis zur äußeren Kante des Festlandrands. Ungeachtet der geomorphologischen und geologischen Gegebenheiten steht jedem Küstenstaat zumindest ein Festlandsockel von 200 Seemeilen zu (ebenfalls gemessen ab der jeweiligen Basislinie), sofern die äußere Kante des Festlandrands tatsächlich in einer geringeren Entfernung verläuft.[34] Die souveränen Rechte, die ein Küstenstaat exklusiv über seinen Festlandsockel ausübt, betreffen die Erforschung des Sockels und die Ausbeutung seiner natürlichen Ressourcen.[35] Diese Rechte berühren allerdings nicht den Rechtsstatus der über dem Festlandsockel befindlichen Gewässer (AWZ und ggf. Hohe See).[36]

22 Siehe ebd. Dazu auch Stuart Kaye, »The Protection of Platforms, Pipelines and Submarine Cables under Australian and New Zealand Law«, in: Natalie Klein/Joanna Mossop/Donald R. Rothwell (Hg.), *Maritime Security. International Law and Policy Perspectives from Australia and New Zealand*, Abingdon 2010, S. 186–201.

23 Kashubsky/Morrison, »Security of Offshore Oil and Gas Facilities« [wie Fn. 19], S. 2. Dazu auch Sarah Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz*, Heidelberg u. a. 2011, S. 181. Je ausgreifender solche Zonen sind und je stärker sie die friedliche Durchfahrt einschränken, desto eher dürfte dadurch Art. 25 Abs. 3 SRÜ tangiert sein, der eine Aussetzung der friedlichen Durchfahrt nur unter engen Voraussetzungen gestattet [siehe Fn. 16].

24 Art. 22 SRÜ.

25 Was »Durchfahrt« bedeutet, ist in Art. 18 SRÜ geregelt.

26 Churchill/Lowe/Sander, *The Law of the Sea* [wie Fn. 5], S. 159.

27 Ebd., S. 149.

28 Siehe Art. 32 SRÜ.

29 Art. 30 SRÜ. Dazu Graf Vitzthum, »Maritimes Aquitorium und Anschlusszone« [wie Fn. 15], S. 126ff, Rn. 127ff.

30 Siehe z. B. Churchill/Lowe/Sander, *The Law of the Sea* [wie Fn. 5], S. 164.

31 Art. 20 SRÜ.

32 Art. 56 Abs. 1 SRÜ.

33 Art. 57 SRÜ.

34 Art. 76 Abs. 1 SRÜ.

35 Art. 77 SRÜ.

36 Art. 78 Abs. 1 SRÜ.

Künstliche Inseln, Anlagen und Bauwerke in der AWZ und auf dem Festlandsockel

In der AWZ und auf dem Festlandsockel hat der Küstenstaat das exklusive Recht, künstliche Inseln, Anlagen und Bauwerke zu errichten sowie deren Errichtung, Betrieb und Nutzung zu genehmigen und zu regeln.[37] Als Anlagen und Bauwerke gelten auch Bohrplattformen für Erdöl und Erdgas sowie Plattformen für die Erzeugung erneuerbarer Energien.[38] In seiner AWZ und auf seinem Festlandsockel übt der Küstenstaat über solche Objekte ausschließliche Hoheitsbefugnisse aus.[39] Falls notwendig, kann der Küstenstaat auch »angemessene« Sicherheitszonen einrichten, in denen er »geeignete« Maßnahmen ergreifen kann, um die Sicherheit der jeweiligen Objekte zu gewährleisten.[40] Solche Zonen dürfen sich höchstens 500 Meter über den Rand der Anlage oder des Bauwerks hinaus erstrecken.[41] Künstliche Inseln, Anlagen und Bauwerke und die sie umgebenden Sicherheitszonen dürfen nicht errichtet werden, wo dies die Nutzung wichtiger internationaler Schifffahrtswege behindern kann.[42]

Zahlreiche Staaten haben Sicherheitszonen in ihrer AWZ eingerichtet.

Der primäre Zweck von Sicherheitszonen besteht darin, Kollisionsunfälle zu verhindern. Einen wirksamen Schutz vor Angriffen können sie wegen ihrer geringen Ausdehnung kaum bieten.[43] Potentielle Angreifer müssen aber zum Beispiel damit rechnen, innerhalb solcher Zonen von Überwachungssystemen erfasst zu werden. Zahlreiche Staaten haben von der Möglichkeit Gebrauch gemacht, Sicherheitszonen in ihrer AWZ einzurichten, darunter Australien, Neuseeland, Russland und Nigeria.[44]

Eine internationale Konvention von 1988 soll helfen, rechtswidrige Handlungen zu unterbinden, die gegen die Sicherheit der Seeschifffahrt gerichtet sind.[45] Die Sicherheit von Plattformen auf dem Festlandsockel wird in einem Protokoll zur Konvention gesondert behandelt.[46] Der Zweck dieser Übereinkommen besteht darin, eine effektive Strafverfolgung zu gewährleisten. Die Vertragsstaaten haben sich verpflichtet, ihre Gerichtsbarkeit auf die in den Übereinkommen definierten Tatbestände auszuweiten und bei der Verfolgung zusammenzuarbeiten. Im Jahr 2005 wurden die Konvention und das Protokoll grundlegend überarbeitet, um terroristische Akte gegen Schiffe und Plattformen bekämpfen und möglichst lückenlos ahnden zu können.[47]

Kabel und Rohrleitungen in der AWZ und auf dem Festlandsockel

Zu den Freiheiten, die alle Staaten in der AWZ genießen, zählt unter anderem das Recht, unterseeische Kabel und Rohrleitungen zu verlegen.[48] Für den Festlandsockel ist dieses Recht im SRÜ gesondert verbrieft.[49] Soweit es um den Meeresboden und Untergrund geht, überlagert das Festlandsockelregime die AWZ-Bestimmungen.[50]

37 Für die AWZ ergeben sich diese Rechte aus Art. 56 Abs. 1 lit. b i) und Art. 60 SRÜ. Für den Festlandsockel gilt Art. 60 SRÜ sinngemäß (Art. 80 SRÜ). Die exklusiven Errichtungs-, Genehmigungs- und Regelungsrechte gelten in Bezug auf künstliche Inseln generell, für Anlagen und Bauwerke jedoch nur, soweit sie den in Art. 56 SRÜ vorgesehenen und anderen wirtschaftlichen Zwecken dienen (Art. 60 Abs. 1 lit. b) bzw. soweit sie die Ausübung der Rechte des Küstenstaates in der Zone beeinträchtigen können (Art. 60 Abs. 1 lit. c).

38 Dazu Alexander Proelss, »Article 60«, in: Proelss (Hg.), *United Nations Convention on the Law of the Sea: A Commentary* [wie Fn. 14], S. 464–480 (470ff, Rn. 9ff).

39 Art. 60. Abs. 2 SRÜ.

40 Art. 60 Abs. 4 SRÜ.

41 Art. 60 Abs. 5 SRÜ.

42 Art. 60 Abs. 7 SRÜ.

43 Dazu Stuart Kaye, »International Measures to Protect Oil Platforms, Pipelines, and Submarine Cables from Attack«, in: *Tulane Maritime Law Journal*, 31 (2007) 2, S. 377–423 (405f); Kashubsky/Morrison, »Security of Offshore Oil and Gas Facilities« [wie Fn. 19], S. 3f.

44 Kashubsky/Morrison, »Security of Offshore Oil and Gas Facilities« [wie Fn. 19], S. 4.

45 *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 10.3.1988, UNTS, Bd. 1678 (1988), S. 221.

46 *Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, 10.3.1988, UNTS, Bd. 1678 (1988), S. 304.

47 *Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 14.10.2005, IMO Doc. LEG/CONF. 15/21, 1.11.2005; *Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, 14.10.2005, IMO Doc. LEG/CONF. 15/22, 1.11.2005.

48 Art. 58 Abs. 1 i.V.m. Art. 87 Abs. 1 lit. c und Art. 112 SRÜ.

49 Art. 79 Abs. 1 SRÜ.

50 Art. 56 Abs. 3 SRÜ.

Der Küstenstaat legt die Bedingungen fest, unter denen Kabel und Rohrleitungen über den Festlandsockel in sein Küstenmeer führen dürfen.[51] Außerdem hat der Küstenstaat Hoheitsgewalt über Kabel und Rohrleitungen, die seine souveränen Rechte am Festlandsockel tangieren. Dies betrifft Kabel und Rohrleitungen, die im Zusammenhang mit der Erforschung des Festlandsockels oder der Ausbeutung seiner Ressourcen verlegt oder genutzt werden.[52] Ebenso fallen darunter Kabel und Rohrleitungen zum Betrieb von künstlichen Inseln, Anlagen oder Bauwerken, die den Hoheitsbefugnissen des Küstenstaates unterliegen.[53]

Etwas anderes gilt für Transitkabel und Rohrleitungen, die lediglich auf den Festlandsockel führen oder diesen durchqueren (ohne in das Küstenmeer des jeweiligen Küstenstaates zu münden oder dieses zu durchqueren) und die nicht mit den eben genannten Nutzungen in Verbindung stehen. In Bezug auf solche Kabel und Leitungen liegen die Hoheitsbefugnisse nicht beim Küstenstaat, sondern bei demjenigen Staat, der die Kabel oder Leitungen verlegt bzw. für die Verlegung durch juristische Personen des Privatrechts unter seiner Rechtsordnung die Verantwortung trägt.[54] Dieser Staat hat das Recht, den Betrieb zu regeln und zu kontrollieren, die Kabel und Leitungen zu inspizieren[55] und mithilfe geeigneter Vorrichtungen dauerhaft zu überwachen.[56]

In der Literatur wird die Auffassung vertreten, dass im Fall von Rohrleitungen der verlegende Staat aus Umweltschutzgründen sogar verpflichtet sei, seine Leitungen vor möglichen Gefahren zu schützen.[57] Verlegende Staaten sind jedoch grundsätzlich nicht befugt, in einer fremden AWZ bzw. auf einem fremden Festlandsockel Schutzzonen für Kabel oder Rohrleitungen einzurichten.[58]

Umstritten ist, ob Küstenstaaten in ihrer AWZ bzw. auf ihrem Festlandsockel Schutzzonen für Kabel und Rohrleitungen einrichten dürfen.

Umstritten ist indes, ob Küstenstaaten in ihrer AWZ bzw. auf ihrem Festlandsockel Schutzzonen für Kabel und Rohrleitungen einrichten dürfen. Hierfür fehlt es an einer ausdrücklichen Rechtsgrundlage im SRÜ. Gleichwohl wird vermehrt argumentiert, dass sich aus den souveränen Rechten, die dem Küstenstaat in seiner AWZ und auf seinem Festlandsockel zustehen, auch die Befugnis ableiten lasse, zumindest zum Zwecke der Durchsetzung dieser Rechte entsprechende Zonen und Korridore zu schaffen.[59] Australien und Neuseeland haben solche Areale ausgewiesen.[60] Jedenfalls haben Küstenstaaten das Recht, auf ihrem Festlandsockel angemessene Maßnahmen zu ergreifen, um Verschmutzungen zu verhüten, die von

51 Siehe Art. 79 Abs. 4 Alt. 1 SRÜ.

52 Art. 79 Abs. 4 Alt. 2 SRÜ.

53 Art. 79 Abs. 4 Alt. 2 SRÜ.

54 Das Eigentum an unterseeischen Kabeln und Rohrleitungen trägt entweder der Staat selbst oder ein Privatrechtssubjekt, etwa ein Kabel- bzw. Rohrleitungsunternehmen oder entsprechende Konsortien. Siehe Rainer Lagoni/Alexander Proelß, »Festlandsockel und ausschließliche Wirtschaftszone«, in: Graf Vitzthum (Hg.), *Handbuch des Seerechts* [wie Fn. 15], S. 161–286 (204, Rn. 126). Dazu auch Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz* [wie Fn. 23], S. 122ff.

55 In Bezug auf Kabel siehe Wolff Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law«, in: Katharina Ziolkowski (Hg.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn 2013, S. 291–318 (303 und 315). In Bezug auf Rohrleitungen siehe Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz* [wie Fn. 23], S. 104ff.

56 Dazu Yoram Dinstein/Arne Willy Dahl, *Oslo Manual on Select Topics of the Law of Armed Conflict – Rules and Commentary*, Cham 2020, S. 56f.

57 Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz* [wie Fn. 23], S. 213f.

58 Ebd., S. 215 und S. 218.

59 Stuart Kaye, *Submission: Proposed Protection Zones Off Sydney*, 26.10.2006, zitiert in: Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 312; Davenport, »Submarine Communications Cables and Law of the Sea« [wie Fn. 21], S. 219. Anderer Auffassung sind z. B. Lagoni/Proelß, »Festlandsockel und ausschließliche Wirtschaftszone« [wie Fn. 54], S. 212f, Rn. 166f; Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 312f. Differenzierend Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz* [wie Fn. 23], S. 217ff. Zumindest zum Schutz von Verdichter-, Pump-, Kontroll- und anderen Begleitinstallationen können Sicherheitszonen nach Art. 60 Abs. 4 SRÜ eingerichtet werden. Siehe Lagoni/Proelß, ebd., S. 213, Rn. 168; Wolf, ebd., S. 197 und S. 217.

60 Siehe Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 313. Zu Australien siehe Holly Elizabeth Matley, »Closing the Gaps in the Regulation of Submarine Cables: Lessons from the Australian Experience«, in: *Australian Journal of Maritime & Ocean Affairs*, 11 (2019) 3, S. 165–184 (173ff).

Rohrleitungen ausgehen können.[61] Hierunter lassen sich auch Maßnahmen fassen, die dazu dienen, Öl- oder Gaspipelines vor Sabotageakten zu schützen.

Im Übrigen enthält das SRÜ Rechtsetzungspflichten für die Verfolgung von Straftaten, die sich gegen Kabel und Rohrleitungen richten. Diese Pflichten gelten sowohl für die Hohe See (dazu im folgenden Abschnitt) als auch für die AWZ. So muss jeder Vertragsstaat die vorsätzliche oder fahrlässige Unterbrechung oder Beschädigung eines Kommunikationskabels, eines Hochspannungskabels oder einer Rohrleitung durch Schiffe, die unter seiner Flagge fahren, oder durch Personen, die seiner Gerichtsbarkeit unterstehen, unter Strafe stellen.[62] Strafbewehrt soll schon jedes Verhalten sein, das darauf gerichtet oder dazu geeignet ist, eine solche Unterbrechung oder Beschädigung herbeizuführen. Das Übereinkommen zum Schutz unterseeischer Telegraphenkabel von 1884,[63] das noch immer in Kraft ist und weitgehend Völkergewohnheitsrecht widerspiegelt[64] (auch in Bezug auf moderne Glasfaserkabel), enthält ähnliche Regelungen. Es geht ebenfalls davon aus, dass die Strafgerichtsbarkeit dem Flaggenstaat sowie dem Staat zufällt, dessen Nationalität die Täter besitzen.

Hohe See

Alle Teile des Meeres, die nicht zu den inneren Gewässern, zum Küstenmeer oder zur AWZ eines Staates oder zu den Archipelgewässern eines Archipelstaates zählen, gehören im seevölkerrechtlichen Sinne zur Hohen See.[65] Die Hohe See steht allen Staaten offen.[66] Die Freiheit der Hohen See beinhaltet unter anderem das Recht, künstliche Inseln und andere völkerrechtlich zulässige Anlagen zu errichten.[67] Sofern der erweiterte Festlandsockel eines Staates über die AWZ hinaus in die Hohe See hineinreicht, gelten für die Errichtung von künstlichen Inseln, Anlagen und Bauwerken in diesem Areal die Vorschriften des Festlandsockelregimes (siehe oben).

Außerdem umfasst die Freiheit der Hohen See das Recht, auf dem Boden der Hohen See jenseits des Festlandsockels Kabel und Rohrleitungen zu verlegen.[68] Auch hier ist der Staat, der die Kabel und Rohrleitungen verlegt bzw. unter dessen hoheitlicher Verantwortung die Verlegung erfolgt, berechtigt, die Leitungen regelmäßig zu inspizieren und sie zu überwachen.[69]

Im Übrigen müssen alle SRÜ-Vertragsstaaten für die Hohe See Gesetze erlassen, wonach jede vorsätzliche oder fahrlässige Unterbrechung oder Beschädigung eines Kabels oder einer Rohrleitung sowie jedes darauf gerichtete oder dazu geeignete Verhalten durch Schiffe, die unter ihrer Flagge fahren, oder durch Personen, die ihrer Gerichtsbarkeit unterstehen, strafbar ist.[70] In der Literatur wird darüber diskutiert, ob ein Staat die Strafverfolgung auch dann aufnehmen darf, wenn ein Flaggen- oder Nationalitätsbezug nicht besteht. Für die Ausübung universeller Gerichtsbarkeit[71] hinsichtlich solcher Taten fehlt es jedoch an einer völkerrechtlichen Grundlage.[72]

Aktive Maßnahmen gegen verdächtige Schiffe auf Hoher See und in der AWZ

Von zentraler Bedeutung ist die Frage, unter welchen Voraussetzungen Staaten aktiv gegen Schiffe vorgehen dürfen, die im Verdacht stehen, Sabotage gegen Kabel oder Rohrleitungen betrieben oder geplant zu haben. Die Freiheit der Hohen See beinhaltet das Recht eines jeden Staates, Schiffe unter eigener Flagge auf Hoher See fahren zu lassen (Freiheit der Schifffahrt).[73] Auf Hoher See unterstehen Schiffe grundsätzlich der ausschließlichen Hoheitsgewalt ihrer Flaggenstaaten.[74] Dies bedeutet, dass sie vor dem Zugriff durch andere Staaten geschützt sind. Dieser Grund-

61 Art. 79 Abs. 2 SRÜ. Siehe auch Art. 208 und 214 SRÜ.
62 Art. 113 SRÜ. Gemäß Art. 58 Abs. 2 SRÜ gilt diese Vorschrift auch für die AWZ.
63 *Convention for the Protection of Submarine Telegraph Cables*, 14.3.1884.
64 Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 297.
65 Art. 86 SRÜ.
66 Art. 87 Abs. 1 S. 1 SRÜ.
67 Art. 87 Abs. 1 S. 3 lit. d SRÜ.
68 Art. 87 Abs. 1 S. 3 lit. c i.V.m. Art. 112 Abs. 1 SRÜ.
69 In Bezug auf Kabel siehe Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 303 und S. 315. In Bezug auf Rohrleitungen siehe Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz* [wie Fn. 23], S. 85 und S. 127.
70 Art. 113 SRÜ.
71 Universelle Gerichtsbarkeit bedeutet, dass ein Staat Taten verfolgen kann, die von Ausländern oder Ausländerinnen im Ausland begangen werden, ohne dass ein Bezug zum Inland gegeben sein muss.
72 Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 314.
73 Art. 87 Abs. 1 S. 2 lit. a i.V.m. Art. 90 SRÜ.
74 Art. 92 Abs. 1 S. 1 SRÜ.

satz unterliegt nur wenigen Ausnahmen. So hat beispielsweise jeder Staat das Recht, ein Seeräuberschiff auf Hoher See aufzubringen.[75] Für den Fall, dass ein Schiff Kabel oder Rohrleitungen sabotiert, statuiert das SRÜ keine universell geltende Eingriffsbefugnis. Insofern liegt das Zugriffsrecht nach der Ordnung der Hohen See allein beim Flaggenstaat. Das gleiche Problem stellt sich in der AWZ. Denn auch dort genießen alle Staaten prinzipiell die Freiheit der Schifffahrt.[76] Selbst der Küstenstaat darf hier nicht in die Freiheit der Schifffahrt eingreifen und Hoheitsgewalt über fremde Schiffe ausüben, es sei denn, der jeweilige Flaggenstaat erteilt seine Zustimmung.

Das Kabelschutzübereinkommen von 1884 sieht zwar vor, dass Schiffe, die im Verdacht stehen, Kabel beschädigt zu haben, von Kriegsschiffen oder anderen speziell autorisierten Schiffen der Vertragsparteien zum Zwecke der strafrechtlichen Beweisaufnahme kontrolliert werden dürfen.[77] Zulässig sind solche Kontrollen auch gegenüber Schiffen fremder Staatszugehörigkeit (ausgenommen sind lediglich fremde Kriegsschiffe und Staatsschiffe, die nicht Handelszwecken dienen). Diese Kontrollbefugnis beschränkt sich jedoch auf die Feststellung der Staatszugehörigkeit des verdächtigen Schiffes. Weitere Schritte zur Verfolgung der Tat bleiben dem Flaggenstaat vorbehalten.

In der Literatur wird indes argumentiert, dass es jedem Staat gestattet sein müsse, »eigene« Kabel vor Angriffen und anderen rechtswidrigen Einwirkungen aktiv zu schützen, etwa auf Grundlage des passiven Personalitätsprinzips[78] oder des Schutzprinzips.[79] Das SRÜ stehe dem nicht entgegen.[80] Diese Argumentation konzentriert sich auf unterseeische Kommunikationskabel, lässt sich aber auch auf Hochspannungskabel und Rohrleitungen übertragen.

Im Übrigen kann in Extremfällen das in Artikel 51 der UN-Charta verbriefte Selbstverteidigungsrecht zum Tragen kommen. Ein Schiff, von dem ein bewaffneter Angriff im Sinne von Artikel 51 ausgeht, darf im Wege der Selbstverteidigung mit Waffengewalt neutralisiert werden.[81] Ob und wann diese Schwelle im Fall von Sabotageakten gegen Kabel oder Rohrleitungen überschritten ist, ist jedoch ungeklärt (dazu sogleich).

Schutz kritischer Seewege in Meerengen

Bestimmte Seewege sind für die internationale Schifffahrt von zentraler Bedeutung. Besonders anfällig für Eingriffe sind Seewege, die durch stark frequentierte Meerengen führen. Der Schutz solcher »Chokepoints« (»Nadelöhre«) ist weder im SRÜ noch in anderen multilateralen seerechtlichen Abkommen systematisch geregelt. Für Meerengen gelten nach dem SRÜ jedoch allgemeine Vorschriften,[82] soweit nicht spezielle internationale Übereinkünfte für einzelne Meerengen Vorrang genießen.[83] Letzteres betrifft etwa die türkischen Meerengen, die dänischen Belts und den Öresund sowie die Straße von Gibraltar.

Die allgemeinen Vorschriften des SRÜ erfassen zwei Kategorien von Meerengen: solche, in denen ein Recht auf Transitdurchfahrt besteht, und solche, in denen die Ordnung der friedlichen Durchfahrt in modifizierter Form zur Anwendung kommt.

Die erste Kategorie bilden Meerengen, die der internationalen Schifffahrt zwischen einem Teil der Hohen See oder einer AWZ und einem anderen Teil der Hohen See oder einer AWZ dienen.[84] Dazu zählen beispielsweise die Straße von Dover und die Straße von Malakka. In solchen Meerengen genießen alle Schiffe und Luftfahrzeuge das Recht der Transitdurchfahrt.[85] »Transitdurchfahrt« bedeutet die in Übereinstimmung mit den einschlägigen Vorschriften erfolgende Ausübung der Freiheit der Schifffahrt und des Überflugs »zum Zweck des ununterbrochenen und zügigen Transits durch die Meerenge«.[86] Schiffe und Luftfahrzeuge, die das Recht der Transitdurchfahrt ausüben, unterliegen währenddessen bestimmten Pflichten. Insbesondere stellt das SRÜ klar, dass sie keine Gewalt gegen die Souveränität, die territoriale Unversehrtheit oder die politische Unabhängigkeit der Meerengen-Anliegerstaaten anwenden oder

75 Art. 105 SRÜ.
76 Art. 58 Abs. 1 SRÜ.
77 Art. X des Übereinkommens zum Schutz unterseeischer Telegraphenkabel [wie Fn. 63].
78 Die Straftat wurde gegen eigene Staatsangehörige begangen.
79 Die Straftat richtet sich gegen bestimmte inländische Rechtsgüter.
80 Zur Argumentation siehe Heintschel von Heinegg, »Protecting Critical Submarine Cyber Infrastructure« [wie Fn. 55], S. 317f. So auch Dinstein/Dahl, *Oslo Manual* [wie Fn. 56], S. 61f.
81 Kaye, »International Measures« [wie Fn. 43], S. 419.
82 Art. 34—45 SRÜ.
83 Art. 35 lit. c SRÜ.
84 Art. 37 SRÜ.
85 Art. 38 SRÜ.
86 Art. 38 Abs. 2 SRÜ.

androhen dürfen.[87] Außerdem sind grundsätzlich sämtliche Tätigkeiten verboten, die nicht mit dem normalen ununterbrochenen und zügigen Transit zusammenhängen.[88] Das Recht der Anliegerstaaten, Vorschriften für die Transitdurchfahrt zu erlassen, ist im Vergleich zur Normsetzungsbefugnis von Küstenstaaten im Küstenmeer begrenzt.[89]

Im SRÜ ist nicht geregelt, wie zu verfahren ist, wenn es zu einer Behinderung kommt, etwa infolge von Unfällen, Sabotage oder terroristischen Akten.

Dahinter steht die Erwägung, dass dem Transitrecht in Meerengen, die der internationalen Schifffahrt dienen, besondere Bedeutung zukommt. Nach dem SRÜ darf die Transitdurchfahrt nicht behindert werden.[90] Allerdings ist darin nicht geregelt, wie verfahren wird, wenn es tatsächlich zu einer Behinderung kommt, etwa infolge von Unfällen, Sabotage oder terroristischen Akten. Das SRÜ schreibt lediglich vor, dass die Anliegerstaaten ihnen bekannte Gefahren für die Schifffahrt oder den Überflug bekannt machen müssen.[91]

Die zweite Kategorie von Meerengen, die das SRÜ in den Blick nimmt, umfasst solche, in denen das Regime der friedlichen Durchfahrt gilt. Hierunter fallen zum einen Meerengen, die zwar der internationalen Schifffahrt dienen und die einen Teil der Hohen See bzw. eine AWZ mit einem anderen Teil der Hohen See oder einer anderen AWZ verbinden, zugleich aber die geografische Besonderheit aufweisen, dass sie zwischen dem Festland und einer Insel ein und desselben Staates liegen, wobei seewärts der Insel »ein in navigatorischer und hydrographischer Hinsicht gleichermaßen geeigneter Seeweg« durch die Hohe See oder durch eine AWZ vorhanden ist.[92] Hierzu zählt die Straße von Messina. Zum anderen findet das Regime der friedlichen Durchfahrt in Meerengen Anwendung, die der internationalen Schifffahrt dienen und die das Küstenmeer eines Staates mit einem Teil der Hohen See oder mit der AWZ eines anderen Staates verbinden.[93] Beispiele sind die Straße von Tiran und der Golf von Akaba. In solchen Meerengen, in denen die Ordnung der friedlichen Durchfahrt greift, sind die Regelungs- und Eingriffsbefugnisse der Anliegerstaaten in Bezug auf die Durchfahrt weitreichender (siehe dazu auch oben die Ausführungen zum Küstenmeer) als in Fällen, in denen das Recht der Transitdurchfahrt besteht. Allerdings darf die Ausübung des Rechts auf friedliche Durchfahrt durch solche Meerengen (anders als im Küstenmeer) nicht ausgesetzt werden.[94]

Völkerrechtliche Regelungen jenseits des Seerechts

Für den Schutz maritimer kritischer Infrastruktur sind neben dem Seevölkerrecht auch andere völkerrechtliche Regelungsregime von Bedeutung. Beispielsweise enthält die Satzung der Internationalen Fernmeldeunion spezielle Verpflichtungen zum Schutz von Kanälen und Anlagen, die für den schnellen und ununterbrochenen Austausch internationaler Telekommunikation notwendig sind.[95]

Soweit es um Angriffe gegen kritische Infrastruktur geht, ergeben sich Konsequenzen aus der Anwendung allgemeiner völkerrechtlicher Normen und Prinzipien. Ein Staat, der im Küstenmeer eines anderen Staates auf Infrastruktur einwirkt, verletzt damit grundsätzlich die Souveränität des anderen Staates. Obgleich Spionage als solche völkerrechtlich nicht verboten ist, stellt etwa das Anzapfen von Datenkabeln zum Zwecke der Überwachung des Telekommunikationsverkehrs einen Eingriff in die Souveränität desjenigen Staates dar, in dessen Territorium die Kabel verlaufen.[96] Außerhalb der Hoheitsgewässer eines Staates

87 Art. 39 Abs. 1 lit. b SRÜ.
88 Art. 39 Abs. 1 lit. c SRÜ.
89 Siehe Art. 42 SRÜ.
90 Art. 38 Abs. 1 und Art. 44 S. 1 SRÜ.
91 Art. 44 S. 1 SRÜ.
92 Art. 45 Abs. 1 lit. a i.V.m. Art. 38 Abs. 1 SRÜ.
93 Art. 45 Abs. 1 lit. b SRÜ.
94 Art. 45 Abs. 2 SRÜ.
95 International Telecommunication Union, *Constitution of the International Telecommunication Union* (1992), Art. 38.
96 Michael N. Schmitt (Hg.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2. Aufl., Cambridge 2017, S. 257. Das *Tallinn Manual 2.0* ist kein offizielles Dokument. Es versteht sich nicht als Referenzquelle für Positionen der Nato oder einzelner Staaten, sondern spiegelt den Herausgebern zufolge allein die persönlichen Auffassungen der beteiligten Experten wider. Sein Anspruch besteht darin, das auf Cyberoperationen anwendbare geltende Völkerrecht in Form kommentierter Regeln darzustellen.

sind solche Aktionen hingegen nicht als Souveränitätsverletzung einzustufen.[97]

Unter welchen Voraussetzungen die Sabotage unterseeischer Rohrleitungen die Schwelle zum bewaffneten Angriff überschreitet, wird kontrovers diskutiert.

Ein Eingriff in die völkerrechtlich geschützte souveräne Sphäre des Küstenstaates unter Ausübung von Zwang verstößt gegen das Interventionsverbot. Bei Anwendung von Gewalt steht auch eine Verletzung von Artikel 2 Nummer 4 der UN-Charta[98] und gegebenenfalls sogar ein bewaffneter Angriff im Sinne von Artikel 51 der Charta im Raum. Eine Gewaltanwendung kann, je nach Ausmaß und Folgen, auch auf Hoher See als bewaffneter Angriff zu werten sein. Unter welchen Voraussetzungen etwa die Sabotage unterseeischer Rohrleitungen die Schwelle zum bewaffneten Angriff überschreitet, wird vor dem Hintergrund der Sprengung der Nord-Stream-Pipelines derzeit noch kontrovers diskutiert.[99]

Völkerrechtswidrige Akte, die keinen bewaffneten Angriff darstellen, dürfen von dem betroffenen Staat nur mit verhältnismäßigen Gegenmaßnahmen unterhalb der Schwelle des Gewalteinsatzes beantwortet werden.[100] Erst wenn ein bewaffneter Angriff vorliegt oder unmittelbar bevorsteht, kann sich der betroffene Staat in Ausübung seines Selbstverteidigungsrechts mit Waffengewalt zur Wehr setzen. Dies gilt im Fall staatlicher Angriffe ebenso wie bei Angriffen, die von nichtstaatlichen Akteuren ausgeführt werden. Sogar Cyberattacken können den Tatbestand einer Gewaltanwendung und eines bewaffneten Angriffs erfüllen. In Extremfällen können sich Staaten zum Schutz kritischer Infrastruktur unter engen Voraussetzungen auch auf Notstand berufen, um Maßnahmen zu rechtfertigen, die eigentlich völkerrechtswidrig wären.[101] Relevant wird dies zum Beispiel, wenn ein Staat kritische Infrastruktur aktiv gegen Cyberangriffe verteidigt und durch seine Hackbacks unbeteiligte Staaten zu Schaden kommen.[102] Für die Einordnung und Aufarbeitung solcher Zwischenfälle spielt das Recht der Staatenverantwortlichkeit mit seinen Zurechnungs- und Haftungsregeln eine zentrale Rolle.

Der Übergang zum bewaffneten Konflikt

Im Fall eines bewaffneten Konflikts kommt das humanitäre Völkerrecht zur Anwendung. In einer solchen Situation kann maritime kritische Infrastruktur zu einem militärischen Ziel werden, das unter Einhaltung der sonstigen Vorschriften des humanitären Völkerrechts von der gegnerischen Konfliktpartei angegriffen werden darf. Als militärische Ziele gelten »Objekte, die aufgrund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den zu dem betreffenden Zeitpunkt gegebenen Umständen einen eindeutigen militärischen Vorteil darstellt«.[103] Danach können etwa Transportsysteme und Hafenanlagen im Einzelfall militärische Ziele dar-

97 Ebd.

98 Gemäß Art. 2 Nr. 4 der UN-Charta unterlassen alle Staaten in ihren internationalen Beziehungen jede gegen die territoriale Unversehrtheit oder die politische Unabhängigkeit eines Staates gerichtete oder sonst mit den Zielen der Vereinten Nationen unvereinbare Androhung oder Anwendung von Gewalt.

99 Siehe z. B. Danae Azaria/Geir Ulfstein, »Are Sabotage of Submarine Pipelines an ›Armed Attack‹ Triggering a Right to Self-defence?«, *EJIL:Talk!* (Blog), 18.10.2022, <https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/>; Alexander Lott, »Attacks against Europe's Offshore Infrastructure within and beyond the Territorial Sea under Jus ad Bellum«, *EJIL:Talk!* (Blog), 17.10.2023, <https://www.ejiltalk.org/attacks-against-europes-offshore-infrastructure-within-and-beyond-the-territorial-sea-under-jus-ad-bellum/>. Dazu auch Christian Schaller, *Spionage und Sabotage vor Europas Küsten – Kritische Infrastruktur im Fadenkreuz*, Berlin: Stiftung Wissenschaft und Politik, 2024 (SWP-Studie 2024), in Vorbereitung.

100 Siehe Art. 22 und 49ff der *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Report of the International Law Commission on the Work of Its 53rd Session (2001) (UN-Dok. A/56/10*).

101 Siehe Art. 25 der *Draft Articles on Responsibility of States* [wie Fn. 100].

102 Dazu Christian Schaller, »Aktive Cyberabwehr und Notstand im Völkerrecht«, in: *Zeitschrift für das Gesamte Sicherheitsrecht*, 1 (2018) 2, S. 57–61.

103 So die völkergewohnheitsrechtlich anerkannte Definition, die in Art. 52 Abs. 2 des I. Zusatzprotokolls zu den Genfer Abkommen Ausdruck gefunden hat (*Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts* [Protocol I], 8.6.1977, UNTS, Bd. 1125 [1979], S. 3).

stellen.[104] Auch unterseeische Stromkabel und Rohrleitungen, die von den Konfliktparteien genutzt werden, dürfen angegriffen werden, sofern sie wirksam zu militärischen Handlungen beitragen und die übrigen Voraussetzungen der Definition erfüllt sind.[105] Das *Tallinn Manual 2.0* geht davon aus, dass Cyberinfrastruktur, die zugleich zivilen und militärischen Zwecken dient, insgesamt als militärisches Ziel zu betrachten ist.[106] Hingegen sieht das *San Remo Manual*, das bewaffnete Konflikte auf See zum Gegenstand hat, die kriegführenden Parteien in der Pflicht, darauf zu achten, dass sie unterseeische Kabel und Rohrleitungen, die nicht ausschließlich den Kriegführenden dienen, nicht beschädigen.[107] Moderne Glasfaserkabel, die das Rückgrat des internationalen Datenverkehrs bilden, dürften nach der Logik des *San Remo Manuals* also eher nicht zum Ziel von Angriffen werden.[108]

104 Wolff Heintschel von Heinegg, »Friedliche Nutzung, Seekriegs- und Neutralitätsrecht, Friedenssicherung«, in: Graf Vitzthum (Hg.), *Handbuch des Seerechts* [wie Fn. 15], S. 491–623 (575, Rn. 190).

105 Allerdings ist zu differenzieren: Kabel und Rohrleitungen, die ein besetztes Gebiet mit dem Territorium eines neutralen Staates verbinden, dürfen nicht zerstört werden. Kabel und Rohrleitungen, die einzelne Teile feindlichen Territoriums (das nicht besetzt ist) verbinden oder von dort in das Territorium eines neutralen Staates führen, dürfen hingegen nach Maßgabe des Seekriegsrechts unterbrochen werden, sofern dies militärisch notwendig ist (Wolff Heintschel von Heinegg, »The Law of Armed Conflict at Sea«, in: Dieter Fleck [Hg.], *The Handbook of International Humanitarian Law*, 2. Aufl., Oxford 2008, S. 475–596 [514f]).

106 Schmitt (Hg.), *Tallinn Manual 2.0* [wie Fn. 96], S. 445ff.

107 *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, San Remo 1994, Regel 37. Auch bei diesem Handbuch handelt es sich nicht um ein offizielles Dokument.

108 Dinstein/Dahl, *Oslo Manual* [wie Fn. 56], S. 63.

Sektoren

Jacopo Maria Pepe

Der Schutz kritischer maritimer Energieinfrastrukturen: Bedeutung, Risiken, Prioritäten*

Einleitung und Problemstellung

Die Anschläge auf die Gaspipelines Nord Stream 1 und 2 haben das Thema der Resilienz der Energieinfrastruktur ins Zentrum öffentlicher und politischer Aufmerksamkeit gerückt. Im Kontext des russischen Angriffskrieges gegen die Ukraine hat dies für Europa, aber insbesondere für Deutschland zweierlei Folgen.

Zum einen wächst die Relevanz maritimer Infrastruktur für die Energieversorgungssicherheit des Landes drastisch. Kurz- bis mittelfristig bleibt vor allem die Versorgung mit Erdgas eine Notwendigkeit. Durch die Entscheidung, sich von Pipelinelieferungen aus Russland abzukoppeln, haben nun aber ausschließlich *maritime* Gaslieferungen, vor allem aus dem Norden und Westen, und im Zuge dessen sowohl alternative Offshore-Pipelines als auch Lieferungen von Flüssigerdgas (LNG) enorm an Bedeutung gewonnen. Mittel- bis langfristig wird sich diese Tendenz als Folge der ambitionierten Klimaziele der Bundesregierung weiter festigen. Dabei rücken auch Offshore-Windanlagen,[1] Stromanbindungsleitungen an das Festland sowie maritime »hybride Interkonnektoren«,[2] aber auch Schiffe und nicht zuletzt Häfen in den Fokus. Diese Umorientierung weg von kontinentalen und von Osten kommenden hin zu ausschließlich maritimen, größtenteils von Westen kommenden Energieflüssen stellt für eine Wirtschaftsmacht wie Deutschland eine geradezu kopernikanische Wende dar.

Zum anderen hat Russlands Angriffskrieg dazu geführt, dass die geopolitischen Spannungen im maritimen Raum zunehmen. Bis zum Kriegsausbruch galt insbesondere in Deutschland die Energieinfrastruktur im Osten des Kontinents trotz der wachsenden geopolitischen Spannungen mit Russland nicht als Zielobjekt hybrider oder asymmetrischer Kriegführung. Die genannten Anschläge gegen beide Ostsee-Pipelines haben nun die auf deutscher und EU-Ebene ohnehin bestehende Neigung verstärkt, die Energieversorgung vermehrt durch eine sicherheitspolitische Brille zu betrachten. Ohne weitere Ausdifferenzierung könnte dies jedoch schnell zu einer problematischen »Versicherheitlichung«[3] der energiepolitischen Debatte führen, die sich dysfunktional oder gar kontraproduktiv auf die Versorgungssicherheit Europas und Deutschlands auswirken würde.

Daher stellt sich zunächst die grundsätzliche Frage, welche maritimen Infrastrukturen tatsächlich von kritischer Bedeutung für die Energieversorgung sind. Des Weiteren geht es darum, zu bestimmen, ob und in welchen Fällen gerade der militärische Schutz bestehender maritimer Energieinfrastruktur hinreichend und über den nationalen Rahmen hinaus

* Der Autor dankt Rosa Melissa Gehrung, Forschungsassistentin der Forschungsgruppe Globale Fragen, sehr für ihre Hilfe bei der Recherche sowie für die wertvollen Kommentare und zahlreichen Überarbeitungen des Manuskripts.

1 Bundesministerium für Wirtschaft und Klimaschutz (BMWK), »BMWK und ÜNB [Übertragungsnetzbetreiber; J. M. P.] veröffentlichen Pläne zur Vernetzung von Offshore-Windparks in der Nordsee«, Berlin, 27.2.2023, <https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2023/02/20230227-bmwk-und-uenb-veroeffentlichen-plaene-zur-vernetzung-von-offshore-windparks-in-der-nordsee.html>.

2 Hybride Interkonnektoren sind Stromleitungen, die über die Grenze zweier benachbarter Länder führen und deren Offshore-Windparks miteinander vernetzen. Siehe BMWK, »BMWK und ÜNB veröffentlichen Pläne zur Vernetzung von Offshore-Windparks in der Nordsee« [wie Fn. 1].

3 Ein Thema kann durch Sprache und (Bedrohungs-)Diskurse ein Teil der Sicherheitspolitik werden, unabhängig von der tatsächlichen Natur dieser Bedrohung. Siehe Barry Buzan/Ole Waever/Jaap de Wilde, *Security. A New Framework for Analysis*, Boulder, CO: Lynne Rienner Publishers Inc, 1997.

gewährleistet werden kann. Und schließlich gilt es mit Blick auf Deutschland zu klären, welche Akteure einbezogen und wie deren Kompetenzen und Aufgaben neu bzw. umverteilt werden sollten.

Dabei geht das Verständnis der *kritischen* maritimen Energieinfrastruktur in diesem Beitrag über die Definition des KRITIS-Dachgesetzes hinaus und bezieht neben geltenden Kriterien und Schwellenwerten insbesondere auch die Handlungsmöglichkeiten der Akteure je nach identifiziertem Schutzgrad der Infrastrukturobjekte mit ein.

Die wachsende Bedeutung maritimer Energieinfrastruktur für Deutschland und die EU

Die energie- und sicherheitspolitischen Folgen des Ukraine-Kriegs sowie die klimapolitischen Prioritäten der EU und der Bundesregierung rücken kurz- bis mittelfristig zwei Arten maritimer Energieinfrastruktur in den Fokus: Zum einen bilden LNG-Terminals an Land, sogenannte schwimmende Terminals (Floating Terminals) auf See, LNG-Schiffe und zukünftig Frachter für Wasserstoff,[4] aber auch Unterseepipelines das infrastrukturelle Rückgrat der Gasversorgung. Zum anderen wird sich ein bedeutender Teil des kontinentalen und insbesondere des deutschen Strombedarfs mittelfristig durch Offshore-Windparks sowie über entsprechende Stromanbindungsleitungen und »hybride Interkonnektoren« decken lassen.

Gas: LNG-Terminals, Schiffe und Offshore-Pipelines

Laut International Energy Agency wird die EU-Nachfrage nach Erdgas zwar bis 2030 von 421 Milliarden Kubikmeter (2021) auf 340 Milliarden Kubikmeter sinken.[5] Dies aber nur, wenn die EU die 2022 im Plan REPowerEU[6] angekündigten Maßnahmen zur Steigerung der Energieeffizienz und zu nachfrageseitigen Einsparungen sowie den beschleunigten Ausbau erneuerbarer Energien und die Ziele ihres »Fit for 55«-Pakets[7] tatsächlich umsetzt.

Deutschland nimmt in diesem Kontext eine Sonderstellung ein. Im Jahr 2021 machte hier Erdgas knapp über 25 Prozent[8] des Energiemixes und 13 Prozent[9] des Strommixes aus. Auch im Kriegsjahr 2022 blieb Gas für Industrie und Haushalte mit einem Anteil von 23,6 Prozent eine entscheidende Energiequelle.[10] Mit Blick auf die begrenzten Eigenproduktionskapazitäten[11] wird sich an der Abhängigkeit von Gasimporten, die zurzeit 95 Prozent ausmachen, kaum etwas ändern.[12]

Während aber 2021 noch etwa 45 Prozent[13] der europäischen und 52 Prozent[14] der deutschen Gas-

4 Gemäß einem erweiterten, dynamischen Verständnis des Begriffs nach Brian Larkin (»The Politics and Poetics of Infrastructure«, in: *Annual Review of Anthropology*, 42 [2013], S. 327–343 [328]) lässt sich Infrastruktur verstehen als »built networks that facilitate the flow of goods, people, or ideas and allow for their exchange over space«. Schiffe zählen in diesem Beitrag zu maritimer Energieinfrastruktur im erweiterten Sinne, da sie mobiler Teil des Logistiknetzwerks sind, das den Energiehandel und die Versorgung ermöglicht.

5 International Energy Agency (IEA), *World Energy Outlook 2022*, Paris, November 2022, S. 453, <https://iea.blob.core.windows.net/assets/830fe099-5530-48f2-a7c1-11f35d510983/WorldEnergyOutlook2022.pdf>.

6 Europäische Kommission, »REPowerEU: erschwingliche, sichere und nachhaltige Energie für Europa«, <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_de>.

7 Europäischer Rat, »Fit for 55«, <https://www.consilium.europa.eu/de/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/>.

8 Arbeitsgemeinschaft Energiebilanzen (AGEB), »AG Energiebilanzen legt Bericht für 2021 vor«, Pressemitteilung, Berlin, 28.3.2022, <https://ag-energiebilanzen.de/ag-energiebilanzen-legt-bericht-fuer-2021-vor/>.

9 Destatis, »Stromerzeugung 2022: Ein Drittel aus Kohle, ein Viertel aus Windkraft«, 9.3.2022, <https://www.destatis.de/DE/Presse/Pressemitteilungen/2023/03/PD23_090_43312.html>.

10 AGEB, »AG Energiebilanzen legt Bericht für 2022 vor«, Pressemitteilung, Berlin, 17.4.2023, <https://ag-energiebilanzen.de/ag-energiebilanzen-legt-bericht-fuer-2022-vor/>.

11 BMWK, *Bericht des Bundeswirtschafts- und Klimaschutzministeriums zu Planungen und Kapazitäten der schwimmenden und festen Flüssigerdgasterminals* (online), Berlin, 3.3.2023, <https://www.bmwk.de/Redaktion/DE/Downloads/Energie/20230303-lng-bericht.pdf?__blob=publicationFile&v=6>.

12 Destatis, »Fakten zur Gasversorgung: Erdgas wichtigster Energieträger für Industrie und private Haushalte«, 21.7.2021, <https://www.destatis.de/DE/Presse/Pressemitteilungen/2022/07/PD22_N044_43.html>.

13 IEA, »How Europe Can Cut Natural Gas Imports from Russia Significantly within a Year«, Pressemitteilung, 3.3.2022, <https://www.iea.org/news/how-europe-can-cut-natural-gas-imports-from-russia-significantly-within-a-year>.

14 Bundesnetzagentur (BNetzA), »Bundesnetzagentur veröffentlicht Zahlen zur Gasversorgung 2022«, Pressemittei-

importe aus Russland stammten, sind die Anteile nach dem Kriegsausbruch und im Laufe des Jahres 2022 kontinuierlich zurückgegangen. Im Juni 2023 betrug er EU-weit nur noch 20 Prozent.[15] Deutschlands Pipeline-Importe aus Russland sind seit Ende August 2022 auf null gesunken.[16]

Als Folge ist der Anteil des durch Onshore-Pipelines gelieferten Erdgases an den gesamten EU-Importen um 46 Prozent zurückgegangen. Dadurch haben insbesondere LNG-Importe an Bedeutung gewonnen: Der LNG-Anteil an den EU-Gaslieferungen betrug 2022 fast 39 Prozent.[17] Hauptlieferanten waren die Vereinigten Staaten und Katar mit 72 bzw. 25 Milliarden Kubikmetern.[18] Russlands LNG-Lieferungen an die EU stiegen im gesamten Jahr 2022 zwar auf fast 19 Milliarden Kubikmeter und sanken im Jahr 2023 nur leicht.[19] Allerdings sollen diese Lieferungen laut EU mittelfristig schrittweise eingestellt werden.

Um dieses zusätzliche Volumen abwickeln zu können, plant die EU, den Ausbau von Regasifizierungskapazitäten und LNG-Terminals an ausgewählten Hafenterminals zu beschleunigen. Im Jahr 2015 waren in der EU 27 LNG-Terminals in Betrieb,[20] in Deutschland gibt es bisher kein einziges landgebundenes Terminal. Die für den deutschen Markt bestimmten LNG-Importe gelangen momentan nahezu ausschließlich über Anlandestellen in Frankreich, Belgien und den Niederlanden ins hiesige Gasnetz.[21] Seit dem Ausbruch des Ukraine-Kriegs plant die Bundesregierung allerdings, bis 2026/27 drei landseitige LNG-Terminals in Wilhelmshaven, Brunsbüttel und Stade sowie bis Ende 2025 fünf schwimmende Terminals (Wilhelmshaven I und II, Lubmin, Brunsbüttel und Stade) mit einer Nominalkapazität von 54 Milliarden Kubikmetern erstmalig in Betrieb zu nehmen.[22]

Durch die Abkoppelung von Russland orientiert sich der Gasmarkt der EU zunehmend gen (Nord-)Westen und Süden.

Durch die Abkoppelung von Russland orientiert sich der Gasmarkt der EU somit zunehmend gen (Nord-)Westen und Süden, so dass insbesondere die Mittelmeer-Atlantik-Routen als Hauptlieferwege dienen. Infolgedessen gewinnen auch LNG-Schiffe an strategischer Bedeutung. Um eine Menge von 167 Milliarden Kubikmeter Gas zu ersetzen, wie sie Russland im Jahr 2020 in die EU geliefert hat, bräuchte man rund 1.800 Schiffsladungen.[23] Für Deutschland hieße das ab 2027 etwas mehr als zwei Ladungen pro Tag. Dafür wären etwa 160 neue Tanker nötig, die momentan jedoch ein knappes Gut sind. Zukünftig könnten außerdem weitere Schiffe für den Transport von Wasserstoff aus den Golfstaaten, aus Südamerika oder Australien unabdingbar werden. Schätzungen zufolge wird sich im Jahr 2030 die Nachfrage nach Wasserstoff europaweit auf 20 Millionen Tonnen[24] und deutschlandweit auf ungefähr 95 bis 130 Terawattstunden (etwa 2,85 bis 3,9 Millionen Tonnen)[25] belau-

lung, Berlin, 6.1.2023, <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2023/20230106_RueckblickGasversorgung.html>.

15 Europäische Kommission, *Quarterly Report on European Gas Markets*, 16 (2023) 2, S. 10, <https://energy.ec.europa.eu/system/files/2023-12/New_Quarterly_Report_on_European_Gas_markets_Q2_2023.pdf>.

16 BNetzA, »Bundesnetzagentur veröffentlicht Zahlen zur Gasversorgung 2022« [wie Fn. 14].

17 Eigene Berechnungen auf Basis von Diane Elijah, »Global LNG Represents 39% of EU Gas Imports in 2022«, *KPLER*, 5.1.2023, <https://www.kpler.com/blog/global-lng-represents-39-of-eu-gas-imports-in-2022>. Gilt für den gesamten Absatz, wenn nicht anders angegeben.

18 Institute for Energy Economics and Financial Analysis (IEEFA), *Europe's LNG Imports*, 2022 »European LNG Tracker«, Lakewood, OH, 2023, <https://ieefa.org/european-lng-tracker>.

19 »Russian LNG Exports to Europe Fell 1.9% in 2023 — LSEG Data«, *Reuters*, 2.1.2024, <https://www.reuters.com/business/energy/russian-lng-exports-europe-fell-19-2023-lseg-data-2024-01-02/>.

20 Gas Infrastructure Europe, *The European LNG Terminal Infrastructure 2015: Status and Outlook*, Abstract LNG Map & Investment Database 2015, 17.6.2015, S. 4, <https://www.gie.eu/wp-content/uploads/filr/2544/20150617%20GLE%20LNG%20abstract_final.pdf>.

21 Ebd.

22 BMWK, *Bericht des Bundeswirtschafts- und Klimaschutzministeriums zu Planungen und Kapazitäten der schwimmenden und festen Flüssigerdgasterminals* [wie Fn. 11], S. 54.

23 Institut für Seeverkehrswirtschaft und Logistik, »Der Angriff Russlands auf die Ukraine stellt die LNG Schifffahrt vor sehr große Herausforderungen«, Pressemitteilung, 1.4.2022, <https://nachrichten.idw-online.de/2022/04/01/der-angriff-russlands-auf-die-ukraine-stellt-die-lng-schifffahrt-vor-sehr-grosse-herausforderungen?groupcolor=5>.

24 Europäische Kommission, »Hydrogen«, <https://energy.ec.europa.eu/topics/energy-systems-integration/hydrogen_en>.

25 BMWK, *Fortschreibung der Nationalen Wasserstoffstrategie*, Berlin, Juli 2023, S. 6, <https://www.bmbf.de/SharedDocs/Downloads/de/2023/230726-fortschreibung-nws.pdf?__blob=publicationFile&v=1l>.

fen. In diesem Zusammenhang wird auch Häfen als Bestandteil von Wasserstoff-Clustern eine entscheidende Rolle zukommen.

Darüber hinaus wird die Infrastruktur von Offshore-Pipelines für Erdgas immer größere Bedeutung erlangen, wenngleich diese Entwicklung differenzierter betrachtet werden muss. Pipelinegebundene Importe aus Norwegen, Nordafrika und Aserbaidschan, den einzigen Alternativen zu Russland, lassen sich aufgrund der Förderkapazitäten der Exporteure nur in begrenztem Umfang erhöhen. Prognosen rechnen daher nur mit einem eingeschränkten Anstieg, wenn nicht gar einer Stagnation.[26] Schließlich könnten aber mittelfristig Pipelines nicht nur aus Norwegen, sondern auch im Mittelmeer indirekt für Deutschlands Wasserstoffversorgung wichtig werden. So wird erwartet, dass bis 2050 etwa 47 Prozent der weltweiten Wasserstoffflüsse im europäischen Markt per Pipeline transportiert werden.[27]

Strom: Offshore-Windparks, Stromanbindungsleitungen und Interkonnektoren

Nach dem schon erwähnten RePowerEU-Plan soll der Anteil erneuerbarer Energien am Strommix in der EU bis 2030 auf 45 Prozent steigen.[28] Der Einsatz von Offshore-Windenergie ist das Kernelement bei der Umsetzung des 2019 vorgestellten europäischen Green Deals. Die installierte Offshore-Windkraftkapazität in der EU soll von 14,6 Gigawatt (GW) (2021)[29] auf rund 111 GW im Jahr 2030[30] steigen.

Deutschland wird im Zuge der Energietransformation zusehends von Offshore-Windanlagen abhängig sein.

Deutschland wird im Zuge der Energietransformation zunehmend von Offshore-Windanlagen abhängig sein. Bei ihren Bemühungen, die höher gesteckten Elektrifizierungsziele (ein Anteil von 80 Prozent erneuerbaren Energien am Strommix bis 2030[31]) zu erreichen, setzt die amtierende Bundesregierung stark auf den Ausbau von Windkraftanlagen. Laut dem 2022 verabschiedeten »Osterpaket« der Bundesregierung und dem im selben Jahr novellierten Windenergie-auf-See-Gesetz soll die Leistung bis zum Jahr 2030 auf insgesamt mindestens 30 GW gesteigert werden.[32] Obwohl der Hauptteil der Windenergiekapazität an Land generiert wird, dürfte der Anteil von Offshore-Windanlagen überproportional wachsen. Betrug das Verhältnis zwischen Windkraftkapazität auf See und an Land im Jahr 2022 noch 1:7, soll es 2030 bei 1:4 liegen.[33] In der Folge gewinnen Umspannwerke und Vernetzungskabel auf See sowie vor allem Stromanbindungsleitungen zum Land und hybride Interkonnektoren an Relevanz.[34]

Für Europa, aber insbesondere für Deutschland ist die Nordsee der Hotspot für Offshore-Windenergie. Im Jahr 2021 befanden sich von den damals betriebenen deutschen Windparks 21 in der Nordsee und

26 Energiewirtschaftliches Institut an der Universität zu Köln (EWI), »Europäischer Gasmarkt orientiert sich nach Westen«, 22.9.2022, <https://www.ewi.uni-koeln.de/de/aktuelles/gasmaerkte-2030/#:~:text=Reduktion%20der%20Gasnachfrage%20ist%20wesentlicher,Russland%20beschr%C3%A4nkt%20ist%20oder%20nicht>.

27 International Renewable Energy Agency (IRENA) (Hg.), *Global Hydrogen Trade to Meet the 1.5°C Climate Goal: Part I – Trade Outlook for 2050 and Way Forward*, Abu Dhabi 2022, S. 7, <https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2022/Jul/IRENA_Global_hydrogen_trade_part_1_2022_.pdf>.

28 Europäische Kommission, »REPowerEU: Ein Plan zur raschen Verringerung der Abhängigkeit von fossilen Brennstoffen aus Russland und zur Beschleunigung des ökologischen Wandels«, Pressemitteilung, Brüssel, 18.5.2022, <https://ec.europa.eu/commission/presscorner/detail/de/ip_22_3131>.

29 Europäische Kommission, »Offshore Renewable Energy«, <https://energy.ec.europa.eu/topics/renewable-energy/offshore-renewable-energy_en>.

30 Europäische Kommission, »Member States Agree New Ambition for Expanding Offshore Renewable Energy«, Pressemitteilung, 19.1.2023, <https://energy.ec.europa.eu/news/member-states-agree-new-ambition-expanding-offshore-renewable-energy-2023-01-19_en>.

31 BMWK, »Ziele«, <https://www.erneuerbare-energien.de/EE/Navigation/DE/Technologien/Windenergie-auf-See/Ziele/ziele.html>.

32 BMWK, *Überblickspapier Osterpaket*, Berlin, 6.4.2022, <https://www.bmwk.de/Redaktion/DE/Downloads/Energie/0406_ueberblickspapier_osterpaket.pdf?__blob=publicationFile&v=12>.

33 Eigene Berechnung auf Basis von Deutsche Windguard, »Windenergie-Statistik: Jahr 2022«, 2022, <https://www.windguard.de/jahr-2022.html>.

34 Zur Verortung dieser Infrastrukturen siehe BMWK, *Ansätze eines Offshore-Stromnetzes in der Ausschließlichen Wirtschaftszone (AWZ)*, Schlussbericht für das Projekt Nr. 014/217.2.2023, <https://www.bmwk.de/Redaktion/DE/Publikationen/Energie/ansaetze-eines-offshore-stromnetzes-in-der-ausschliesslichen-wirtschaftszone-awz.pdf?__blob=publicationFile&v=3>; Deutscher Bundestag, *Maritime Raumordnung in der Ausschließlichen Wirtschaftszone Deutschlands. Überblick über Akteure und Zuständigkeiten*, 31.8.2022, <https://www.bundestag.de/resource/blob/918050/2aefbc158a3a2f627cdc51f395c266a6/WD-5-091-22-WD-8-056-22-WD-2-055-22-pdf-data.pdf>.

lediglich vier in der Ostsee.[35] In Bau oder geplant bis 2030 sind zusätzliche elf in der Nordsee und vier in der Ostsee.[36] Dabei finden die aktuelle Nutzung und der weitere Ausbau zwar in deutschen Gewässern statt, aber vornehmlich in der ausschließlichen Wirtschaftszone (AWZ) und damit außerhalb der Zwölf-Seemeilen-Zone (Küstengewässer), was ihren zukünftigen Schutz erheblich erschwert.

Zwischen erhöhtem Schutzbedarf und dem Risiko einer dysfunktionalen Versicherheitlichung

Energiepolitik zielt im Optimalfall auf eine austarierte Kombination von Versorgungssicherheit, Umweltverträglichkeit und Wirtschaftlichkeit ab.[37] In Europa und in Deutschland wurde der Fokus lange Zeit vor allem auf die letzten beiden Faktoren gelegt. Dabei wurden nicht nur Abhängigkeiten, sondern auch potentielle Bedrohungen oder Risiken für kritische Energieinfrastruktur und Lieferketten ignoriert und unterschätzt. Erst der Ukraine-Krieg, der russische Energielieferstopp und die Anschläge auf die Nord-Stream-Pipelines haben zu einem Umdenken geführt und die Versorgungssicherheit und den Schutz kritischer Energieinfrastruktur stärker in den Fokus gerückt.

Dabei ist die politische Debatte — gerade in den Wochen und Monaten nach den Anschlägen — zunehmend durch eine sicherheitspolitische Sichtweise geprägt worden, ohne allerdings detaillierter auf Prioritäten einzugehen, die für die zu schützende Infrastruktur gelten sollten.[38] Angesichts zunehmender geopolitischer Spannungen und aufflammender Großmachtrivalitäten muss die sicherheitspolitische und militärische Dimension der Energieversorgung zweifellos stärker betont und aufgewertet werden. Zugleich bedarf es jedoch einer frühzeitigen, sachlichen und differenzierten Diskussion darüber, von welchen Bedrohungen und Risiken konkret auszugehen ist und mit welchen Instrumenten und Akteuren ihnen angemessen begegnet werden kann. Nur so lassen sich Prioritäten für die zu schützende Infrastruktur setzen, und nur so lässt sich der Gefahr einer dysfunktionalen oder gar schädlichen Versicherheitlichung der Energieversorgungssicherheit vorbeugen.

Nimmt man »maritime Sicherheit« als undifferenzierten Sammelbegriff für unterschiedliche Bedrohungen — wie Drogenhandel, Piraterie, Umweltkatastrophen, gefährliche Fracht, militärische Zusammenstöße und staatliche oder illegale Aktivitäten —, gerät der maritime Raum tendenziell zu einem »Knotenpunkt diverser überlappender Versicherheitlichungen«, die es erschweren, Handlungsprioritäten zu setzen.[39] In der Folge wird sein Schutz auch nicht in ein Verhältnis zu Kosten, Nutzen und (begrenzten) Ressourcen gesetzt. Die Gefahr ist groß, dass auf diese Weise zum einen konkrete Bedrohungen für die Versorgungssicherheit nicht erkannt oder falsch konstruiert werden und dass sich zum anderen das Ziel eines allumfassenden Schutzes als unrealistisch und

35 Bundesministerium des Innern (BMI), *Raumordnungsplan für die deutsche ausschließliche Wirtschaftszone in der Nordsee und Ostsee*, Berlin, 1.9.2021, S. 5, <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/08/awz-auswertung-beteiligung-9-abs2-rog.pdf?__blob=publicationFile&v=5>.

36 Deutsche Windguard, *Status des Offshore-Windenergieausbaus in Deutschland*, 2023, S. 5, <https://www.windenergie.de/fileadmin/redaktion/dokumente/publikationen-oeffentlich/themen/06-zahlen-und-fakten/20230725_Status_des_Offshore-Windenergieausbaus_Halbjahr_2023.pdf>; BNetzA, »Ergebnisse der Offshore-Ausschreibungen für zentral voruntersuchte Flächen«, Pressemitteilung, Berlin, 10.8.2023, <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2023/20230810_OffshoreErgebnisse.html?nn=265778>; Vattenfall, »Vattenfall plant weiteren großen Offshore-Windpark in der Nordsee«, Pressemitteilung, 14.9.2023, <https://group.vattenfall.com/de/newsroom/pressemitteilungen/2023/vattenfall-plant-weiteren-groben-offshore-windpark-in-der-nordsee>.

37 Karen Pittel, *Das energiepolitische Zieldreieck und die Energiewende*, München: Ifo-Institut, 2021, S. 22, <https://www.ifo.de/DocDL/ifosd_2012_12_7.pdf>.

38 Zur Debatte siehe u. a. das Statement von Ursula von der Leyen: »Critical infrastructure is the new frontier of warfare« (Eszter Zalan, »Von der Leyen: EU Must Now Protect Critical Infrastructure«, *EU Observer*, 10.10.2022, <https://euobserver.com/world/156259>); oder das von Bundesinnenministerin Nancy Faeser: »alles, was schwimmen kann, ist auf dem Wasser [in Bezug auf Einsatz von Schiffen der Bundespolizei]« (zit. in: BMI, »›Die Sicherheit unserer kritischen Infrastruktur hat höchste Priorität‹«, 17.10.2022, <https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2022/10/schutz-kritischer-infrastrukturen.html>).

39 Siehe hierzu Christian Bueger, »Theorien der Maritimen Sicherheit Versicherheitlichungstheorie und sicherheitspolitische Praxeographie«, in: Sebastian Bruns u. a. (Hg.), *Maritime Sicherheit*, Wiesbaden: Springer Verlag, 2013, S. 25—36 (31).

allzu ambitioniert erweist, weil Akteure, Instrumente und Ressourcen kontraproduktiv eingesetzt werden.

Kritische Infrastrukturen aus der Perspektive Deutschlands

Kriterien für einen effektiven Schutz

Um tatsächliche Bedrohungen für die deutsche Energieversorgung identifizieren zu können, ist zunächst klarzustellen, was als *kritische* maritime Energieinfrastruktur gelten soll. In diesem Beitrag geht das Verständnis von Kritikalität in Bezug auf maritime Energieinfrastruktur über die dem KRITIS-Dachgesetzentwurf zugrundeliegende Definition[40] hinaus; konkret schließt sie die folgenden drei selbstausgearbeiteten Kriterien als erste Orientierung ein:[41] erstens den Grad der Abhängigkeit von einem Energieträger und dazugehöriger Infrastruktur sowie daraus resultierender Kaskadeneffekte unter Einbezug des Zeithorizonts bis und ab 2030; zweitens die Entfernung der zu schützenden Infrastruktur von Territorialgewässern und Küstenmeer, die wichtig ist für die Identifizierung der Schutz- und Interventionsmöglichkeiten; drittens die lokale, regionale (im Umfeld der Infrastruktur) und globale geopolitische Sicherheitslage im Umfeld der Infrastruktur, die über das Maß des Risikos von Anschlägen oder Sabotageakten bestimmt.

Obwohl die beiden letztgenannten Kriterien — die Entfernung zu Territorialgewässern und das geopolitische Umfeld — nicht im engeren Sinne in die Definition von Kritikalität einfließen, sind sie in Korrelation mit dem Grad der Abhängigkeit von einzelnen Energieinfrastrukturen mitbestimmend für die Kritikalität. Sie bestimmen mit sowohl über die Möglichkeit als auch die Notwendigkeit einer Intervention und über die Priorisierung der Maßnahmen zum physischen Schutz der Infrastruktur. Dieser Umstand gewinnt nicht zuletzt aufgrund der wachsenden Spannungen im Indo-Pazifik, am Suezkanal und im Hohen Norden an Bedeutung, führen diese doch zu einer Militarisierung maritimer Verbindungsräume, in denen sich Interessen regionaler und globaler Großmächte überlappen.

Mittels der genannten Kriterien ist es möglich, eine Priorisierung der zu schützenden Infrastruktur in Deutschland vorzunehmen. Dabei ergibt sich folgendes Bild.

Gas: bestehende Kritikalität

Bis Ende 2026 sollte vor allem der Schutz der Pipelines zwischen Norwegen und Deutschland (Europipe 1 und 2) höchste Priorität bekommen, denn zum einen ist der Grad der Abhängigkeit sehr hoch,[42] zum anderen kann ein kompletter Ausfall der Lieferungen über diese Pipelines massive Kaskadeneffekte ähnlich wie bei der Finanz- und Covidkrise nach sich ziehen.[43] Zur Kritikalität trägt außerdem bei, dass eine Reparatur von Pipelines mehrere Monate bis Jahre in Anspruch nehmen kann. Ein Ausfall dieser Lieferungen wäre kurzfristig durch LNG nicht wettzumachen und mittelfristig nur unter der Voraussetzung, dass der LNG-Markt genügend Volumen zur Verfügung stellt und Sicherheitspuffer wirksam sind.[44] Allenfalls die Hälfte der wegfallenden Importe ließe sich kurzfristig durch andere Quellen und Einsparungen kompensieren.[45] Die Suche nach langfristigen Alternativen dürfte überaus zeitintensiv sein und sehr viel Aufwand erfordern.

40 Laut BMI, *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, Berlin 2009, <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=4> gilt »Kritikalität als relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat«. Siehe auch: *Referentenentwurf des Bundesministeriums des Innern und für Heimat. Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen*, Berlin, 25.7.2023, S. 5, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG.pdf?__blob=publicationFile&v=3j>.

41 In einem weiteren Schritt wurde eine Nutzwertanalyse durchgeführt, in welcher die Kriterien gewichtet und Punkte vergeben wurden.

42 BNetzA, »Rückblick: Gasversorgung im Jahr 2022«, 2023, <https://www.bundesnetzagentur.de/DE/Gasversorgung/aktuelle_gasversorgung/Rueckblick/start.html>.

43 Tom Krebs, *Auswirkungen eines Erdgasembargos auf die gesamtwirtschaftliche Produktion in Deutschland*, Düsseldorf: Institut für Makroökonomie und Konjunkturforschung, 2022, <https://www.boeckler.de/de/faust-detail.htm?sync_id=HBS-008318>.

44 BMWK, *Bericht des Bundeswirtschafts- und Klimaschutzministeriums zu Planungen und Kapazitäten der schwimmenden und festen Flüssigerdgasterminals* [wie Fn. 11].

45 Ebd.

Von Relevanz ist außerdem, dass die Pipelines zum größten Teil außerhalb der deutschen Territorialgewässer und AWZ durch dänische und norwegische Gebiete verlaufen. Auch wenn der Küstenstaat einige ausschließliche Hoheitsbefugnisse besitzt, ist er auf zwischenstaatliche Kooperation angewiesen.[46] Im Falle Deutschlands kommt erschwerend hinzu, dass nicht die deutsche Marine, sondern allein die Bundespolizei verfassungsrechtlich befugt ist, für die Sicherheit der Über- und Unterseeinfrastruktur in den Küstengewässern und in der AWZ zu sorgen.

Von 2027 an wird sich die Situation auf dem Gasmarkt dank einer besseren Angebotslage vermutlich etwas entspannen.[47] Auch wenn der Schutz der Pipelines weiter gewährleistet sein sollte, werden ab diesem Zeitpunkt nicht nur die LNG-Terminals, sondern auch die dafür bestimmten Häfen und Schiffe weitaus stärker als zu schützende Infrastruktur in den Vordergrund rücken. Insbesondere Häfen und Schiffe sind nicht nur dem Risiko von Spannungen im Indo-Pazifik und an sogenannten Chokepoints wie der Straße von Hormus oder dem Suezkanal, sondern auch dem einer Eskalation im russisch-westlichen Konflikt im Nordatlantik und im Hohen Norden ausgesetzt.

Der Schutz dieser Schiffe kann daher nicht alleine von Deutschland gewährleistet werden und würde erst recht akut, sollte die US Navy ihre Rolle als Garant der Freiheit der Meere nicht mehr ausüben wollen oder können. Der Ausfall eines Schiffes wäre zwar bei Weitem nicht so gravierend wie der einer der Europipes, gemessen an der Menge des transportierten Gases pro Jahr. Solche Schiffe sind allerdings knapp, und eine Wiederbeschaffung wäre nicht einfach. Zudem könnte eine unsichere Seeroute Entscheidungen von LNG-Produzenten negativ beeinflussen und zu Versorgungsengpässen führen.

Nicht weniger bedeutsam ist der Schutz von LNG-Terminals, kurzfristig vor allem jener schwimmenden Terminals in Lubmin und Stade, welche die größten Importkapazitäten bieten. Die Umsetzung ist hier jedoch deutlich weniger komplex, da sich beide an der Grenze zu bzw. auf deutschem Festland befinden und nicht auf offener See. Zudem wird es bis 2025 drei weitere schwimmende Terminals in Deutschland (und zusätzlich landseitige Terminals in der EU) geben und somit Ausweichmöglichkeiten im Falle eines Angriffs. Der Wiederaufbau landseitiger LNG-Terminals würde allerdings mehrere Monate in Anspruch nehmen.[48] Da die Terminals fester Bestandteil der Hafeninfrastruktur sind bzw. sein werden, müssen auch diese einen noch stärkeren Schutz erfahren, zumal ihr Wiederaufbau nicht nur Monate, sondern Jahre dauern würde.

Inwiefern Wasserstoff als weiterer Energieträger die Gewichtung im Rahmen des Energiemix ändern wird, ist noch offen. Zum einen könnten bei der Entwicklung eines regionalen Marktes Offshore-Pipelines wieder an Bedeutung gewinnen, zum anderen könnte die Entwicklung eines globalen Marktes die Rolle von Schiffen noch weiter hervorheben. In beiden Fällen würde Häfen als potentiellen Wasserstoff-Clustern eine noch größere strategische Bedeutung zukommen, die wiederum mit einer höheren Schutzwürdigkeit bzw. -notwendigkeit einherginge.

Strom: wachsende Kritikalität

Offshore-Windparks und Stromanbindungsleitungen in Nord- und Ostsee sollen im Zuge des Ausbaus der erneuerbaren Energien 2030 bereits ein Viertel des deutschen Stroms liefern, 2045 sogar die Hälfte.[49] Ihr Schutz sowie der von hybriden Interkonnektoren sollte daher von 2030 an priorisiert werden.

Die Energieerzeugung findet meist außerhalb der Zwölf-Meilen-Zone statt, wo der Schutz physischer Infrastruktur seerechtlichen Einschränkungen unterliegt.

Die Energieerzeugung findet allerdings meist in der AWZ statt, also außerhalb der Zwölf-Meilen-Zone, wo der Schutz physischer Infrastruktur seerechtlichen Einschränkungen unterliegt. Darüber hinaus werden deutsche Offshore-Windparks nicht nur Deutschland, sondern über hybride Interkonnektoren perspektivisch auch andere EU-Staaten beliefern. Diese Interkonnek-

46 Siehe dazu den Beitrag von Christian Schaller in dieser Studie, S. 14ff.

47 BMWK, *Bericht des Bundeswirtschafts- und Klimaschutzministeriums zu Planungen und Kapazitäten der schwimmenden und festen Flüssigerdgasterminals* [wie Fn. 11].

48 »Längerer Ausfall bei LNG-Terminalbetreiber Freeport treibt Gaspreise in Europa«, in: *Der Spiegel* (online), 15.6.2022, <https://www.spiegel.de/wirtschaft/lng-laengerer-ausfall-bei-lng-terminalbetreiber-freeport-treibt-gaspreise-in-europa-a-5087a499-fc51-4c00-94cb-833dac8c5b42>.

49 Bundesregierung, *Mehr Windenergie auf See*, <https://www.bundesregierung.de/breg-de/themen/klimaschutz/windenergie-auf-see-gesetz-2022968>.

toren verlaufen in den AWZ anderer Staaten, was die Koordinierung der Schutzmaßnahmen erschwert, zumal aufgrund der Spannungen mit Russland vor allem im Ostseeraum die Militarisierung voranschreitet. Die besondere Kritikalität dieser maritimen Energieinfrastruktur zeigt sich nicht zuletzt daran, dass die physische Wiederherstellung beschädigter oder zerstörter Windenergieanlagen Tage bis Wochen dauern kann,[50] eine Reparatur nach Cyberangriffen teilweise Monate.[51] Zerstörte Stromanbindungskabel und Interkonnektoren wiederum lassen sich im besten Fall innerhalb eines Monats reparieren,[52] im schlimmsten Fall sind sie aber erst nach sechs Monaten wieder einsatzfähig.[53]

Zuständigkeiten sowie Instrumente zum Schutz

Auf EU-Ebene gibt es bereits Bemühungen, den Schutz kritischer Infrastrukturen mit der maritimen Dimension zu verknüpfen.[54] Weniger einheitlich sind die Bestrebungen auf Ebene der EU-Mitgliedstaaten, bei denen Energie nur in seltenen Fällen zentraler Bestandteil maritimer Sicherheitskonzepte ist. Doch gibt es einige positive Ausnahmen, insbesondere Spanien, das in seiner nationalen Energiesicherheitsstrategie betont, dass Land- und Seeverkehrsnetze wesentliche Bestandteile des Energiesystems sind.[55] Zudem wird dort die Zusammenarbeit zwischen privaten und staatlichen Akteuren als essentiell angesehen.

In Deutschland koordiniert auf Bundesebene das Bundesministerium des Innern (BMI) Strategien und Maßnahmen zum Schutz kritischer Infrastrukturen, wozu auch Energie zählt. Bereits die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz von 2016 stuft die Strom-, Gas-, Kraftstoff-, Heizöl- und Fernwärmeversorgung als kritische Dienstleistungen ein und definiert Schwellenwerte. Allerdings werden weder eine Priorisierung der zu schützenden Infrastruktur noch die Reaktionsmöglichkeiten bei physischen Angriffen oder der Bezug zum Maritimen thematisiert[56] — obwohl bereits der Nationale Masterplan Maritime Technologien des (ehemaligen) BMWi von 2011 auf die Sicherung von Offshore-Anlagen für Öl und Gas eingeht.[57] Auch die Eckpunkte des KRITIS-Dachgesetzes sowie der im Sommer 2023 veröffentlichte Entwurf gehen, abgesehen von der Erwähnung von Meldepflichten und Störungs-Monitoring seitens der Anlagebetreiber, hierauf nicht näher ein.[58] Vor allem aber ist in Deutschland der Einsatz des Militärs in den Territorialgewässern, speziell in der AWZ, zu Überwachungs- und Schutzzwecken grundsätzlich nicht möglich und allenfalls zeitlich beschränkt im Rahmen der Amtshilfe erlaubt. Auch die Einsatzmöglichkeiten auf Hoher See bleiben begrenzt.

50 Sulzer, »Cutting Repair Times for Wind Turbines«, *Power Engineering International*, 10.3.2022, <https://www.power engineeringint.com/renewables/wind/cutting-repair-times-for-wind-turbines/>.

51 Enercon, »Over 95 Per Cent of WECs Back Online Following Disruption to Satellite Communication«, 19.4.2022, <https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/>.

52 Bundesverband der Energie- und Wasserwirtschaft (BDEW), »In tiefer Verbundenheit: Seekabel für die Energiewende«, 5.1.2022, <https://www.bdew.de/online-magazin-zweitausend50/schwerpunkt-europa/in-tiefer-verbundenheit-seekabel-fuer-die-energiewende/>.

53 Nexans, »Nexans Completes Repair of Malta-Sicily Subsea Interconnector«, 14.5.2020, <https://www.nexans.com/en/newsroom/news/details/2020/05/nexans-completes-repair-malta-sicily-subsea-interconnector.html>.

54 Europäische Kommission, »Critical Infrastructure Protection«, <https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en>. Siehe hierzu auch den Beitrag von Raphael Bossong in dieser Studie, S. 34ff.

55 Spanish Department of National Security, *National Energy Security Strategy*, Madrid 2015, <https://www.dsn.gob.es/ca/file/2127/download?token=EuGMXvAF>.

56 BMI, *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)* (online), <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2016/kritis-vo.pdf?__blob=publicationFile&v=2>.

57 BMWi, *Nationaler Masterplan Maritime Technologien (NMMT)*, Berlin, April 2014, <https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/nationaler-masterplan-maritime-technologien-flyer.pdf?__blob=publicationFile&v=1>.

58 BMI, *Eckpunkte für das KRITIS-Dachgesetz*, Berlin, Dezember 2022, <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2022/eckpunkte-kritis.pdf?__blob=publicationFile&v=1>; BMI, *Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen*, Berlin, 25.7.2023, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG.pdf?__blob=publicationFile&v=3j>.

Schlussfolgerungen und Handlungsempfehlungen

Angesichts der sich verändernden energiepolitischen Prioritäten, des sich verschlechternden geo- und sicherheitspolitischen Umfelds und der überproportional wachsenden Rolle maritimer Energieversorgung ist es insbesondere in Deutschland erforderlich, dass der Schutz maritimer Energieinfrastruktur zentraler Bestandteil von (maritimen) Sicherheitskonzepten wird.

Nötig ist eine zeitlich, räumlich und sicherheitspolitisch differenzierte Priorisierung der zu schützenden Objekte.

Erstens bedarf es einer *zeitlich*, *räumlich* sowie *sicherheitspolitisch* differenzierten Priorisierung der zu schützenden Objekte, die zudem eine breitere und dynamischere Definition von Kritikalität als die gegenwärtig diskutierte voraussetzt. Dabei wird von den späten 2020er und frühen 2030er Jahren an die Aufgabe des Schutzes weiter an Komplexität gewinnen; denn neben Pipelines werden vermehrt Schiffe, Offshore-Windparks und Stromanbindungsleitungen in den Vordergrund rücken.

Zweitens müssen in diesem Zusammenhang auch die jeweiligen Aufgaben von Militär und Zivilschutz hinsichtlich Kompetenzen, Handlungsmöglichkeiten und identifizierten Handlungsprioritäten neu definiert und abgegrenzt werden. Da die Komplexität der maritimen Energieversorgungsinfrastruktur zunehmen dürfte und die institutionellen Prozesse langwierig sind, erscheint eine Diskussion darüber schon jetzt dringend geboten.

Bei der gewichteten Kombination der identifizierten Kriterien lässt sich anhand der Analyse festhalten, dass der militärischen Dimension eine besondere Bedeutung zukommen dürfte. Gleichwohl muss in jedem Fall der Versuchung widerstanden werden, maritime Energieinfrastruktur undifferenziert ausschließlich militärisch oder ausschließlich national schützen zu wollen. Eine umfassende und gleichzeitige Überwachung aller Infrastrukturobjekte durch das nationale Militär ist unrealistisch.

Deutschland, so das Ergebnis dieser Analyse, steht zunächst vor der Aufgabe, für die technische Verbesserung von Pipelines und den Ausbau von Reparaturkapazitäten zu sorgen, beides entsprechend der tatsächlichen Entwicklung des Energiebedarfs, des Energiemixes, der Rolle von einzelnen Energieträgern und deren Importen, aber auch der geografischen Entfernung der Infrastrukturanlagen und der geopolitischen wie regionalen Lage im Umfeld bzw. entlang der Infrastruktur. Darüber hinaus sollte sich Deutschland auf folgende konkrete Maßnahmen konzentrieren:

Kurz- bis mittelfristig insbesondere auf den Schutz der beiden Europipes durch häufigere Patrouillen und verstärkte Überwachung, womöglich in dauerhafter Zusammenarbeit mit Norwegen, auch entlang der Abschnitte, die über die AWZ bis in die eigenen Territorialgewässer hineinreichen.[59]

Mittelfristig sollte der Schutz von LNG-Lieferungen (insbesondere durch Schiffe) entlang der Asien-Golf-Mittelmeer-Route mit ihren Chokepoints wie dem Suezkanal sowie entlang der nordatlantischen Route priorisiert werden. Die Komplexität dieser Aufgabe wird aber zwingend eine enge Koordination sowohl in gesamteuropäischen als auch in minilateralen Adhoc-Formaten sowie im Rahmen der EU-Nato-Kooperation erfordern, wie sie bereits in der Maritimen Sicherheitsstrategie der EU avisiert ist, beispielsweise im Kontext der EU-Nato-Task Force.[60] Auch einer direkten Kooperation mit den Vereinigten Staaten kommt dabei eine bedeutende Rolle zu. Neben der physischen Überwachung der genannten Routen wird vor allem eine satellitengestützte Überwachung unerlässlich sein.

Mittel- bis langfristig wäre darüber hinaus der Schutz von Offshore-Windparks, Stromanbindungsleitungen und Interkonnektoren in den territorialen Gewässern zu priorisieren, insbesondere aber in der AWZ. Hier wäre vor allem im Bereich der Nordsee eine physische Überwachung und eine Abschreckungspräsenz nur in Zusammenarbeit mit anderen Anrainerstaaten wie Dänemark und Norwegen sowie in anderen minilateralen Formaten möglich. Die Joint Expeditionary Force zum Schutz kritischer Infrastrukturen bietet ein

59 Die Deutsche Marine beteiligt sich bereits an der Überwachung des Seegebietes im Raum der Nato-Nordflanke mit Norwegen, allerdings nur in norwegischen Gewässern. Siehe dazu Bundeswehr, »Deutsche Marine beteiligt sich am Schutz der kritischen Infrastruktur Norwegens«, Pressemitteilung, 4.11.2022, <https://www.bundeswehr.de/de/organisation/marine/aktuelles/schutz-kritischer-infrastruktur-norwegens-5519846>.

60 Europäische Kommission, »Launch of the EU-NATO Task Force: Strengthening Our Resilience and Protection of Critical Infrastructure«, Brüssel, 16.3.2023, <https://ec.europa.eu/commission/press corner/detail/en/STATEMENT_23_1705>.

Beispiel für eine mögliche Zusammenarbeit.[61] Eine konkrete Möglichkeit für einen effektiveren physischen Schutz wäre die räumliche Ausweitung der Schutzzonen um die Offshore-Windparks in Koordination mit den betroffenen Anrainerstaaten und privaten Betreibern.

Davon abgesehen sollten Hafenanlagen, landseitige Terminals und in Küstengewässern befindliche Infrastrukturobjekte wie Offshore-Windparks und Pipelineabschnitte durch Bundespolizei, Küstenwache und zivile Mechanismen weiterhin verstärkt überwacht und zusätzlich durch eine robuste Cyberabwehr geschützt werden.

Vor diesem Hintergrund und angesichts der zunehmenden Komplexität des Schutzes maritimer Energieinfrastruktur ist allerdings auch damit zu rechnen, dass der Deutschen Marine eine größere Rolle zuwächst.[62] An dieser Stelle ist lediglich festzuhalten, dass eine bessere Koordinierung und Verzahnung zwischen Marine, Bundes- und Landespolizei schon heute und unter den aktuellen rechtlichen Bestimmungen und Aufgabenteilungen möglich und notwendig ist. Die in dieser Analyse identifizierten Kriterien zur Handlungspriorisierung könnten dazu beitragen, einen besseren, wenngleich keineswegs allumfassenden Schutz maritimer Energieinfrastruktur zu gewährleisten und zugleich einer dysfunktionalen Versicherheitlichung vorzubeugen.

61 Dutch Ministry of Defence, »European Countries Join Forces against Undersea Threats«, Pressemitteilung, Amsterdam, 13.6.2023, <https://english.defensie.nl/latest/news/2023/06/13/european-countries-join-forces-against-undersea-threats>.

62 Vgl. in dieser Studie den Beitrag von Göran Swistek, S. 61ff, und die Schlussfolgerungen, S. 80ff.

Bettina Rudloff

(K)ein Schiff wird kommen: Maritimer Nahrungstransport als vernetzte kritische Infrastruktur der EU

Einleitung

Einige Ereignisse der jüngsten Vergangenheit haben gezeigt, dass Störungen im maritimen Gütertransport unmittelbare und gravierende Folgen für die Nahrungsversorgung haben können:

- Die Explosion im *Hafen* von Beirut im Frühjahr 2020, ausgelöst durch die dort gelagerte explosive Düngemittelkomponente Ammoniumnitrat, forderte nicht nur viele Todesopfer. Neben den Düngerlagern wurden auch hafenansässige Getreidesilos zerstört, was zu einer angespannten Versorgungslage im Libanon führte und bis heute ein grundlegend neues Importmanagement nötig macht: Da Lagerkapazitäten begrenzt sind, ist für das stark importabhängige und auf Nahrungshilfen angewiesene Land[1] nunmehr eine kontinuierliche Nahrungszulieferung erforderlich.
- Der russische Angriffskrieg gegen die Ukraine im Frühjahr 2022 verringerte die Produktionskapazität des großen Getreidelands Ukraine und schränkte auch mögliche Lieferungen über *Seewege* durch das Schwarze Meer aus der gesamten versorgungswichtigen Region Ukraine und Russland ein. Hieraus resultierten anfänglich vor allem unmittelbare Lieferengpässe für diejenigen Länder, die typischerweise aus der betroffenen Region importieren, wie etwa Ägypten und Libanon. Durch den Preisauftrieb als Folge der stark beschränkten Gesamtlieferungen kam es aber auch zu internationalen Versorgungsproblemen, die insbesondere finanzschwache Importländer betrafen.[2] Die Engpässe versuchte die internationale Gemeinschaft durch ein Zusammenspiel von Maßnahmen in sehr unterschiedlichen Politikbereichen aufzufangen, etwa mit einer Verbesserung der Transportlogistik, der Lagerhaltung in Häfen und der Hafenanbindung. Vor allem wurden terrestrische Alternativen zur Seepassage gesucht (»solidarity lanes«), darüber hinaus wurde handelspolitisch die Grenzabwicklung erleichtert und verstärkt humanitäre Hilfe geleistet. Unter Führung der Vereinten Nationen und Beteiligung der Ukraine, Russlands und der Türkei öffnete die im Sommer 2022 gestartete »Schwarzmeerinitiative« schließlich die entsprechende Seepassage wieder als Transportweg für Agrar- und Düngemittel aus der Ukraine und aus Russland. Insgesamt sorgten diese Maßnahmen dafür, dass sich die Preis- und damit auch die Versorgungslage entspannen konnten. Allerdings drohte Russland immer wieder damit, die getroffene Vereinbarung über die Nutzung des Transportwegs durch das Schwarze Meer aufzukündigen, um diesen Schritt dann im Sommer 2023 tatsächlich zu vollziehen. Seitdem kam der Transport von Agrar- und Düngemitteln auf dieser Route bis auf wenige einzelne Versuche privater Anbieter zum Erliegen. Die unsichere Gesamtsituation machte es von Beginn an erforderlich, nach Alternativen zu suchen.

1 United Nations World Food Programme, »More People Than Ever Rely on Food Assistance across Lebanon«, 21.10.2022, <https://www.wfp.org/news/more-people-ever-rely-food-assistance-across-lebanon> (eingesehen am 12.4.2023).

2 Bettina Rudloff/Linde Götz, *Ukraine-Krieg und Ernährungssicherheit. Umsichtige »Food First«-Strategie für den Herbst entwickeln*, Berlin: Stiftung Wissenschaft und Politik, 9.3.2023 (SWP Kurz gesagt), <https://www.swp-berlin.org/publikation/ukraine-krieg-und-ernaehrungssicherheit-umsichtige-food-first-strategie-fuer-den-herbst-entwickeln> (eingesehen am 12.4.2023).

SWP Berlin
Maritime kritische Infrastrukturen
Februar 2024

- Seit der durch die Terrorangriffe gegen Israel im Oktober 2023 neuerlich angeheizten Nahost-Krise häufen sich terroristische Attacken auf Handelsschiffe durch die Hamas-unterstützende Huthi-Miliz im Roten Meer. Als Folge davon kommt es zur Umleitung der Schiffe über das Kap der Guten Hoffnung, deren Fahrt nun deutlich länger dauert, was etwa die Treibstoffkosten — neben weiteren Kosten wie den für das Personal, die mit längerer Dauer der Fahrt steigen — drastisch erhöht.[3]

Nahrungsversorgung und maritimer Transport sind als kritische Infrastruktur definiert.

Ungeachtet dieser jüngsten Gefährdungen gelten in Deutschland und der EU sowohl die Nahrungsversorgung als auch maritimer Transport schon länger als essentiell für das Funktionieren der eigenen Volkswirtschaften und Gesellschaften und damit als jeweils zu schützende kritische Infrastruktur. Eine besondere Herausforderung stellt dabei deren gemeinsamer, gleichzeitiger Schutz dar, sind die beiden Bereiche doch eng miteinander verwoben. Eine stärkere politische Koordinierung ihres Schutzes ist daher unabdingbar.

Sichere internationale und europäische Nahrungsversorgung als Ziel der Politik

Nach einer Definition der Ernährungs- und Landwirtschaftsorganisation der Vereinten Nationen (Food and Agriculture Organization, FAO) beruht Versorgungssicherheit auf vier unterschiedlichen Säulen. Diese decken auch Handelsaspekte und damit gleichzeitig maritimen Transport für eine sichere Versorgung ab,[4] denn internationaler Agrarhandel erfolgt zu 80 Prozent über Seewege.

1. *Nahrungsverfügbarkeit* umfasst neben eigener Produktion und Lagerung auch Importe und Nahrungshilfen, die ebenfalls hauptsächlich über den Seeweg erfolgen.
2. *Zugang zu ausreichend Nahrung* bedeutet nicht nur den physischen Zugang zu Märkten. Der ökonomische Zugang wird durch das Preisniveau bestimmt, das bei Störungen maritimer Lieferstrukturen schnell ansteigen kann. Hierdurch werden vor allem ärmere Haushalte in ihrer Versorgung belastet, es steigen aber auch die nationalen Ausgaben für Importe und Hilfslieferungen.
3. *Nutzbarkeit* von verfügbarer Nahrung meint auch das Vorhandensein relevanter weiterer Faktoren wie etwa Energie für Transport, Düngemittelerzeugung und Nahrungsverarbeitung, aber auch Trinkwasser zur Zubereitung.
4. *Stabilität* schließlich meint die Sicherheit über alle zuvor genannten Säulen hinweg, die im Übrigen gleichzeitig vorhanden sein müssen.

Europäische Versorgungssicherung: eher mittelbar anfällig durch Transportstörung

Seit Gründung der Europäischen Wirtschaftsgemeinschaft (EWG) konnte die europäische Nahrungsversorgung kontinuierlich verbessert werden. Im Sinne der Definition der FAO steigerten erst die EWG und dann die EU insbesondere die Verfügbarkeit von Nahrung, indem sie durch immense politische Regulierung und finanzielle Anreize ihre eigene Produktion ankurbelten. Bis auf Produkte wie Obst und Gemüse und besondere tropische Erzeugnisse wie Kaffee und Tee liegt der Selbstversorgungsgrad der EU heute bei den meisten Nahrungsmitteln nahe 100 Prozent oder sogar darüber, so dass exportiert wird.[5]

Damit hat sie auch als internationaler Handelsakteur kontinuierlich an Bedeutung gewonnen: So ist die EU in den letzten Jahren weltweit sowohl größter Exporteur als auch wichtigster Importeur von Agrarerzeugnissen gewesen. Insgesamt erscheint daher die erste Säule der Versorgungssicherheit für die EU selbst stabil.[6] Ein größeres Risiko zeigt sich aktuell für

3 »Höhere Preise und leere Regale durch Huthi-Angriffe im Roten Meer?«, *Tagesschau*, 20.12.2023, <https://www.tagesschau.de/inland/regional/nordrheinwestfalen/wdr-hoehere-preise-und-leere-regale-durch-huthi-angriffe-im-roten-meer-100.html> (eingesehen am 21.12.2023).

4 Food and Agriculture Organization of the United Nations (FAO), *The State of Food and Agriculture 1996, Food Security: Some Macroeconomic Dimensions*, Rom 1996 (FAO Agriculture Series Nr. 29).

5 Alan Buckwell/Alan Matthews/David Baldock/Erik Mathijs, *CAP – Thinking Out of the Box, Further Modernisation of the CAP – Why, What and How?*, Brüssel: RISE Foundation, 2017, S. 35, <https://risefoundation.eu/cap-thinking-out-of-the-box-report/> (eingesehen am 12.4.2023).

6 The Economist Group, *Global Food Security Index 2022*, Economist Impact, 2022, <https://impact.economist.com/sustainability/project/food-security-index/reports/Economist_Impact_GFSI_2022_Global_Report_Sep_2022.pdf> (eingese-

die zweite Säule, da auch in Deutschland und in der EU die Nahrungspreise steigen — sogar stärker als das allgemeine Inflationsniveau: Sie lagen in Deutschland laut statistischem Bundesamt im Juni 2023 mit 13,7 Prozent mehr als doppelt so hoch wie die allgemeine Inflation und viermal höher als die Energiepreisinflation.[7]

Diese Teuerung bei den Nahrungspreisen lässt sich unter anderem mit den internationalen Preisanstiegen in einem global verflochtenen Handelssystem erklären; sie ist insofern auch eine Folge der Störung der Agrartransporte über das Schwarze Meer, die aus dem Krieg Russlands gegen die Ukraine resultiert. Daneben spielen höhere Energiekosten für Produktion und Verarbeitung eine Rolle, möglicherweise aber auch vom Einzelhandel ausgereizte Preismargen in einem System mit ohnehin begrenzter Wettbewerbsstruktur. Im Ergebnis trifft diese Teuerung vor allem ärmere Haushalte in der EU, die ohnehin schon einen verhältnismäßig hohen Anteil des Einkommens für Nahrung ausgeben.

Internationale Versorgungssicherung: stark anfällig für Transportstörungen, die mittelbare Risiken für die EU bergen

Der Preisanstieg, eine Dimension der Versorgungsrisiken, wirkt sich international in Ländern mit vielen armen Haushalten deutlich gravierender aus als in der EU. Auch geraten gesamtwirtschaftlich ärmere Staaten durch steigende Importausgaben finanziell unter Druck, was ihre Möglichkeiten begrenzt, Nahrung und dafür relevante Düngemitteln aufzukaufen und verfügbar zu halten. Teurer werden auch benötigte Hilfslieferungen. Die Blockade der Seepassage durch das Schwarze Meer nach der russischen Invasion machte gerade zu Beginn des Kriegs deutlich, dass in der Folge die Versorgung der Hauptbezugsländer von Getreide aus der Konfliktregion gefährdet ist — etwa von Ländern in Nordafrika. Insgesamt verursachen Störungen im maritimen Transportsystem also eher Versorgungsrisiken in armen Ländern als in der EU.

Internationale Versorgungsrisiken betreffen die EU eher indirekt.

Diese internationalen Nahrungsversorgungsrisiken können die EU gleichwohl indirekt betreffen, indem sie die politische Glaubwürdigkeit der Union als großer internationaler Akteur der Entwicklungs- und humanitären Hilfe beeinträchtigen. Etwaige Teuerungen bei Agrarprodukten führen oftmals dazu, dass mit einer länger im Voraus festgelegten Hilfssumme gerade dann weniger Nahrung gekauft werden kann, wenn größerer Unterstützungsbedarf besteht.

Zudem wird in Phasen von Agrarknappheit und damit steigenden Preisen auch in großen Agrarländern innerhalb der EU der Ruf laut, die heimische Produktion auszuweiten, um die Preise zu dämpfen. Dies kann wiederum Zielkonflikte mit Umweltschutzregelungen hervorrufen, wie etwa die politische Entscheidung der Bundesregierung gezeigt hat, als Reaktion auf die russische Invasion bereits beschlossene, ökologisch motivierte Stilllegungen von Anbauflächen auszusetzen.[8] Eine solche Maßnahme kann nicht zuletzt die internationale Glaubwürdigkeit Deutschlands und der EU beschädigen, wenn sie auf diese Weise Abstriche bei der Einhaltung der Nachhaltigkeitsziele der Vereinten Nationen machen.

Versorgungsprobleme anderer Staaten können Deutschland und die EU schließlich mit Risiken einer sicherheitspolitischen Destabilisierung konfrontieren oder als politisches Druckmittel gegen sie genutzt werden. Hierzu zählt beispielsweise ein befürchteter oder auch als Narrativ heraufbeschworener Migrationsstrom von Armuts- und Hungergefährdeten in Richtung Europa, der Migrationsabkommen etwa mit afrikanischen Staaten motiviert. Noch sicherheitsrelevanter ist der aktuelle Vorwurf Russlands und einiger afrikanischer Akteure, durch westliche Sanktionen unbeabsichtigt verursachte Versorgungsengpässe, die als Folge verringerter Transporte entstehen, träfen nicht nur das sanktionierte Russland,

hen am 12.4.2023); Europäische Kommission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Food Security and Reinforcing the Resilience of Food Systems*, COM(2022) 133 final, Brüssel, 22.3.2022, S. 5, <https://agriculture.ec.europa.eu/system/files/2022-03/safeguarding-food-security-reinforcing-resilience-food-systems_0.pdf> (eingesehen am 12.4.2023).

7 Statistisches Bundesamt, »Inflationsrate im Juni 2023 voraussichtlich +6,4%«, Pressemitteilung Nr. 255, Berlin, 29.6.2023, <https://www.destatis.de/DE/Presse/Pressemitteilungen/2023/06/PD23_255_611.html> (eingesehen am 23.1.2024).

8 Bettina Rudloff/Christine Wieck, »Zukunftsfähige Agrarpolitik«, in: *Internationale Politik* (online), 27.2.2023, <https://internationalepolitik.de/de/zukunftsfaehige-agrarpolitik> (eingesehen am 16.9.2023).

sondern auch afrikanische Regionen. Denn dieser Vorwurf erschwert es der EU, außenpolitische Koalitionen zu bilden.[9]

Seerouten und Häfen: anfällige Chokepoints für die globale Nahrungsversorgung

Um eine sichere Nahrungsversorgung gewährleisten zu können, müssen die relevanten maritimen Transportrouten und Häfen identifiziert und auf ihre Kritikalität hin beurteilt werden. Ihre Relevanz für den Seehandel von Nahrungsprodukten hängt zunächst einmal von der globalen räumlichen Allokation von Produktion und Verbrauch ab. Diese bestimmt Ex- und Importflüsse und somit Herkunfts- und Ankunftshäfen. Das Transport- und Hafenmuster unterscheidet sich dabei je nach Agrargut bzw. Düngeprodukt.

Global gesehen liegt ein Herkunfts- und damit Exportschwerpunkt für viele Agrarrohstoffe in den großen Erzeugerregionen USA, Brasilien und Argentinien (Getreide, Ölsaaten, Fleisch). Ankunftshäfen für diese Produkte konzentrieren sich wiederum eher in den Importregionen Europa und Asien.[10]

Für die Absatzregion Europa sind andere Routen relevant als für Importregionen in anderen Teilen der Welt (siehe Tabelle):

- Mit Blick auf die *weltweite* Nahrungsversorgung ist beispielsweise die Straße von Malakka, ebenso wie die Straße von Gibraltar, dominierend für Düngemittelimporte etwa aus China, Russland und Marokko. Auch für den globalen Getreidetransport spielt sie eine Rolle, kaum jedoch für die europäische Versorgung. Am bedeutsamsten für weltweite Getreidetransporte sind die türkischen Gewässer, die Suezroute und die Bab-al-Mandab-Straße, über die unter anderem Getreideimporteure in Afrika, im Nahen Osten und in Asien versorgt werden.
- Für die *europäische* Versorgung sowohl mit Düngemitteln als auch mit Getreide sind die türkischen Seerouten sowie die Häfen von Gibraltar und Dover derzeit von kritischer Bedeutung. Wie sich der Brexit längerfristig auf diese Transportroute auswirken wird, bleibt abzuwarten. Für die Getreideversorgung spielen außerdem die Suezroute und die Bab-al-Mandab-Straße auch für Europa eine Rolle.

Neben Seerouten und der Hafenkonzentration ist auch die inländische Verkehrsanbindung der Häfen von Belang für den Weitertransport und damit für die internationale Versorgung. Nicht nur die Mengenverfügbarkeit, auch der Preis als versorgungsrelevanter Parameter wird von Produktions- und Transportkosten beeinflusst.[11] Diese setzen sich zusammen aus Schiffsmiete (Zeitcharter), Treibstoff (Bunker), Hafen- und Kanal- sowie Versicherungsgebühren. Auch handelspolitische Kosten bei der Verladungsabwicklung, wie zum Beispiel Zollkontrollen und die Kontrollen von Einfuhrstandards, spielen eine Rolle. Die Schwankungen bei diesen maritimen transportbezogenen Kosten sind im Schnitt größer als die bei den zugrundeliegenden Rohstoffpreisen. Schätzungen zufolge sind einkommensschwache Länder im Unterschied zu entwickelten Ländern eher von einem Anstieg der Rohstoffpreise betroffen als von steigenden Transportkosten. Ein Grund dafür kann ihre verhältnismäßig geringere Teilnahme am Handel sein. Transportkosten sind laut Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) gerade in jüngster Zeit besonders volatil gewesen — solche Schwankungen lassen in der Regel auf große, auch den Transport behindernde Einflüsse schließen. Insgesamt schwankte der Frachtkostenanteil an den Gesamtkosten bei Getreide und Ölsaaten in den Jahren 2007 bis 2021 zwischen 2 und 30 Prozent.[12]

9 Bettina Rudloff, »Nahrungsversorgungsrisiken im Sanktionsumfeld strategisch begrenzen«, in: Janis Kluge (Koord.), *Wirtschaftssanktionen gegen Russland – internationale Perspektiven und globale Auswirkungen*, Berlin: Stiftung Wissenschaft und Politik, 11.7.2022 (360 Grad), <https://www.swp-berlin.org/publikation/wirtschaftssanktionen-gegen-russland-internationale-perspektiven-und-globale-auswirkungen#publication-article-59> (eingesehen am 12.4.2023).

10 Rob Bailey/Laura Wellesley, *Chokepoints and Vulnerabilities in Global Food Trade*, London: Chatham House, 27.6.2017 (Chatham House Report), S. 48, <https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-27-chokepoints-global-food-trade-embargoed.pdf> (eingesehen am 20.5.2023).

11 Annelies Deuss/Clara Frezal/Frederica Maggi, *Maritime Transportation Costs in the Grains and Oilseeds Sector. Trends, Determinants and Network Analysis*, Paris: OECD Publishing, Juni 2022 (OECD Food, Agriculture and Fisheries Papers Nr. 179), S. 21, <https://www.oecd-ilibrary.org/docserver/b1cdf6b7-en.pdf?expires=1681295352&id=id&accname=guest&checksum=1624E83706E850B99806BD7B40151493> (eingesehen am 12.4.2023).

12 Ebd.

Tabelle

Produktspezifische Bedeutung einzelner Seerouten am Beispiel des Transports von Getreide und Dünger (Anteil Importmenge, Durchschnitt 2018–2020, fett und blau: wichtigste Routen)

	Türkische Seerouten (Bosporus, Dardanellen)	Suez	**Bab al-Mandab**	**Malakka**	**Gibraltar**	Panama	Hormus	**Dover**
Getreide								
EU	**11,0 %**	**4,7 %**	**4,7 %**	2,0 %	**5,1 %**	2,3 %	0,0 %	**5,9 %**
Welt	**16,7 %**	**14,6 %**	**13,6 %**	13,5 %	10,7 %	9,5 %	6,4 %	3,2 %
Dünger								
EU	**6,0 %**	1,2 %	1,2 %	0,7 %	**4,0 %**	1,4 %	0,2 %	**6,8 %**
Welt	11,8 %	**14,5 %**	**14,4 %**	**15,7 %**	**17,6 %**	7,2 %	8,5 %	6,8 %

Anpassung: 2023 Stiftung Wissenschaft und Politik (SWP); Quelle: Richard King, *Exploring the Cascading Impacts from Climate Shocks to Chokepoints in Global Food Trade*, London: Chatham House, 2022, Abbildung 2, resourcetrade.earth, <https://resourcetrade.earth/publications/cascading-impacts-from-climate-shocks-to-food-trade-chokepoints> (eingesehen am 20.4.2023).

Kritikalität: Welche Seerouten und Häfen im Agrarhandel sind wodurch gefährdet?

Risiken für eine sichere Nahrungsversorgung durch maritimen Transport treten im ganzen Spektrum der Faktoren auf, die Einfluss auf Routen und Häfen haben. Sie können sich je nach Route unterscheiden:

Bereits die *zugrundeliegenden Produktions- und Verbrauchsmuster von Agrarprodukten* sind anfällig. So können natürliche Störfaktoren wie Großwetterereignisse (Dürren, Überflutung) oder Krankheits- und Schädlingsdruck (Pilzbefall, Heuschreckenplage) Produktionsschwerpunkte verschieben. Je nachdem werden dadurch andere Ausfuhrrouten und mit ihnen andere Transportanbindungssysteme inklusive Häfen und Zufahrten relevant. Auch die Zerstörung von Anbauflächen oder die Konfiszierung von Vorräten, wie sie derzeit Russland in der Ukraine betreibt, hat Einfluss darauf, ob und wie viel eine Region produzieren und exportieren kann. Daraus können sich auch alternative Transportrouten wie aktuell die Solidaritätskorridore für ukrainische Exporte ergeben.

Maritime Transportrisiken im engeren Sinne umfassen alle möglichen Bedrohungen, darunter auch intendierte und nicht intendierte Störungen wie natürliche Ereignisse und Unfälle:

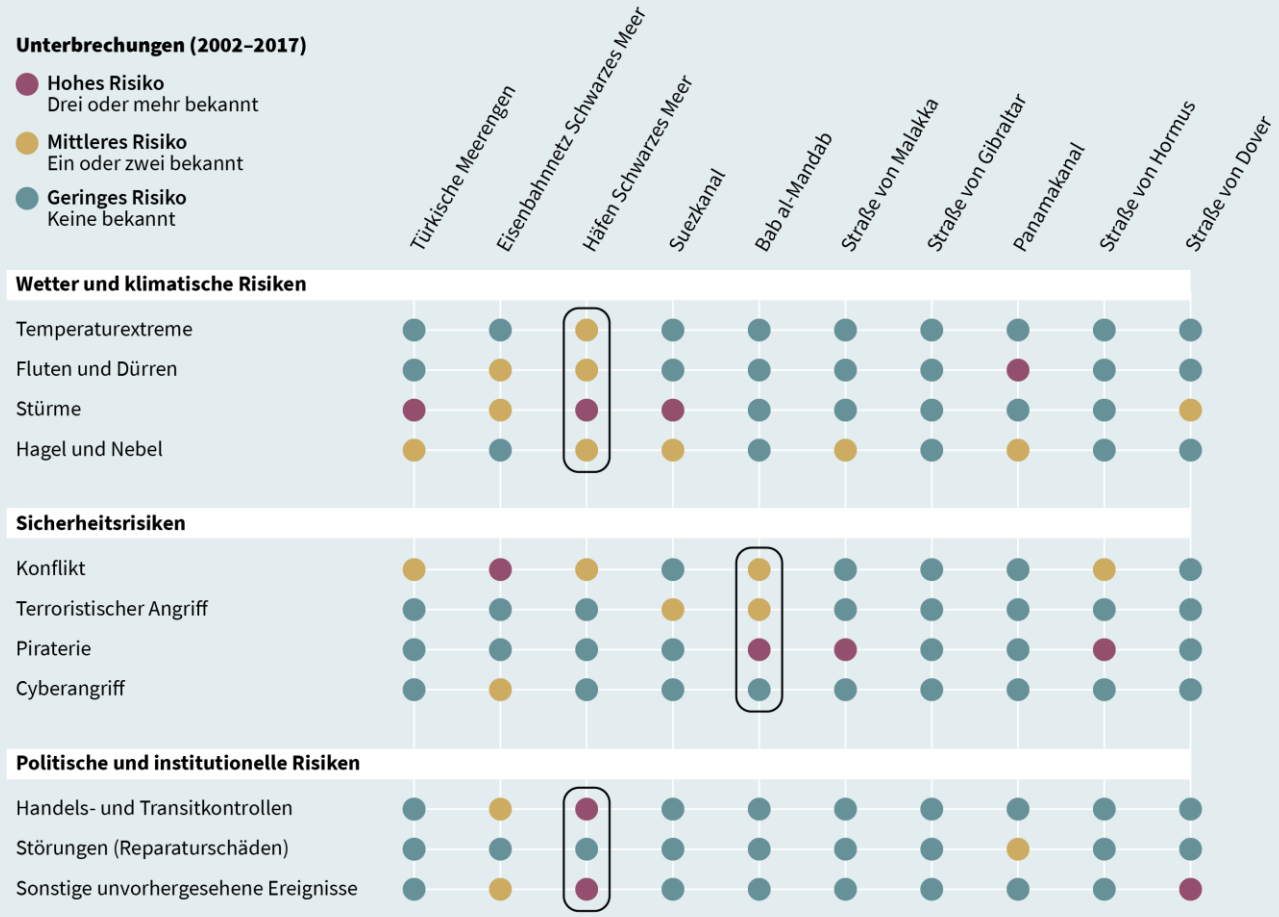
- *Wetterereignisse und klimatische Faktoren* können zu Zerstörungen von Infrastrukturen in Häfen und deren Anbindung führen oder die Transportbedingungen auf See erschweren.
- *Sicherheitsfaktoren* wie Kriegs- und Terrorgefährdungen von Routen verteuern den Transport, weil sie zu Umwegen zwingen können, Versicherungsprämien ansteigen lassen oder weil Handelsrouten infolge von Sanktionen nur eingeschränkt genutzt werden können. Letztere sollen nach völkerrechtlichem Konsens zwar explizit nicht auf Nahrung angewendet werden, doch können sich auch nichtnahrungsbezogene Sanktionen indirekt auf die Versorgung auswirken.[13] Auch Cyberattacken und Piraterie können der Transport- und Hafenlogistik Schaden zufügen. An der Küste Westafrikas beispielsweise wurden im Jahr 2019 fast 100 Piratenübergriffe registriert.[14] Und im Zuge des sich jüngst extrem verschärfenden Nahost-Konflikts häufen

13 Rudloff, »Nahrungsversorgungsrisiken im Sanktionsumfeld strategisch begrenzen« [wie Fn. 9].

14 Bettina Rühl/Benjamin Moscovici, »Unsichere Handelswege, Piraten vor Afrikas Küsten«, in: *Deutschlandfunk*, 28.2.2021, <https://www.deutschlandfunk.de/unsichere-handelswege-piraten-vor-afrikas-kuesten-100.html> (eingesehen am 12.4.2023).

Abbildung

Maritimer Nahrungstransport



Anpassung und Übersetzung: 2024 Stiftung Wissenschaft und Politik (SWP)

Quelle: Rob Bailey / Laura Wellesley, *Chokepoints and Vulnerabilities in Global Food Trade*, London: Chatham House, 27.6.2017 (Chatham House Report), S. 48, <https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-27-chokepoints-global-food-trade-embargoed.pdf> (eingesehen am 12.4.2023).

sich Angriffe der Hamas-nahen Huthi-Miliz auf große Transportschiffe im Roten Meer.

- *Politische und institutionelle Faktoren* können etwa in Form von Exportverboten Ausfuhren unterbinden, während die Kapazität von Zollbehörden die Verweildauer und damit die Versorgungsschnelligkeit beeinflusst. Gerade in puncto Verweildauer erweist sich speziell der Nahrungstransport als überaus anfällig. Agrarprodukte sind schnell verderblich, Verzögerungen führen darum in der Regel zu Qualitäts- und damit zu Preisverlust.[15] Darüber hinaus sind diese Produkte von besonders vielen Qualitätsprüfungs-Regelungen betroffen, die je nach Verwaltungskapazität wiederum die Liefergeschwindigkeit und damit die Versorgungssicherheit beeinträchtigen können. Die durchschnittliche Liegezeit in Häfen differiert stark: Im globalen Median lag sie im Jahr 2022 bei dem für den Agrartransport relevanten Schiffstyp Massengutfrachter *(bulk carrier)* bei 2,11 Tagen.[16] Deutschland liegt mit fast zwei Tagen im Durchschnitt. Die Abwicklung

15 J. Verschuur/E. E. Koks/J. W. Hall, »Ports' Criticality in International Trade and Global Supply-Chains«, in: *Nature Communications*, 13 (2022) 4351, doi: 10.1038/s41467-022-32070-0.

16 César Ducruet/Hidekazu Itoh/Olaf Merk, *Time Efficiency at World Container Ports*, International Transport Forum, August 2017 (Discussion Paper Nr. 2014-08), <https://www.itf-oecd.org/sites/default/files/docs/dp201408.pdf> (eingesehen am 12.4.2023.

in türkischen Häfen der wichtigen Ostafrika-Route dauert dagegen mit über vier Tagen doppelt so lang. Sie wurde jüngst infolge des abgeschlossenen Schwarzmeerabkommens noch zeitaufwendiger, da dieses Abkommen besondere Kontrollen verlangte, um sicherzustellen, dass keine verdeckten Waffenlieferungen stattfinden.[17] Zum Teil gab es Vorwürfe, diese Kontrollintensität werde von russischer Seite auch als politischer Hebel genutzt, um Zugeständnisse zu erwirken.

Die bislang wenigen Analysen zu aufgetretenen Störungen zeigen unterschiedliche Anfälligkeiten für die global relevanten Nahrungstransporthäfen auf. Beispielsweise haben Bailey und Wellesley von Chatham House bis zum Jahr 2017 eher klimatisch und institutionell-politisch bedingte Störereignisse ermittelt, andere Sicherheitsfaktoren spielten dagegen nur eine geringe Rolle. Die Passage und die Abwicklung über die Schwarzmeerhäfen waren allerdings auch schon vor der russischen Invasion stark durch Handelsmaßnahmen und damit verbundene Kontrollen belastet.[18]

Fehlende Vernetzung von Schutzregimen für sichere Nahrungsversorgung und sicheren maritimen Transport

Sowohl für die Nahrungsversorgung als auch für die maritime Infrastruktur existieren zahlreiche Schutzansätze auf unterschiedlichen Regimeebenen. Sie funktionieren in der Regel allerdings isoliert. Ihre Vernetzung wäre dringend geboten, da Versorgungssicherheit bei Nahrung unmittelbar mit maritimem Transport verknüpft ist.

Basis: Sichere Nahrungsversorgung als Menschenrecht

Nahrungsversorgung als zu schützendes Ziel hat in vielen Ländern, letztlich aber auch global eine lange politische Tradition. Als Menschenrecht ist sie in Artikel 11 des Sozialpakts der UN von 1966 verankert, der inzwischen von über 170 Staaten ratifiziert wurde. Daraus ergeben sich besondere staatliche Achtungs- und Gewährleistungspflichten, die unter anderem die Sicherstellung der Ernährung für Individuen umfassen, etwa in Form von ausreichend vorhandener Nahrung. Die Schutzpflicht gilt dabei auch für den Fall von Übergriffen durch dritte, nichtstaatliche Akteure wie etwa Unternehmen. Diese Aufgabe kann unter Umständen extraterritoriale Wirkungen entfalten, beispielsweise den Schutz des Rechts auf Nahrung in Drittstaaten. Aus dem Menschenrecht auf Ernährungsschutz ergeben sich einige politische Regeln auch für die EU: So besteht etwa der menschenrechtlich begründete internationale Konsens, bei Sanktionen wie den derzeit gegen Russland verhängten Nahrungsprodukte auszunehmen.[19]

Internationale Ansätze für Versorgungssicherheit und sicheren Transport

Zunächst sind *seerechtliche Regelungen* für den maritimen Transport relevant:[20] Dank starker Hoheitsrechte kann ein Hafenstaat bestimmen, ob und wie er Einfahrt gewährt. Insofern besteht auch kein prinzipielles Recht, fremde Häfen anzulaufen, um dort Handel zu treiben.[21] Diese Möglichkeit kann aber im Falle von Handel mit Nahrung von Bedeutung sein, um das globale Menschenrecht auf Nahrung umsetzen zu können.

Handelspolitische Regelungen können wiederum das dem maritimen Transport zugrundeliegende Routenmuster beeinflussen. So machen etwa Zollvergünstigungen bestimmte Ankunftsländer attraktiver als andere. Bei Handelsvereinbarungen gilt für die EU als Mitglied der Welthandelsorganisation (WTO) deren Regelwerk. Danach gelten im Interesse einer sicheren Nahrungsversorgung allerdings explizit viele Aus-

17 United Nations Conference on Trade and Development (UNCTAD), *Port Call and Performance Statistics. Time Spent in Ports, Vessel Age and Size, Annual*, UNCTAD database, 2021, <https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=170027> (eingesehen am 12.4.2023).

18 Bailey/Wellesley, *Chokepoints and Vulnerabilities* [wie Fn. 10], S. 48.

19 Diane Desierto, »The Human Right to Food, Freedom from Hunger, and SDG 2: Global Food Crisis and Starvation Tactics from the Russian Invasion of Ukraine«, *EJIL:Talk! Blog of the European Journal of International Law*, 9.6.2022, <https://www.ejiltalk.org/the-human-right-to-food-freedom-from-hunger-and-sdg-2-global-food-crisis-and-starvation-tactics-from-the-russian-invasion-of-ukraine/> (eingesehen am 12.4.2023).

20 Vgl. den Beitrag von Christian Schaller in dieser Studie, S. 14ff.

21 Moritz Bollmann u. a., »Das Internationale Seerecht — ein potentes Regelwerk«, in: *World Ocean Review*, 1 (2010) 10, S. 207, <https://worldoceanreview.com/wp-content/downloads/wor1/WOR1_de_Kapitel_10.pdf> (eingesehen am 12.4.2023).

nahmen von der Grundregel offenen Handels.[22] So kann ein Land bei Versorgungsengpässen etwa sehr rigide Exportverbote erlassen (GATT XI). Werden sie von großen Agrarexportländern erlassen, verknappen sie das Weltmarktangebot für importabhängige Länder und treiben so die Preise in die Höhe. Auf Importseite sind wiederum Erhöhungen von — auch von der EU vor langer Zeit definierten — Zöllen auf Agrarerzeugnisse zum Schutz eigener Produktion möglich (Agrarabkommen der WTO, Art. 5), was wiederum die globalen Preise drücken kann, falls es sich um große Nachfrageländer handelt. Zusätzliche *Maßnahmen zur Handelserleichterung* im WTO-Abkommen von 2017 sind etwa eine beschleunigte Grenzabwicklung durch Digitalisierung und technische Unterstützung der konkreten Hafenorganisation. Hierdurch lässt sich die gerade bei Agrarprodukten belastende Umschlagsdauer verkürzen.[23]

Bestehende Monitoring- und Frühwarnsysteme können unterschiedliche Dimensionen von Handel und maritimem Transport verbinden. Anlässlich der letzten großen globalen Agrarpreiskrisen 2008 und 2011 gründete die G20 das Agricultural Market Information System (AMIS). Es soll durch eine bessere Kommunikation über eingetretene Knappheitssituationen Märkte beruhigen und kontraproduktive politische Maßnahmen wie die gerade im Agrarbereich häufigen Exportrestriktionen vermeiden. Zu diesem Zweck erfasst es verschiedene zusammenwirkende Störfaktoren: Neben Preisen ausgewählter Agrarprodukte und Düngemittel zählen dazu auch Energiekosten, die in Form von Öl- und Ethanolpreisen im System erfasst werden. Als Transportinformationen werden bislang hingegen nur die durchschnittlichen Frachtkosten für maritimen Transport erfasst.

Deutsche und europäische Ansätze für Versorgungssicherheit und sicheren Transport

In der EU und in Deutschland entstammen Regelungen zum Schutz maritimer Nahrungsversorgung sehr unterschiedlichen politischen Rahmensetzungen, die unterschiedlichen Schutzlogiken folgen. Sie unterscheiden sich auch je nachdem, ob staatliche oder private Akteure in der Pflicht stehen.

In expliziten *Regulierungen zum Schutz kritischer Infrastruktur* im engeren Sinne wird vor allem die Rolle privater Betreiber definiert. Maritimer Agrarhandel kombiniert dabei zwei oft einzeln behandelte kritische Strukturen — Nahrungssicherung und maritimen Transport. Diese werden in bestehenden Regelungsansätzen unterschiedlich berücksichtigt:

- Der *Nahrungssektor* wurde in Deutschland und der EU lange Zeit mit unterschiedlichen Definitionen als schutzrelevante kritische Infrastruktur bestimmt. Als eine solche Infrastruktur zählte er in Deutschland auch schon vor der neuen Verordnung zur Bestimmung Kritischer Infrastrukturen aus dem Jahr 2023, auf EU-Ebene hingegen erst nach der Reform der beiden Europäischen Richtlinien sowohl zu kritischen Einheiten als auch zur Cybersicherheit. Die beiden EU-Richtlinien stufen den Nahrungssektor allerdings unterschiedlich ein: Unter der neuen *Richtlinie über die Resilienz kritischer Einrichtungen (CER)*[24] gilt Ernährung als einer der elf kritischen Sektoren, für die Pflichten zu Risikoschätzung, -management und -dokumentation sowie festgelegten Überwachungsregeln gelten. Unter der neuen *Richtlinie zur Cybersicherheit (NIS-2)*[25] gilt Nahrung dagegen — anders als etwa Trinkwasser — nur als einer der sieben wichtigen Sektoren, die weniger strengen Betreiberpflichten zum Cybermanagement und schwächeren Kontrollen unterliegen als die elf sogenannten essentiellen Sektoren, die aber wiederum die Seefahrt abdecken.
- *Maritimer Transport* ist in Deutschland in der Komponente »Verkehrssystem in Binnen- und als Seeschifffahrt« im Sektor Transport erfasst. Nach der

22 Bettina Rudloff, *Trade Rules and Food Security – Scope for Domestic Support and Food Stocks*, Berlin: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), September 2015, <https://snrd-asia.org/download/sector_project_agricultural_trade_and_value_chains/Trade-Rules-and-Food-Security.pdf> (eingesehen am 12.4.2023).

23 UNCTAD, *Review of Maritime Transport 2021, Chapter 6: Legal and Regulatory Developments and the Facilitation of Maritime Trade*, 18.11.2021, S. 135, <https://unctad.org/system/files/official-document/rmt2021ch6_en.pdf> (eingesehen am 12.4.2023).

24 Richtlinie (EU) 2022/2557 vom 14.12.2022, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557> (eingesehen am 27.1.2024).

25 Richtlinie (EU) 2022/2555 vom 14.12.2022, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555> (eingesehen am 27.1.2024).

neuen Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)[26] von 2021 zählen zu diesem Sektor auch explizit Häfen, differenziert in drei Anlagetypen inklusive Umschlagsanlagen. Nach der 2022 novellierten EU-Richtlinie für den Schutz kritischer Infrastrukturen (CER) ist Transport ein kritischer Sektor. Maritimer Transport wird darin wie in Deutschland nach unterschiedlichen Typen von Anlagen in Häfen differenziert.

Auf diese zwei als kritisch definierte Infrastrukturen verweisen auch weitere Politikansätze, die jenseits von Betreiberpflichten bestimmte Schutzziele verfolgen:

Bei *Prüfverfahren zu Auslandsinvestitionen* können Investitionen etwa in Infrastrukturen dann ausgeschlossen werden, wenn sie eine Gefährdung der öffentlichen Ordnung befürchten lassen.[27] Während entsprechende Prüfungen in Deutschland nach dem Außenwirtschaftsgesetz (AWG) und der Außenwirtschaftsverordnung (AWV) Nahrungsversorgung nicht als Sektor behandeln, der einem besonderen Gefährdungspotential ausgesetzt ist, verstehen die EU-Regeln der Investitions-Screening-Verordnung bei der Prüfung die Nahrungsgefährdung als mögliches Indiz dafür, ob die öffentliche Ordnung durch Auslandsinvestitionen in Gefahr ist. Maritimer Transport ist insofern implizit abgedeckt, als generell auf Transport als physische kritische Infrastruktur verwiesen wird.

Weitere Schutzansätze stammen aus dem *Katastrophen- und Krisenschutz*, darunter auch aktuell neu verabschiedete »Resilienzansätze«, die vor allem auf Vorsorge für Katastrophenfälle abzielen. In der deutschen Resilienzstrategie beispielsweise werden Ernährung und Transport — allerdings nicht spezifiziert als maritimer Transport — als relevante Themenfelder genannt.[28] Im Nahrungssektor führt dieses Resilienzverständnis etwa dazu, dass Krisen-Nahrungsreserven angelegt werden. Auf EU-Ebene dient die strategische Vorausschau dazu, für unterschiedliche Dimensionen von Resilienz zu sensibilisieren. In dem konkreten und regelmäßigen Monitoring zur Identifizierung von Anfälligkeiten im Rahmen von »Dashboards« taucht maritimer Transport jedoch bislang nicht auf, anders als die Nahrungsmittelversorgung.[29] Angesichts der aufgezeigten Bedeutung von maritimem Transport für die Nahrungsversorgung erscheint ein gemeinsames Monitoring aber dringend geboten.

Das 2022 von der EU-Kommission vorgeschlagene neue *Notfallinstrument für den Binnenmarkt (SMEI)* soll sicherstellen, dass der Binnenmarkt auch in Krisenzeiten wie beispielsweise während der Corona-Pandemie weiterhin funktioniert. Für als kritisch definierte Güter und Dienstleistungen werden dabei verschiedene Maßnahmen vorgeschlagen, die von eher losen Formaten für den Dialog zwischen Agrarakteuren bis hin zu staatlicher Lagerhaltung oder staatlichen Produktionsvorgaben reichen. Gerade die sehr interventionistischen Vorschläge stoßen bei einzelnen Mitgliedstaaten und in der Wirtschaft aber auf starke Kritik. Wirtschaftspolitisch sind sie riskant, da entsprechende Maßnahmen häufig ineffizient sind und der Staat als eigener Marktakteur Ressourcen fehlsteuert. Im Ernährungssektor gibt es mit dem Europäischen Mechanismus zur Krisenvorsorge und Krisenreaktion im Bereich der Ernährungssicherheit (EFSCM) bereits ein eigenes neues Modul, das konkrete Maßnahmen aber bislang auf Austauschformate begrenzt.[30] Dieser Ansatz ist Teil eines spezifischen »Notfallplans«, der in Reaktion auf die Covid-Krise etabliert wurde.[31] Ein weiterer Notfallplan besteht für Transport, inklusive maritimen Transport, im Falle einer Krise; er hat verschiedene Schwerpunkte wie die

26 »Dritte Verordnung zur Änderung der BSI-Kritisverordnung«, in: *Bundesgesetzblatt I*, (1.3.2023) 53, <https://www.recht.bund.de/bgbl/1/2023/53/VO.html> (eingesehen am 4.9.2023).

27 Vgl. den Beitrag von Raphael Bossong in dieser Studie, S. 71ff.

28 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, *Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen*, Berlin, Juli 2022, <https://www.bbk.bund.de/DE/Themen/Nationale-Kontaktstelle-Sendai-Rahmenwerk/Resilienzstrategie/resilienz-strategie_node.html> (eingesehen am 12.4.2023).

29 Europäische Kommission, *2020 Strategic Foresight Report. Charting the Course towards a More Resilient Europe*, COM(2020) 493 final, Brüssel, 9.9.2020, <https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2020-strategic-foresight-report_en> (eingesehen am 12.4.2023).

30 Bettina Rudloff, *Wirtschaftliche Resilienz: Kompass oder Catchword? Welche Fallstricke und Folgeeffekte die EU im Krisenmanagement beachten muss*, Berlin: Stiftung Wissenschaft und Politik, Februar 2022 (SWP-Studie 1/2022), <https://www.swp-berlin.org/publikation/wirtschaftliche-resilienz-kompass-oder-catchword> (eingesehen am 12.4.2023).

31 Europäische Kommission, *Contingency Plan for Ensuring Food Supply and Food Security in Times of Crisis*, COM(2021) 689 final, Brüssel, 12.11.2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:689:FIN> (eingesehen am 12.4.2023).

Koordination von Transportakteuren und die Koordination mit internationalen Partnern.[32]

Schutzregelungen gibt es auch zu Einzelaspekten der Nahrungsversorgung, etwa die *Rohstoffpolitik der EU*, die auch die düngerrelevanten Rohstoffe Phosphat und Phosphorit als kritische Rohstoffe definiert. Für deren internationalen Bezug und damit auch für ihren maritimen Transport sind besondere internationale Partnerschaften und Investitionsförderungen vorgesehen. Die *Gemeinsame Agrarpolitik der EU* schließlich definiert nicht zuletzt nach den Erfahrungen eigener Versorgungsdefizite im Anschluss an den Zweiten Weltkrieg die Nahrungsmittelversorgung der Bevölkerung als relevantes Politikziel.[33]

Die *Europäische maritime Sicherheitsstrategie* von 2014 wird aktuell überarbeitet, der sie ergänzende Aktionsplan nennt explizit die wirtschaftliche und transportrelevante Sicherheit als Schutzziel. Im Zusammenhang mit Nahrungshilfe wird dabei allerdings nur am Rande auf das Thema Nahrungsversorgung eingegangen.[34]

Das größte Defizit all dieser Ansätze, die auf unterschiedlichen regulatorischen Ebenen greifen und unterschiedliche Schwerpunkte haben, ist die Tatsache, dass sie nicht hinreichend über die beiden kritischen Infrastrukturen Nahrung und maritimen Transport hinweg vernetzt sind. Doch nur in ihrem Zusammenspiel lässt sich Versorgungssicherheit als vernetzte kritische Infrastruktur realisieren.

Empfehlungen: Volle Kraft voraus in Richtung mehr Koordinierung, Vernetzung und Internationalität

Die als kritisch identifizierten maritimen Seewege und Häfen sind je nach Region unterschiedlichen Störungsrisiken ausgesetzt, die verschiedene Schutzmaßnahmen erfordern. Einige bestehende Ansätze sind durchaus gut entwickelt, könnten aber weiter ausgebaut werden:

Eine *kontinuierliche Beobachtung* von Störfaktoren ließe sich durch das von der G7 initiierte internationale Monitoringsystem AMIS bewerkstelligen, das auf Erweiterungsmöglichkeiten geprüft werden sollte. Auftretende Störungen des maritimen Transportsystems werden bislang nur dann erfasst, wenn sie sich in globalen Frachtpreisen auf dem internationalen Agrarmarkt niederschlagen. Im »Politikmodul« von AMIS, in dem bislang handelspolitische und marktstörende Maßnahmen wie Exportverbote einzelner Länder erfasst werden, sollten Informationen zu Störungen in maritimen Passagen stärker nach Regionen differenziert werden. Zudem ließe sich die von Baily und Wellesley 2017 (siehe Abbildung, S. 42) eingeführte Risikoampel kontinuierlich weiterentwickeln, indem auftretende Störungen wie etwa der gegenwärtige Angriffskrieg Russlands laufend eingespeist würden.

Eine *Abschätzung möglicher Alternativrouten*, die gegebenenfalls schnell nutzbar sind, sollte kontinuierlich erfolgen. Hierfür ist nicht nur eine vorausschauende Kooperation mit dafür relevanten Partnern nötig, sondern auch eine rechtzeitige Kommunikation, um die erforderliche politische Akzeptanz sicherzustellen. Dies zeigt sich aktuell an den Konflikten über Solidaritätskorridore für Agrarexporte aus der Ukraine, die osteuropäische EU-Mitgliedstaaten einem erhöhten Wettbewerbsdruck aussetzen.

Angesichts der Vernetztheit der beiden Infrastrukturen Nahrung und maritimer Transport ist vor allem eine *politikübergeifende Koordinierung* angezeigt. Die geeigneten und bestehenden vielfältigen Schutzmaßnahmen entstammen sehr unterschiedlichen Politikbereichen, etwa der Handels-, Entwicklungs-, Umwelt-, Katastrophenschutz-, Verteidigungs- und Sicherheitspolitik. Im Zuge des Kriegs gegen die Ukraine hat sich gezeigt, dass es möglich ist, verschiedene Akteure und Politikfelder zusammenzubringen, um nachteilige Folgen für die Nahrungsversorgung aufzufangen. So finden sich in dem Unterstützungspaket der EU für die Ukraine Maßnahmen zur Handelserleichterung sowie zur Unterstützung von Routen, die Alternativen zur Schwarzmeerpassage bieten, teils auf dem Landweg, teils über Gewässertransportwege wie der Donau.[35] Die darauf beruhende Koope-

32 Europäische Kommission, *A Contingency Plan for Transport*, COM(2022) 211 final, Brüssel, 23.5.2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A211%3AFIN> (eingesehen am 12.4.2023).

33 Rudloff, *Wirtschaftliche Resilienz* [wie Fn. 30].

34 Rat der Europäischen Union, *Council Conclusions on the Revision of the European Union Maritime Security Strategy (EUMSS) Action Plan (26 June 2018)*, Brüssel, 26.6.2018, <https://oceans-and-fisheries.ec.europa.eu/system/files/2021-03/2018-06-26-eumss-revised-action-plan_en.pdf> (eingesehen am 30.10.2023).

35 Bettina Rudloff, »Politischer Umgang mit Nahrungsrisiken: Herausforderungen, Optionen und Verbesserungsansätze«, in: *Wirtschaftsdienst: Zeitschrift für Wirtschaftspolitik*, Konferenzheft: Ökonomische Folgen des Krieges, 103 (2023) 13, S. 50–56, <https://www.wirtschaftsdienst.eu/

ration erfolgte aber eher als Ad-hoc-Krisenreaktion und beruhte weniger auf vorausschauender und prinzipieller Koordinierung. Hier ließen sich bestehende, bislang aber eher national ausgerichtete Ansätze europäischer und auch internationaler vernetzen, was in der aktuellen Revision der Maritimen Sicherheitsstrategie der EU berücksichtigt werden sollte.[36]

Der vernetzte Schutz kritischer Infrastruktur sollte international koordiniert erfolgen.

Eine verstärkte internationale Koordinierung des Schutzes kritischer Infrastruktur ist aber — abgesehen vom Monitoring — nach wie vor kaum festzustellen. Im Rahmen der G7 böte ein besserer und intensiverer Austausch über maritime und nahrungsbezogene Infrastrukturen die Möglichkeit, Koordinierungsansätze zu ermitteln. Die USA und Kanada etwa verfolgen einen ähnlichen Schutzansatz wie die EU und streben schon länger eine bilaterale Kooperation an.[37] Angesichts der Tatsache, dass die G7 große Agrarproduktions- und -exportländer vereint, könnte eine engere Koordination der Maßnahmen zum Schutz kritischer Transportinfrastruktur allein dieser Staaten einen großen Beitrag zur Verbesserung der Versorgung leisten, etwa indem sie im Falle von Transporthemmnissen gemeinsam agieren.

Diese Infrastrukturansätze definieren meist private Pflichten, die aber mit anderen Ansätzen von Regierungsakteuren wie etwa der Handelspolitik zusammengedacht werden sollten: So können sich handelspolitische Ansätze und Infrastrukturmaßnahmen wechselseitig unterstützen. Basierend auf einem kritikalitätsbezogenen Monitoring könnte die EU darüber hinaus entsprechende Transport-Partnerschaften gezielt mit jenen Ländern anstreben, die für strategisch relevante und vulnerable Passagen und Häfen entscheidend sind — etwa mit der Türkei in Bezug auf die Schwarzmeerpassage und mit Ägypten in Bezug auf den Suezkanal (siehe Tabelle, S. 41). Dies könnte auch ein Gegengewicht zu Chinas Projekt einer neuen Seidenstraße bilden, das bereits in zahlreichen Ländern zumindest Partnerschaftsabkommen mit China auch zu Hafenprojekten umfasst.

In Einzelfällen kann schließlich auch eine militärische Absicherung von Seewegen oder Häfen sinnvoll sein: So wurden etwa zur Eindämmung der versorgungsgefährdenden Piraterie militärisch initiierte Operationen wie die EU-Mission »Atalanta« durchgeführt. Entscheidend sind hier die jeweilige Bedrohungslage, aus der sich eine mögliche Begründung für militärische Einsätze ableiten lässt. Aktuell haben die USA eine internationale Allianz initiiert, die den militärischen Schutz von Handelsschiffen im Roten Meer gegen die Angriffe der Huthi-Rebellen sicherstellen sollen.[38]

Alle genannten Empfehlungen könnten sich prioritär auf die Chokepoints beziehen, die als maßgeblich für die Nahrungsversorgung identifiziert worden sind. Wo immer Chokepoints, die für den Transport von Nahrung und Energie relevant sind, nicht nur einen Staat allein betreffen, sollten international Synergien genutzt und gemeinsame Maßnahmen getroffen werden (siehe die Karte in den Schlussfolgerungen, S. 81).

inhalt/jahr/2023/heft/13/beitrag/politischer-umgang-mit-nahrungsrisiken-herausforderungen-optionen-und-verbesserungsansaetze.html> (eingesehen am 12.4.2023).

36 Rat der Europäischen Union, *European Union Maritime Security Strategy*, Brüssel, 24.6.2014, <https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf> (eingesehen am 30.10.2023).

37 Public Safety Canada/US Homeland Security, *Canada–United States Action Plan for Critical Infrastructure*, 2010, <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx> (eingesehen am 12.4.2023).

38 Vgl. den Beitrag von Göran Swistek in dieser Studie, S. 59ff.

Daniel Voelsen

Untersee-Datenkabel. Kritische Knotenpunkte im Netz globaler Kommunikation

Einleitung

Seit dem 19. Jahrhundert werden Kabel am Meeresboden genutzt, um Informationen zwischen den Kontinenten auszutauschen. Entstanden in Zeiten ausgedehnter kolonialer Imperien, bildet das Netz der Unterseekabel heute das physische Fundament des globalen Internets. Mehr als 95 Prozent des interkontinentalen Datenverkehrs werden über diese Kabel abgewickelt.[1] Vieles spricht dafür, dass zukünftig der bisher nur sehr randständige Austausch von Daten über Satelliten an Bedeutung gewinnen und damit den Kabeln Konkurrenz machen wird.[2] Auf absehbare Zeit wird der wachsende Bedarf an Austausch von Daten zwischen den Kontinenten gleichwohl auch weiterhin nicht ohne Unterseekabel zu decken sein.

Angesichts der enormen Bedeutung dieser Kabel ist es durchaus erstaunlich, dass sie in der Regel nur wenig Aufmerksamkeit erfahren.[3] Für die Nutzerinnen und Nutzer digitaler Dienste gibt es im Grunde keinen Anlass, sich mit der dahinterstehenden Infrastruktur zu beschäftigen, seien es die grundlegenden technischen Protokolle und Standards oder eben die physischen Verbindungswege. Das Gleiche gilt für Unternehmen wie auch für die meisten öffentlichen Institutionen. Hinzu kommt, dass Datenkabel am Grund des Meeres den meisten Menschen auch visuell verborgen bleiben.

Die zunehmenden geopolitischen Konflikte der letzten Jahre haben das Netz der Unterseekabel jedoch verstärkt in den Fokus gerückt, vor allem im politischen Raum. In der Konfrontation zwischen den USA und China lassen beide Seiten ein ausgeprägtes Bewusstsein für die strategische Bedeutung dieser Kabel erkennen — was auch in anderen Staaten mittlerweile entsprechende Debatten auslöst. Im Zentrum stehen dabei in der Regel die Gefahren durch Spionage und Sabotage sowie das Risiko wachsender technologischer Abhängigkeiten.

Eine konkrete Zuspitzung finden diese Debatten im Kontext der europäischen und deutschen Bemühungen um den Schutz kritischer Infrastrukturen. So definiert die jüngste Verordnung zum deutschen IT-Sicherheitsgesetz vom 23. Februar 2023 erstmals Anlandestationen von Unterseekabeln als kritische Infrastrukturen. Klärungsbedarf besteht allerdings noch bei den Kabeln selbst. Zwar definierte schon die erste Verordnung zum IT-Sicherheitsgesetz »Übertragungsnetze« als kritische Infrastruktur; da die Seekabelanlandestationen nun aber eigens aufgeführt werden und die Verordnungen ansonsten sehr explizit und präzise sind, ist davon auszugehen, dass Unterseekabel bisher nicht zu den besonders schützenswerten Übertragungsnetzen gezählt werden.

Die im November 2022 in Kraft getretene überarbeitete europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) weist im Kontext der Ausführungen zu Anbietern öffentlicher elektronischer Kommunikationsnetze hingegen explizit auf die Bedeutung von Unterseekabeln hin. Verbunden wird dies mit dem Auftrag an die Mitgliedstaaten, die Sicherheit der Kabel im Rahmen nationaler Cybersicherheitsstrategien zu berücksichtigen. Allerdings findet sich hier eine interessante Einschränkung: Im englischen Text heißt es, der Schutz dieser Kabel sei sicherzustellen,

1 Douglas R. Burnett/Robert Beckman/Tara M. Davenport (Hg.), *Submarine Cables. The Handbook of Law and Policy*, Leiden 2013, S. 9; Alan Mauldin, »Do Submarine Cables Account for over 99% of Intercontinental Data Traffic?«, <https://blog.telegeography.com/2023-mythbusting-part-3>.

2 Daniel Voelsen, *Internet aus dem Weltraum*, Berlin: Stiftung Wissenschaft und Politik, Februar 2021 (SWP-Studie 2/2021), doi: 10.18449/2021S02.

3 Vgl. Christian Bueger/Tobias Liebetrau, »Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network«, in: *Contemporary Security Policy*, 42 (2021) 3, S. 391—413.

SWP Berlin
Maritime kritische Infrastrukturen
Februar 2024

»where relevant« — im Deutschen etwas eigentümlich übersetzt mit »gegebenenfalls«.[4]

Tatsächlich verbirgt sich hinter diesen sprachlichen Wendungen ein für die Praxis relevantes Problem: Während das System der Unterseekabel als Ganzes unverzichtbar ist, lässt sich dies nicht sinnvoll für jedes einzelne Kabel und auch nicht für jeden einzelnen Anlandepunkt behaupten. Insofern gilt es in der Tat zu klären, wo der Schutz von Unterseekabeln in besonderem Maße relevant ist — und wo nicht.

Dazu soll im Folgenden das Netz der Unterseekabel als ein technisches und soziales Netzwerk untersucht werden, in dem im Laufe der Zeit zentrale Knotenpunkte entstanden sind.[5] An diesen Knotenpunkten ist die Gefahr von Spionage und Sabotage besonders groß, so dass sich diese Teile des Netzwerkes tatsächlich als in besonderem Maße kritisch verstehen lassen. Aus der Perspektive deutscher Außen- und Sicherheitspolitik ist demnach eben nicht jedes einzelne Kabel entscheidend. Vielmehr gilt es in den Blick zu nehmen, welche Verbindungen zu anderen Weltregionen für Deutschland als Teil Europas von besonderer Bedeutung sind. In den Fokus rücken damit konkret die Verbindungen nach Nord- und Südamerika, nach Afrika sowie nach Asien. Historische Erfahrungen liefern dabei Hinweise darauf, wie genau sich die Bedrohungen erfassen lassen, denen diese Verbindungen ausgesetzt sind.

Das globale Netzwerk der Unterseekabel

Wie eingangs angedeutet, reicht die Geschichte der Unterseekabel bis in die Zeit des Kolonialismus zurück. Die Entwicklung erster Kabel war maßgeblich getrieben vom Interesse europäischer Regierungen, schnell auf Ereignisse in den Kolonien reagieren zu können. Neben diesem staatlichen Interesse gab es aber auch damals schon Unternehmen, die sich von dieser neuen Kommunikationstechnologie Vorteile für den weltweiten Handel versprachen. Die Folge war eine oftmals eher undurchsichtige Kooperation von Staaten und Unternehmen.[6]

Heute geht es nicht mehr um die Sicherung kolonialer Herrschaft. Unterseekabel sind aber weiterhin ein Instrument politischer wie wirtschaftlicher Machtprojektion.

Seit den Zeiten der Kolonialreiche hat sich die Technologie weiterentwickelt; moderne Glasfaserleitungen können heute Daten in Mengen und Geschwindigkeiten übertragen, die im 19. Jahrhundert und auch noch bis weit in das 20. Jahrhundert hinein unvorstellbar waren. Die strategische Bedeutung der Kabel aber ist ähnlich geblieben: Wenngleich es heute nicht mehr um die Sicherung kolonialer Herrschaft geht, gilt doch weiterhin, dass Unterseekabel ein Instrument politischer wie wirtschaftlicher Machtprojektion sind. Politisch erlauben sie den Zugriff auf Datenströme bis hin zu deren Kontrolle; wirtschaftlich erschließen sie neue Märkte und eröffnen Raum für neue Geschäftsmodelle.

Eine weitere Konstante ist das Nebeneinander staatlicher wie unternehmerischer Aktivitäten. Mehr als 90 Prozent der Kabel sind im Besitz von Unternehmen,[7] von denen sich wiederum einige zum Teil oder auch gänzlich in staatlichem Besitz befinden. Zudem üben Staaten die Kontrolle über die Küsten und damit über die Anlandepunkte der Kabel aus.

Ein gewichtiger Unterschied zwischen den frühen Kabelverbindungen und dem heutigen Netzwerk besteht in der Art und Weise, wie die Informationen übertragen werden. Technisch vereinfacht gesprochen, waren frühe Kabel, wie etwa auch im Fall des klassischen analogen Telefons, Punkt-zu-Punkt-Verbindungen. Zwischen zwei Endpunkten wurde physisch eine Verbindung hergestellt, die exklusiv dazu diente, Daten zwischen diesen Endpunkten auszutauschen.

Der heutige Datenverkehr des Internets dagegen wird auf Ebene der Protokolle gänzlich anders gesteu-

4 Europäisches Parlament/Europäischer Rat, *Richtlinie 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*, Brüssel, 14.12.2022, Kapitel II, Artikel 7, 2 (d), <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555>.

5 Zum netzwerktheoretischen Hintergrund der folgenden Ausführungen siehe Julia Pohle/Daniel Voelsen, »Das Netz und die Netze. Vom Wandel des Internets und der globalen digitalen Ordnung«, in: *Berliner Journal für Soziologie*, 32 (2022) 3, S. 455—487.

6 Heidi J. Tworek, *News from Germany. The Competition to Control World Communications, 1900—1945*, Cambridge 2019.

7 Douglas R. Burnett/Robert Beckman/Tara M. Davenport (Hg.), *Submarine Cables. The Handbook of Law and Policy*, Leiden 2013, S. 9.

ert. Wiederum vereinfacht dargestellt: Allen Endgeräten stehen hier grundsätzlich alle physischen Verbindungen zur Verfügung, also auch alle Kabelverbindungen. Die Kommunikation zwischen zwei Endgeräten wird dabei in kleine Informationspakete aufgeteilt, die sich von allen möglichen Verbindungswegen den jeweils zu dem Zeitpunkt schnellsten verfügbaren Weg aussuchen. Somit ist es ganz normal, dass nicht alle Datenpakete den gleichen Weg nehmen. Vor allem aber verfügt das System über ein hohes Maß an Resilienz, da Ausfälle einzelner Verbindungen nahezu in Echtzeit über die Auswahl einer neuen Verbindung kompensiert werden können.[8]

Diese Idee des paketbasierten Transfers hat sich vielfach bewährt, stößt allerdings immer wieder auch auf Hindernisse. Denn neben den technischen Grundlagen basiert dieses System eben auch auf einem sozialen Netzwerk, in dem die Eigentümer und Betreiber von Teilsystemen sich darauf verständigen müssen, wie und unter welchen Bedingungen sie den Transfer der Datenpakete durch die von ihnen betriebenen Teilnetze erlauben.

Obwohl die Vorstellung von einem dezentralen Internet bis heute wirkmächtig ist, zeigen sich gerade mit Blick auf die Unterseekabel starke Zentralisierungstendenzen. Für die beteiligten Unternehmen spielen hierbei insbesondere Kostenfaktoren eine Rolle. Es ist in der Regel günstiger, Anlandepunkte und Routen mehrfach zu nutzen, wenn diese sich in der Vergangenheit bewährt haben. Nicht zufällig sind dementsprechend auch in der Topografie des Netzwerks der Unterseekabel noch immer Spuren der Kolonialgeschichte zu erkennen.[9]

Spionage und Sabotage

Die Kommunikation über Unterseekabel ist mit zwei zentralen Gefahren konfrontiert: einerseits der Spionage und andererseits der Sabotage. Da zu aktuellen Vorfällen wenig Informationen verfügbar sind, lohnt sich der Blick in die Geschichte, um diese Risiken zu verdeutlichen.

Spionage

Ein spektakuläres Beispiel für eine Spionageaktion, die auf ein Unterseekabel zielte, ist die von den USA ab 1971 durchgeführte Operation »Ivy Bells«. Vor dem Hintergrund des Kalten Krieges wurde ein Abhörgerät an einem Kabel angebracht, das durch das Ochotskische Meer verlief und der Anbindung einer sowjetischen Marinestation auf der Halbinsel Kamtschatka diente. Die Aufnahmen, die jeden Monat von Tauchern eingesammelt werden mussten, sollen den USA hoch relevante Einsichten vermittelt haben. Den Berichten zufolge wurde ihre Auswertung dadurch erleichtert, dass die sowjetische Marine bei der Nutzung dieses Kabels angeblich auf jedwede Verschlüsselung verzichtet hatte.[10]

Im Zuge der Enthüllungen von Edward Snowden wurde im Jahr 2013 öffentlich bekannt, dass die amerikanische National Security Agency (NSA) in Zusammenarbeit mit dem britischen Government Communications Headquarters (GCHQ) im großen Stil den Datenverkehr über Unterseekabel erfasst und auswertet, anscheinend sowohl durch das Abhören von Kabeln als auch durch das direkte Abgreifen von Daten an den Seekabelanlandestationen. In ähnlicher Weise, wenn auch nicht direkt auf maritime Infrastrukturen bezogen, erfasst der deutsche Bundesnachrichtendienst Daten am größten deutschen Internetknotenpunkt De-Cix.[11]

Vor dem Hintergrund dieser öffentlichen Informationen über die Fähigkeiten westlicher Nachrichtendienste ist davon auszugehen, dass auch andere Staaten über solche Möglichkeiten verfügen oder zumindest danach streben, entsprechende Fähigkeiten zu erlangen. So mehren sich seit einigen Jahren Berichte über verdächtige Aktivitäten russischer Schiffe in der Nähe relevanter Unterseekabel.

8 Daniel Voelsen, *Risse im Fundament des Internets. Die Zukunft der Netz-Infrastruktur und die globale Internet Governance*, Berlin: Stiftung Wissenschaft und Politik, Mai 2019 (SWP-Studie 12/2019), doi: 10.18449/2019S12.

9 Nicole Starosielski, *The Undersea Network*, Durham 2015.

10 Caitlin Morris, »Operation IVY BELLS: Lessons Learned from an ›Intelligence Success‹«, in: *Journal of the Australian Institute of Professional Intelligence Officers*, 20 (Juli 2015) 3, S. 17–29.

11 Bundesverwaltungsgericht, »Klage der DE-CIX Management GmbH erfolglos«, Pressemitteilung, Berlin, 31.5.2018, <https://www.bverwg.de/pm/2018/38> (eingesehen am 27.9.2023).

Vieles spricht dafür, dass Unterseekabel schon heute Angriffspunkte für Spionage-Operationen sind und dies auch in Zukunft sein werden.

In der Summe spricht vieles dafür, dass Unterseekabel schon heute Angriffspunkte für Spionage-Operationen sind und dies auch in Zukunft sein werden. Weiter ist davon auszugehen, dass diese Operationen nicht nur auf staatliche Stellen zielen, sondern auch Wirtschaft, Wissenschaft und Zivilgesellschaft betreffen.

Sabotage

Jedes Jahr kommt es zu Ausfällen und Störungen einzelner Unterseekabel. Die Ursache sind häufig Materialschäden aufgrund der Belastungen, denen die Kabel am Meeresgrund ausgesetzt sind. Immer wieder wird auch davon berichtet, dass sich Schleppnetze von Fischerbooten in den Kabeln verhaken und dabei beschädigen. Die Betreiber der Unterseekabel sind auf diese Vorfälle eingestellt, so dass die Verbindungen in der Regel rasch repariert werden können.

Neben diesen natürlich verursachten oder im Falle der Fischer zumindest nicht beabsichtigten Störungen gilt die Sorge aber auch gezielten Angriffen, also der Sabotage von Unterseeleitungen.

Eine Reihe westlicher Regierungen warnt davor, dass insbesondere Russland die Fähigkeiten besitzt, Unterseekabel auch in großer Tiefe zu beschädigen. Wie im Falle der Spionage ist allerdings davon auszugehen, dass weitere Staaten über entsprechende Möglichkeiten verfügen. Es ist insofern durchaus bemerkenswert, dass es seit der Ausbreitung des Internets in den 1990er Jahren keinen Fall gab, in dem eindeutig und öffentlich festgestellt wurde, dass der Ausfall eines Kabels auf gezielte Sabotage zurückzuführen ist.

Dies lässt sich zum einen dadurch erklären, dass es vergleichsweise einfach ist, eine gezielte Sabotage als Unfall erscheinen zu lassen. So kann ein Staat seine Fähigkeit, einem anderen Staat zu schaden, vorführen, ohne dafür in der Öffentlichkeit einen diplomatischen Preis zahlen zu müssen. Ein aktuelles Beispiel hierfür ist die Durchtrennung von zwei Kabeln, die eine Inselgruppe mit Taiwan verbinden, durch chinesische zivile Schiffe im März 2023.[12] Angesichts der Spannungen zwischen China und Taiwan sind zwei derartige Unfälle in jedem Fall verdächtig. Eine militärische Operation Chinas wird aber kaum als solche nachzuweisen sein. Und dies ist im Übrigen gar nicht nötig, denn auch ohne Nachweis wurde Taiwan durch diesen Vorfall die eigene Verletzbarkeit an dieser Stelle vor Augen geführt.[13]

Würde ein Staat sich offen dazu bekennen, Kabelverbindungen von strategischer Bedeutung für einen anderen Staat anzugreifen, würde der betroffene Staat dies sicher als Aggression werten und wahrscheinlich mit entsprechenden Reaktionen beantworten. Anders als im Falle von Spionage oder niedrigschwelligeren Cyberangriffen erscheint ein solch physischer Angriff also vor allem im Kontext einer offenen zwischenstaatlichen Konfrontation vorstellbar. Hierzu passt auch das historisch prominenteste Beispiel: Unmittelbar nach Beginn des Ersten Weltkrieges bestand eine der ersten Aktionen der britischen Marine darin, Telegraphenverbindungen des Deutschen Reiches zu kappen.

Der Umstand, dass russische Schiffe und U-Boote in den letzten Jahren wiederholt in der Nähe wichtiger transatlantischer Kabelverbindungen vor der Küste Großbritanniens gesichtet wurden, ist vor diesem Hintergrund sicher kein Zufall, sondern als bewusste Drohung zu verstehen.[14]

Neben physischen Angriffen auf die Kabelverbindungen besteht zudem das Risiko von Störungen der Steuerungssysteme durch Cyberangriffe. Würden diese Systeme zur Steuerung der Datenflüsse etwa

12 Martin Holland, »Taiwan: Chinesische Schiffe durchtrennen zwei Unterseekabel zu Inselgruppe«, in: *heise online*, 8.3.2023, <https://www.heise.de/news/Taiwan-Chinesische-Schiffe-duchtrennen-gleich-zwei-Unterseekabel-zu-Inselgruppe-7538607.html> (eingesehen am 14.8.2023); Huizhong Wu/Johnson Lai, »Taiwan Suspects Chinese Ships Cut Islands' Internet Cables«, *AP News*, 18.4.2023, <https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70> (eingesehen am 15.8.2023).

13 Roman Winkelhahn u. a., »Lehren aus dem Ukrainekrieg: Wie Taiwan eine digitale Festung errichtet«, in: *Handelsblatt* (online), 2.12.2022, <https://www.handelsblatt.com/politik/international/satelliten-gegen-propaganda-lehren-aus-dem-ukraine-krieg-wie-taiwan-eine-krisensichere-digitale-festung-errichtet/28826932.html> (eingesehen am 22.8.2023).

14 Lukas Mäder u. a., »Unterwasser-Krieg: Wie verletzlich sind Europas Internetkabel?«, in: *Neue Zürcher Zeitung* (online), 5.10.2022, <https://www.nzz.ch/technologie/nach-anschlag-auf-pipeline-europas-datenkabel-liegen-tief-im-meer-ungeschuetzt-vor-spionage-und-sabotage-ld.1705274> (eingesehen am 15.8.2023).

Tabelle

Anlandepunkte von Unterseekabeln an der deutschen Küste

Anlandepunkt in Deutschland	*Name des Kabels*	*Endpunkt*	*Inbetriebnahme*	*Kapazität (Tbps)*
Sylt	Atlantic Crossing 1	Brookhaven, NY, USA	1998	5,2
Sylt	Cantat 3	Vestmannaeyjar, Island	1994	0,0075
Rostock	C-Lion 1	Hanko, Finnland	2016	144
Rostock	Elektra-GlobalConnect 1	Gedser, Dänemark	2000	n. a.
Rostock	GlobalConnect-KPN	Gedser, Dänemark	2006	n. a.
Rostock-Markgrafenheide	Germany-Denmark 3	Gedser, Dänemark	2000	n. a.
Puttgarden	Fehmarn Bält	Rødbyhavn, Dänemark	2000	0,0025
Sassnitz	Digital E4	Stockholm, Schweden	2023	3052

gezielt manipuliert, könnte das die Kabel vorübergehend unbrauchbar machen.

Kritische Knotenpunkte

Das Ausmaß der Bedrohung einzelner Staaten durch Spionage und Sabotage hängt wesentlich davon ab, wie diese an das Netz der Unterseekabel angebunden sind. Besonders gefährdet sind Verdichtungen von Verbindungen an zentralen Knotenpunkten: Je stärker konzentriert die Datenverbindungen sind, desto größer ist das Potential für ein erfolgreiches Abgreifen von Daten oder für folgenreiche Störungen von Datenflüssen.

Deutschland

Im Falle Deutschlands geraten zunächst die vier Anlandepunkte an Nord- und Ostsee in den Blick (siehe Tabelle).

Die Übersicht zu den direkten deutschen Kabelverbindungen zeigt anschaulich die technische Entwicklung im Laufe der Zeit: Viele ältere Kabelverbindungen haben heute nur noch geringe Bedeutung, weil neuere Kabelverbindungen eine um ein Vielfaches höhere Übertragungskapazität aufweisen. Die Anbindung an das transatlantische Kabel von Sylt aus etwa spielt mit einer Übertragungskapazität von 5,2 Tbps (Terabit pro Sekunde) kaum eine Rolle im Vergleich zu neueren transatlantischen Kabeln wie EllaLink oder Marea, die jeweils Übertragungskapazitäten von mehreren Hundert Tbps haben. Dementsprechend wäre davon auszugehen, dass diese älteren Verbindungen allenfalls nachrangige Ziele von Sabotageakten und Spionagemaßnahmen wären.

Der europäische Kontinent

Um die Bedrohung für Deutschland zu erfassen, ist es daher notwendig, den europäischen Kontinent als Ganzes in den Blick zu nehmen. Deutschland ist in vielfältiger Weise über terrestrische Verbindungen mit seinen Nachbarn verbunden — und über diese an das Netz der Unterseekabel angeschlossen.

So rückt im zweiten Schritt die Frage in den Fokus, welchen Bedrohungen die Anbindung der Staaten Europas insgesamt ausgesetzt ist.[15]

15 Vgl. für ähnlich vorgehende Analysen auch Christian Bueger/Tobias Liebetrau/Jonas Franken, *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*, Europäisches Parlament, Policy Department for External Relations, 1.6.2022, S. 16ff, <https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf>; Johann Schlamp/Thomas C. Schmidt/Matthias Wählisch, *Auslandsverbindungen und CDN-Kompetenz (ZwIBACK). Zweite Internet Backbone-Studie – Projekt 415 Los 1*, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 21.2.2022, S. 198ff, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ZwiBACK/ZwiBACK-Studie.pdf?__blob=publicationFile&v=3> (eingesehen am 22.8.2023).

- Die Verbindungen in die *USA* sind in der Vergangenheit zum größten Teil von der Südwestküste des Vereinigten Königreichs und der südlichen Küste Irlands ausgegangen (zusammengerechnet Kapazitäten von 329 Tbps).[16] In den letzten Jahren sind allerdings einige neue Kabel in Betrieb genommen worden, die einen zweiten europäischen Landepunkt in Spanien (Grace Hopper) oder Frankreich (Amitie/AEC-2) haben oder sogar ausschließlich von Spanien (Marea) oder Frankreich (Dunant) in die USA reichen. Diese neuen Kabel verfügen zusammen über eine Kapazität von 1.132 Tbps, also ungefähr vier Mal so viel wie die älteren Kabel, die im Vereinigten Königreich starten. Wenn 2024 die US-Firma Meta das Kabel Anjana von Spanien aus in Betrieb nimmt, kommen noch einmal 480 Tbps hinzu. Neben den Gewässern an der Südwestküste Englands wächst damit die Bedeutung der Biskaya für die Verbindungen in die USA.
- Verbindungen nach *Nordafrika*, in den *Nahen Osten* und weiter bis nach *Asien* starten zu einem großen Teil in Marseille, oftmals ergänzt durch Anschlüsse an weitere EU-Staaten mit Mittelmeerküste. Aktuell sind hier zehn Kabel in Betrieb, von denen zwei bis Indien (2Africa, IMEWE), eines direkt bis nach China (Asia-Africa-Europe) und zwei bis Singapur als einem zentralen Hub in Asien (PEACE, Sea-Me-We 4) reichen. Wie bei den Verbindungen in die USA zeichnen sich neue Kabelverbindungen durch deutlich höhere Übertragungskapazitäten aus: So hat das PEACE-Kabel eine maximale Kapazität von 192 Tbps; während Sea-Me-We 4 nur 4,6 Tbps erlaubt, soll der für 2025 angekündigte Nachfolger Sea-Me-We 6 eine Kapazität von 126 Tbps ermöglichen. Viel Aufmerksamkeit hat das 2Africa-Kabel erfahren, das unter starker Beteiligung von Meta wie auch China Mobile den afrikanischen Kontinent mit einer neuen Kabelverbindung umschließt, die mit 180 Tbps über eine sehr hohe Datenübertragungskapazität verfügt.
- Schließlich kommt der portugiesischen Atlantikküste eine besondere Bedeutung zu. Das 2Africa-Kabel hat dort neben Marseille seinen zweiten Anlandepunkt auf dem europäischen Festland. Zudem startet von hier das von der EU geförderte EllaLink-Kabel, das Europa ohne den Umweg über Nordamerika erstmals direkt mit *Lateinamerika* verbindet. EllaLink weist eine maximale Übertragungskapazität von 100 Tbps auf.

Weil ein Großteil des internationalen Datenverkehrs aus Europa heraus über diese Knotenpunkte verläuft, sind sie prinzipiell im Sinne der Spionage von besonderem Interesse.

Auch das Risiko der Sabotage ist an all diesen Knotenpunkten besonders hoch. Wie eine aktuelle Studie im Auftrag des BSI technisch detailliert nachzeichnet, würden Störungen an einem der zentralen Landungspunkte gleichwohl keine ernsthafte Bedrohung darstellen.[17] So wurden im Oktober 2022 drei von Marseille ausgehende Kabel gleichzeitig beschädigt — unter noch ungeklärten Umständen. Dies hatte zwar durchaus Verzögerungen und Datenverluste auf den direkt betroffenen Routen zur Folge, konnte aber im Wesentlichen durch Umleitungen des Datenverkehrs auf andere Routen ausgeglichen werden.

Träten gleichzeitig Störungen an mehreren für Europa zentralen Anschlüssen an das globale Netz der Unterseekabel auf, würde es bedrohlich.

Eine echte und ernsthafte Bedrohung entstünde allerdings dann, wenn es gleichzeitig zu Störungen an mehreren der für Europa zentralen Anschlüsse an das globale Netz der Unterseekabel kommen würde. Ein koordinierter Angriff wäre, wie schon beschrieben, nur im Kontext einer massiven zwischenstaatlichen Konfrontation vorstellbar, bei der sich die EU Staaten gegenübersähe, die über entsprechende maritime Fähigkeiten verfügten. Ein solches Szenario ist zwar nach wie vor sehr unwahrscheinlich, aber nicht gänzlich auszuschließen.

Marktkonzentration als politisches Risiko

Neben den räumlichen Verdichtungen an diesen Knotenpunkten zeigt sich mit Blick auf das europäische Netz der Unterseekabel auch noch in anderer Hinsicht eine Verdichtung: Ein Großteil der neueren Kabelprojekte, die durch ihre hohen Datentransferkapazitäten herausstechen, wird exklusiv oder zumindest unter substanzieller Beteiligung der großen US-Tech-Konzerne betrieben — also Alphabet, Ama-

16 Insbesondere zur Bedeutung Irlands siehe Robert McCabe/Brendan Flynn, »Under the Radar: Ireland, Maritime Security Capacity, and the Governance of Subsea Infrastructure«, in: *European Security*, (2023), S. 1—21.

17 Schlamp/Schmidt/Wählisch, *Security Threats to Undersea Communications Cables and Infrastructure* [wie Fn. 15].

zon, Meta und Microsoft.[18] Im globalen Netz der Unterseekabel kommt überdies dem chinesischen Unternehmen HMN (früher Huawei Marine Networks) eine herausgehobene Stellung zu; einigen Berechnungen zufolge hat HMN mittlerweile ein Viertel aller Unterseekabel weltweit verlegt und agiert in vielen Fällen auch als Betreiber.

Diese wirtschaftliche Konzentration verschärft die beschriebenen Risiken von Spionage und Sabotage. Zur räumlichen Konzentration kommt hinzu, dass die Kontrolle über eine große Anzahl wichtiger Kabelverbindungen in den Händen weniger Unternehmen liegt. Diese Verbindungen sind daher besonders attraktive Ziele für Spionage- und Sabotageaktionen. Ein erfolgreicher Cyberangriff auf die Steuersysteme eines solchen Mega-Betreibers etwa könnte globale Auswirkungen haben. Obendrein wächst die technologische Abhängigkeit: Im Falle Europas verschärft sich gerade auf der grundlegenden Infrastrukturebene jene Abhängigkeit von US-Tech-Konzernen, wie sie im Bereich von Anwendungen wie Social-Media-Plattformen und Cloud-Diensten schon seit einigen Jahren zunehmend kritisch gesehen wird.

Kritische Punkte im globalen Netz

Neben diesen für den europäischen Kontinent unmittelbaren Bedrohungen gibt es aber auch Risiken, die sich aus der Topografie des globalen Netzes ergeben. So wie es für Europa Landungspunkte und Routen von besonderer strategischer Bedeutung gibt, finden sich auch im globalen Netz Verdichtungen bzw. Konzentrationen. Durchaus bewusst mit warnendem Unterton wird hier in der internationalen Debatte auch von »Chokepoints« (im Deutschen etwas weniger dramatisch: Nadelöhren) gesprochen. Aus Sicht Europas strategisch besonders wichtig ist dabei die Konzentration von Verbindungslinien im Suezkanal. Nahezu alle Verbindungen Europas mit Asien kommen hier zusammen. Eine Störung dieser Kabel im Suezkanal könnte für Europa somit ebenfalls weitreichende Folgen haben. Zudem ist davon auszugehen, dass sie ein attraktives Ziel von Spionageaktionen darstellen.[19]

Für die Verbindungen nach Asien, insbesondere auch nach China, kommt zudem Singapur die Stellung eines wichtigen Clusters zu. Ein weiteres Beispiel ist Fortaleza in Brasilien: Fast alle Verbindungen zwischen Nord- und Südamerika wie auch die direkte Anbindung Europas über das EllaLink-Kabel laufen dort zusammen.[20]

Schließlich kommt als strategische Herausforderung hinzu, diesen europäischen Blick um eine Perspektive zu ergänzen, welche die Bedrohungen der Partner und Verbündeten Deutschlands in Bezug auf ihre Anbindung an das globale Netz der Unterseekabel mitberücksichtigt. Staaten wie Japan, Taiwan und Australien sind aufgrund ihrer Insellage in besonderem Maße auf Unterseekabel angewiesen, zugleich aber auch noch deutlich unmittelbarer mit dem politischen Machtanspruch Chinas konfrontiert. Viele Partner der deutschen Entwicklungszusammenarbeit sind zudem bloß eingeschränkt und oftmals sogar nur mit einem Kabel an das globale Netz angeschlossen — und entsprechend verwundbar.[21]

Schutzmaßnahmen

Ein umfassender Schutz aller Unterseekabel ist nicht möglich und würde einen unverhältnismäßigen Aufwand erfordern. Die Identifizierung von Knotenpunkten, die aus europäischer Sicht besonders kritisch sind, erlaubt aber zielgerichtete Maßnahmen, um an ebendiesen Stellen den Schutz zu verbessern.

Einstufung ausgewählter Verbindungen als KRITIS

Wie einleitend erwähnt, schreibt die NIS-2-Richtlinie den Mitgliedstaaten die Aufgabe zu, Unterseekabel zu schützen, wo diese besonders relevant sind. Eine Analyse wie die hier durchgeführte bietet dafür die Grund-

18 Andrew Blum/Carey Baraka, »Sea Change«, in: *Rest of World*, 10.5.2022, <https://restofworld.org/2022/google-meta-underwater-cables/> (eingesehen am 22.8.2023); Christopher Mims, »Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power«, in: *The Wall Street Journal* (online), 15.1.2022, <https://www.wsj.com/articles/google-amazon-meta-and-microsoft-weave-a-fiber-optic-web-of-power-11642222824> (eingesehen am 22.8.2023).

19 Paul Cochrane, »Red Sea Cables: How UK and US Spy Agencies Listen to the Middle East«, *Middle East Eye*, 4.3.2021, <https://www.middleeasteye.net/news/red-sea-cables-how-us-uk-spy-agencies-listen-middle-east> (eingesehen am 22.8.2023).

20 Vgl. Voelsen, *Risse im Fundament des Internets* [wie Fn. 8], S. 19ff.

21 Jonas Franken u. a., »The Digital Divide in State Vulnerability to Submarine Communications Cable Failure«, in: *International Journal of Critical Infrastructure Protection*, 38 (2022), Art. 100522.

lage. Würden besonders wichtige Verbindungen auch formal als kritische Infrastrukturen eingestuft, so würde dies nicht nur ein verbindliches Niveau an IT-Sicherheit sicherstellen, sondern auch — und mindestens ebenso wichtig — den Informationsaustausch bei kritischen Vorfällen regeln.

Da Deutschland, wie beschrieben, darauf angewiesen ist, die Unterseekabel seiner europäischen Nachbarn zu nutzen, liegt es in Deutschlands eigenem Interesse, hier eine europäische Verständigung zu finden — die im Sinne eines kontinentalen Blicks auf Europa auch Großbritannien einschließen sollte.

Die Einstufung ausgewählter Unterseekabel und Seekabelanlandestationen kann dazu dienen, ein hohes Grundniveau an Schutz zu gewährleisten.

Die Einstufung ausgewählter Unterseekabel und Seekabelanlandestationen kann dazu dienen, ein hohes Grundniveau an Schutz zu gewährleisten. Allerdings kann den Unternehmen kaum die Verantwortung zugewiesen werden, ihre Anlagen vor gezielten Angriffen durch staatliche Akteure zu schützen. Hier bedarf es ergänzender Schutzmaßnahmen durch staatliche Stellen.

Schutz vor Spionage

Auch in Zukunft werden für eine Reihe von Staaten Versuche attraktiv bleiben, an zentralen Knotenpunkten im Netz der Unterseekabel Daten abzugreifen.

- Das nach jetzigem Stand wirksamste Gegenmittel bildet die starke und konsequente Ende-zu-Ende-Verschlüsselung von Datentransfers. Sind Daten zuverlässig und auf dem aktuellen Stand der Kryptografie verschlüsselt (womöglich in Zukunft unter Rückgriff auf Quanten-Computing), ist es weit weniger ergiebig, in großem Stil Daten im Transfer abzugreifen. Um einen möglichst hohen Schutz zu gewährleisten, müssen dabei auch Metadaten so weit wie technisch möglich verschlüsselt werden, also jene Daten, die Aufschluss darüber geben, wer wann welche Informationen abruft oder mit wem kommuniziert. Regierungen können hier also den Schutz vor Spionage erhöhen, indem sie konsequente Verschlüsselung aktiv befördern, zumindest aber nicht unterminieren.
- Neben dem Einsatz von Verschlüsselungsmethoden besteht eine weitere Möglichkeit des Schutzes vor Spionage darin, den Transfer von Daten über internationale Verbindungen zu reduzieren. Während grundsätzlich der Datenaustausch über das Internet so flexibel angelegt ist, dass Daten auch beim Austausch zwischen zwei Endpunkten, die sich innerhalb eines Landes befinden, bisweilen über andere Länder geleitet werden, erscheint es gerade für besonders sensible Regierungskommunikation wichtig, konsequent darauf zu achten, dass diese über die eigenen Regierungsnetze verläuft oder zumindest so weit wie möglich die Umleitung über internationale Unterseekabel vermeidet. Das kann in einigen Situationen gewisse Einbußen bei der Übermittlungsgeschwindigkeit bedeuten, reduziert dafür aber die Angriffsfläche für Spionageaktivitäten.

Schutz vor Sabotage

Auch mit Blick auf Maßnahmen zum Schutz vor Sabotageaktionen bietet die Identifikation von kritischen Knotenpunkten eine Möglichkeit, Ressourcen gezielt dort einzusetzen, wo der Schutz der Kabel besonders kritisch ist.

- Der wahrscheinlich größte Zugewinn an Sicherheit ließe sich durch eine verstärkte Diversifizierung von Verbindungen erreichen, und zwar sowohl mit Blick auf Landungspunkte als auch auf Routen. Ein Beispiel hierfür ist das von der EU geförderte EllaLink-Kabel zur Verbindung nach Lateinamerika. In eine ähnliche Richtung gehen die Überlegungen für ein Kabel durch die Arktis nördlich von Kanada, das für Europa eine weitere Verbindung nach Asien schaffen soll.[22] Falls dieses Kabel tatsächlich gebaut wird, würde die deutsche Verbindung von der Ostsee nach Finnland über C-Lion und nach Schweden über Digital E4 erheblich an Bedeutung gewinnen — und sollte dann auch als kritische Infrastruktur eingestuft werden. Die Herausforderung besteht hier darin, die öffentliche Förderung solcher Projekte so zu gestalten, dass sie nicht in zu starkem Maße zu Wettbewerbsverzerrungen führt; so könnten die Regierungen beispielsweise darauf verzichten, spezifische technische Vorgaben zu

22 Achim Sawall, »EU will Seekabel über Arktis nach Asien finanzieren«, *Golem*, 17.10.2022, <https://www.golem.de/news/nordwestpassage-eu-will-seekabel-ueber-arktis-nach-asien-finanzieren-2210-168998.html> (eingesehen am 22.8.2023).

machen, und sich auf die Rolle von »Ankerkunden« beschränken.

- Ebenfalls ausbaufähig ist die technische und politische Resilienz. Dazu gehört der europaweite Informationsaustausch über kritische Vorfälle und deren Ursachen. Vor allem aber kommt es darauf an, die Kapazitäten für die Reparaturen von Kabeln auszubauen.[23] In einem ersten Schritt würde sich dazu eine Art »Stresstest« anbieten, mit dem sich simulieren ließe, welche Kapazitäten bei den Reparaturschiffen für den Fall erforderlich wären, dass mehrere für Europa kritische Kabel gleichzeitig unterbrochen würden. Zu prüfen wäre dabei, ob neben den privaten Anbietern auch die Seestreitkräfte der europäischen Mitgliedstaaten in gewissem Maße entsprechende Kapazitäten vorhalten sollten, im besten Fall abgestimmt auch im Rahmen der Nato.
- Es scheint zudem ratsam, den Schutz vor physischen Angriffen gerade bei jenen Landungspunkten zu erhöhen, die an den Küsten europäischer Staaten liegen und von besonderer Relevanz für Europa sind. Auch wenn sich nicht alle Kabel in ihrer gesamten Länge schützen lassen, würde ein verstärkter Schutz der Landungspunkte sowie der ersten, noch in geringer Tiefe verlaufenden Abschnitte der Kabel deren Sicherheit erhöhen. Verstärkte militärische Patrouillen könnten hier der Aufklärung wie auch der Abschreckung dienen.[24] Möglicherweise ließen sich gerade hier in Zukunft auch Drohnen einsetzen, um die Kabel im nahen Küstenbereich teilautonom zu überwachen.[25] Im Rahmen der Planung dieser militärischen Schutzmaßnahmen wäre zu prüfen, ob die formale Einrichtung von Schutzzonen entlang der küstennahen Kabel, wie sie etwa Australien vorgenommen hat, einen Zugewinn an Sicherheit bieten oder zumindest die Patrouillen erleichtern kann.[26]
- Mit Blick auf die Stabilität des globalen Netzes bietet es sich außerdem an, Kooperationen über die EU hinaus zu intensivieren. Einerseits mit Staaten, in deren Hoheitsgebiet wichtige Chokepoints liegen, also zum Beispiel mit Ägypten oder mit Singapur. Andererseits aber auch mit den Partnern der Entwicklungszusammenarbeit, etwa wenn es um die Anbindung von Ländern geht, die bisher nur unzureichend an das globale Netz der Unterseekabel angeschlossen sind. Ein wichtiges Forum hierfür ist die G7, die sich zuletzt verstärkt mit dem Thema Unterseekabel beschäftigt hat.[27] Regierungen können und sollten zudem aktiv den Austausch mit dem International Cable Protection Committee (ICPC) suchen. Im ICPC haben sich fast alle Betreiber von Unterseekabeln zusammengeschlossen; auch wenn hier keine verbindlichen Regeln vereinbart werden, könnten Regierungen dieses Forum nutzen, um sich im globalen Maßstab mit den Betreibern der Kabel abzustimmen. Nicht zuletzt hat das ICPC seinerseits 2022 den Regierungen vorgeschlagen, Unterseekabel als kritische Infrastrukturen zu verstehen.[28]
- Mittel- und langfristig könnte Deutschland schließlich darauf hinwirken, den Schutz von Unterseekabeln auch völkerrechtlich noch stärker zu flankieren.[29] Das Seerechtsübereinkommen der Vereinten Nationen fordert in Artikel 113 die Unterzeichnerstaaten auf, mittels nationaler Gesetzgebung gezielte Beschädigungen von Kabeln strafrechtlich zu ahnden. Seit Jahren unterstützt Deutschland eine wiederkehrende Resolution in der UN-Generalversammlung mit dem Titel »Oceans and the Law of the Sea« (jüngst beschlos-

23 Christian Bueger/Tobias Liebetrau, »Critical Maritime Infrastructure Protection: What's the Trouble?«, in: *Marine Policy*, 155 (2023), Art. 105772; Bueger/Liebetrau/Franken, *Security Threats to Undersea Communications Cables and Infrastructure* [wie Fn. 15], S. 53f.

24 Zu den rechtlichen Voraussetzungen für den Einsatz der Marine im deutschen Hoheitsgebiet siehe den Beitrag von Göran Swistek, S. 61ff.

25 Achim Sawall, »Autonome Glider der Marine überwachen Seekabel«, *Golem*, 5.12.2022, <https://www.golem.de/news/glasfaser-autonome-glider-der-marine-ueberwachen-seekabel-2212-170261.html> (eingesehen am 22.8.2023). Siehe zu dieser Frage auch den Beitrag von Christian Schaller, S. 14ff.

26 Tara Davenport, »Submarine Communications Cables and Law of the Sea: Problems in Law and Practice«, in: *Ocean Development & International Law*, 43 (2012) 3, S. 201–242 (219).

27 Mayumi Hirosawa/Ryohei Yasoshima, »G-7 to Support Deep-sea Cable Network for Emerging Nations«, in: *Nikkei Asia* (online), 25.4.2023, <https://asia.nikkei.com/Business/Telecommunication/G-7-to-support-deep-sea-cable-network-for-emerging-nations> (eingesehen am 16.8.2023).

28 International Cable Protection Committee (ICPC), *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*, 2022, <https://www.iscpc.org/documents/?id=3733>.

29 Kevin Frazier, »On Protecting the Undersea Cable System«, *Lawfare*, 12.1.2023, <https://www.lawfaremedia.org/article/protecting-undersea-cable-system>.

sen im Januar 2023, A/RES/77/248), in der die kritische Bedeutung der Kabel betont und an die entsprechende Vorgabe aus dem Seerechtsübereinkommen erinnert wird. Nach wie vor haben indes noch immer viele Staaten keine entsprechenden gesetzlichen Vorgaben verabschiedet.[30]

Die meisten der aufgeführten Maßnahmen wären mit zusätzlichen Kosten verbunden. Wie in anderen Bereichen stellt sich auch hier die Frage, wie diese zusätzlichen Kosten als Preis für ein höheres Maß an Sicherheit zu verteilen sind. Zu beachten ist dabei allerdings, dass die meisten Maßnahmen nicht nur für den unwahrscheinlichen Fall eines gezielten, umfassenden Angriffs relevant sind, sondern gleichermaßen dabei helfen würden, besser auf die sehr viel häufiger auftretenden, nicht intentional herbeigeführten Störungen zu reagieren.

30 Davenport, »Submarine Communications Cables and Law of the Sea« [wie Fn. 26], S. 219.

Ansätze zum Schutz maritimer kritischer Infrastrukturen

Göran Swistek

Der Schutz maritimer Infrastrukturen aus militärisch-sicherheitspolitischer Perspektive: Nato und Bundeswehr

In der Folge des Westfälischen Friedens von 1648 entwickelte sich in der westlichen Staatenwelt die Erwartung, dass sich die Kriegführung völkerrechtlich einhegen lasse.[1] Seit Ende des 19. Jahrhunderts und insbesondere nach den zerstörerischen Weltkriegen des 20. Jahrhunderts entstanden völkerrechtliche Regelungen und Verträge, die das heutige humanitäre Völkerrecht (auch als Kriegsvölkerrecht bezeichnet) bilden.[2] In den Konflikten der ersten zwei Jahrzehnte des 21. Jahrhunderts zeigt sich jedoch eine zunehmende Tendenz, die Regeln des Völkerrechts zu umgehen oder gänzlich zu ignorieren. Vor dem Hintergrund sich wieder verschärfender Großmachtrivalitäten nimmt vor allem die Ausübung von Gewalt jenseits des klassischen Krieges in sogenannten Grauzonen oder hybriden Lagen zu.[3]

Dabei rücken auch maritime kritische Infrastrukturen vermehrt in den Fokus. Der Einsatz von Streitkräften zum Schutz dieser Infrastrukturen ist dabei mit zwei Herausforderungen konfrontiert: Zum einen ist zu klären, welchen Beitrag die Streitkräfte in Zuständen leisten können, die zwar nicht als friedlich gelten können, aber noch deutlich von der Schwelle zu einem bewaffneten Konflikt entfernt sind. Zum anderen stellt sich die Frage, welchen Beitrag die Streitkräfte zum Schutz von Infrastrukturen leisten sollen, die zwar auch eine militärische Dimension haben, in erster Linie aber zivilen Zwecken dienen und von privaten Unternehmen gehalten und betrieben werden.[4] Häfen, Seewege und Datenkabel sind dabei nur die offensichtlichen Beispiele für einen solchen »Dual-use«-Charakter.[5]

Die Nato nimmt diese Fragen schon seit einigen Jahren verstärkt in den Blick, zuletzt auch auf Initiative der Bundesregierung. Dabei hält die Debatte über diese Initiative in Deutschland weiter an. Im Zentrum steht eine verfassungsrechtliche wie auch praktisch-operative Diskussion über die Möglichkeiten eines Einsatzes der Streitkräfte mit dem Ziel, maritime Infrastrukturen zu schützen.

Hybride Bedrohungen und maritime kritische Infrastruktur

Bereits seit vielen Jahren hat sich in der sicherheitspolitischen Analyse die Erkenntnis durchgesetzt, dass Sicherheitspolitik sich immer umfassenderen Herausforderungen zu stellen hat. In diesem Zusammenhang sind innere und äußere Sicherheit nicht mehr deutlich voneinander zu trennen. Gleichzeitig kommen Bereiche hinzu, die bislang eher selten aus einem sicherheitspolitischen Blickwinkel betrachtet wurden. In der Debatte über neue sicherheitspolitische Realitäten[6] gelten Energiesicherheit, Klima-

1 Ove Bring, »The Westphalian Peace Tradition in International Law. From *Jus ad Bellum* to *Jus contra Bellum*«, in: *International Law Studies*, 75 (2000) 1, S. 57–80, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1435&context=ils>.

2 Näheres dazu im Beitrag von Christian Schaller in dieser Studie, S. 14ff.

3 James J. Wirtz, »Life in the ›Grey Zone‹: Observations for Contemporary Strategists«, in: *Defence & Security Analysis*, 32 (2017) 2, S. 106–114.

4 Siehe dazu den Ansatz der »integrierten Sicherheit«, der durch die Nationale Sicherheitsstrategie der Bundesregierung eingeführt wurde. Eine Erläuterung zum Begriff erfolgt bereits im Vorwort: Bundesregierung, *Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie*, Berlin, 14.6.2023, S. 6, <https://www.bmvg.de/resource/blob/5636374/38287252c5442b786ac5d0036ebb237b/nationale-sicherheitsstrategie-data.pdf>.

5 Wirtz, »Life in the ›Grey Zone‹« [wie Fn. 3].

6 Der Begriff der neuen sicherheitspolitischen Realitäten im Zusammenhang mit der Analyse der derzeitigen internationalen und sicherheitspolitischen Lage zwischen Groß-

wandel, Migration, Handelsströme und globale Lieferketten sowie Schutz von bzw. Zugang zu Ressourcen als zwingend zu berücksichtigende Aspekte moderner Sicherheitspolitik.

In den letzten Jahren lässt sich parallel eine Zunahme schwer attribuierbarer Aktivitäten beobachten, die teilweise gravierende Sicherheitsimplikationen haben. Dazu zählen unter anderem die Beeinflussung von Stimmungen im Informationsraum,[7] der Einsatz von Drohnen entlang kritischer militärischer und maritimer Infrastruktur,[8] die bewusst gesteuerte Verunsicherung durch Beeinflussung der europäischen Energiesicherheit sowie die Ausführung von Spionage- oder Sabotageaktivitäten, ohne dass diese Maßnahmen eindeutig bestimmten Akteuren oder Staaten zugeordnet werden können.

All diese Aktivitäten lassen sich unter den Begriff der hybriden Kriegführung[9] fassen; gemeint ist damit das gesteuerte Einwirken unterhalb der physischen Gewaltschwelle mit dem Ziel, einen Akteur oder Staat zu schwächen und ihm zu schaden. Dabei bleiben der Auslöser oder Verursacher sowie der konkrete Zweck bewusst im Unklaren.[10] Das psychologische Ziel solcher Aktivitäten ist die Verunsicherung der Bevölkerung, das Erzeugen von Stressoren[11] oder am Ende gar die Destabilisierung westeuropäischer Gesellschaften. Konkrete Beispiele aus den zurückliegenden Jahren sind unter anderem die Zerstörung von Unterwasserkabeln und -sensoren in Norwegen,[12] Drohnenaktivitäten über schwedischen Atomkraftwerken,[13] norwegischen Flughäfen und Offshore-Einrichtungen[14] sowie deutschen Truppenübungsplätzen,[15] außerdem die Zerstörung der Nord-Stream- und BalticConnector-Pipelines und verdächtige Aufklärungsaktivitäten entlang maritimer Infrastruktur.

Im maritimen Umfeld wird eine große Zahl von Infrastrukturen errichtet, von denen moderne Staaten und Gesellschaften abhängig sind.

Diese neue Bedrohungslage betrifft insbesondere den maritimen Raum, der immer intensiver als Ort des Handels, als Kommunikationsweg, als Wirtschaftsraum oder als Ressourcenbasis genutzt wird. Der maritime Raum umfasst zudem riesige Gebiete, die noch nicht vollständig erforscht sind und zum Teil nur schwer zu erforschen sein werden. Gleichzeitig werden die Meeresgebiete zusehends intensiver genutzt, um unsere menschlichen Bedürfnisse zu

machtrivalität und einem Neo-Imperialismus, der Gewalt einsetzt — veranschaulicht durch den russischen Angriffskrieg gegen die gesamte Ukraine seit dem 24. Februar 2022 —, hat sich nicht nur in der Fachdebatte verbreitet, sondern ist auch in Bundestagsdokumenten zu finden. Siehe hierzu u. a. Antrag der Fraktion der CDU/CSU, *Deutschland braucht eine Nationale Sicherheitsstrategie*, Deutscher Bundestag, 28.3.2023 (Drucksache 20/6182), <https://dserver.bundestag.de/btd/20/061/2006182.pdf>.

7 Frank Gardner, »What Is Hybrid Warfare? Inside the Centre Dealing with Modern Threats«, *BBC*, 6.2.2023, <https://www.bbc.com/news/uk-64511670>.

8 Eine kleine Auswahl von Presseberichten dazu: »Sweden Drones: Sightings Reported over Nuclear Plants and Palace«, *BBC*, 18.1.2022, <https://www.bbc.com/news/world-europe-60035446>; Thomas Nilsen, »Norwegian Police Detains Son of Close Putin Ally for Flying Drone at Svalbard«, in: *The Barents Observer*, 19.10.2022, <https://thebarentsobserver.com/en/security/2022/10/russian-dual-citizenship-detained-flying-drone-svalbard>; »Bundeswehr-General Breuer warnt vor mehr Angriffen auf Deutschland: ›Jede Pipeline, jedes Kraftwerk kann attackiert werden‹«, *Business Insider Deutschland*, 10.10.2022, <https://www.businessinsider.de/politik/deutschland/bundeswehr-general-breuer-warnt-vor-mehr-angriffen-auf-deutschland-jede-pipeline-jedes-kraftwerk-kann-attackiert-werden-a/>.

9 Annegret Bendiek/Raphael Bossong, *Hybride Bedrohungen. Vom Strategischen Kompass zur Nationalen Sicherheitsstrategie*, Berlin: Stiftung Wissenschaft und Politik, Juni 2022 (SWP-Aktuell 40/2022), doi: 10.18449/2022A40.

10 Gardner, »What Is Hybrid Warfare?« [wie Fn. 7].

11 Olaf E. Truszczynski/Piotr Pacek, »Hybrid War and Its Psychological Consequences«, in: *Torun International Studies*, 1 (2020) 13, S. 23—30.

12 Siehe u. a. »4.3 Kilometers of Subsea Cable Vanished Off North Norwegian Coast«, *High North News*, 10.11.2021, <https://www.highnorthnews.com/en/43-kilometers-subsea-cable-vanished-north-norwegian-coast>; David Averre, »Undersea Cable Connecting Norway and Arctic Satellite Station Is Mysteriously Damaged«, *Mail online*, 11.1.2022, <https://www.dailymail.co.uk/news/article-10390555/Undersea-cable-connecting-Norway-Arctic-satellite-station-mysteriously-damaged.html>.

13 Siehe u. a. »Sweden Drones: Sightings Reported over Nuclear Plants and Palace« [wie Fn. 8].

14 Siehe u. a. »Fears Grow as More Suspicious Drones Appear above Norway's Offshore Facilities«, *Euronews*, 23.10.2022, <https://www.euronews.com/2022/10/23/fears-grow-as-more-suspicious-drones-appear-above-norways-offshore-facilities>.

15 Siehe u. a. Tim McMillan, »Suspicious Drones Seen over German Military Sites Training Ukrainian Soldiers«, *The DeBrief*, 6.10.2022, <https://thedebrief.org/suspicious-drone-seen-over-german-military-sites-training-ukrainian-soldiers/>.

befriedigen. Dementsprechend wurde und wird im maritimen Umfeld eine große Zahl von Infrastrukturen errichtet, von denen moderne Staaten und Gesellschaften abhängig sind. Diese sind besonders anfällig für Sabotage- und Spionageaktivitäten.

Maritime kritische Infrastruktur und deren Relevanz aus Perspektive der Nato

Bis zum Ende des 20. Jahrhunderts galt aus militärischer Perspektive im engeren Sinne nur jene maritime Infrastruktur als besonders kritisch, die als militärisches Objekt oder Gerät zur militärischen Operationsführung benötigt wurde. Die Zunahme terroristischer Aktivitäten und deren Ausgreifen auch auf den maritimen Raum zu Anfang des 21. Jahrhunderts[16] hat ebenso wie die Ausbreitung der Piraterie an zentralen maritimen Engstellen (Chokepoints) dafür gesorgt, dass maritime Handelswege und Seeverbindungslinien in den Fokus rückten, die vitale Bedeutung für globalisierte Wirtschaftsstandorte haben und deren Sicherheit bedroht ist. Die Anschläge auf den zivilen Seeverkehr im Roten Meer seit dem Spätherbst 2023 hatten einen ähnlichen Effekt.

Bereits in der im Jahr 2011 erlassenen Alliierten Maritimen Strategie der Nato zählten zur bedrohten Infrastruktur im maritimen Raum nicht nur Seewege, sondern auch kritische Energieinfrastruktur sowie Datenkabel.[17] Den Auftrag alliierter Seestreitkräfte sah man zukünftig nicht allein in der Durchführung rein militärischer Operationen, sondern auch in der Unterstützung anderer hoheitlicher Sicherheitsorgane und in der Wahrung von Bestimmungen des internationalen Seerechts, insbesondere des Rechts zur freien Seefahrt, basierend auf Mandaten und Resolutionen der Vereinten Nationen. Praktisch wirksam wurde dieses Auftragsverständnis in mandatierten maritimen Operationen, wie etwa der »Operation Enduring Freedom« am Horn von Afrika zum Schutz originär militärischer Transporte gegen terroristische Anschläge sowie in den Operationen »Active Endeavour« und später »Sea Guardian« im Mittelmeer, die dazu dienten, umfassende Lagebilder zu erstellen und terroristische Versorgung zu unterbinden. Später kamen am Horn von Afrika und im Golf von Guinea auch maritime Operationen der Europäischen Union hinzu, bei denen es um die Bekämpfung von Piraterie und den Schutz von Handelsschiffen ging, insbesondere von Schiffen des Welternährungsprogramms.

Mit Russlands völkerrechtswidriger Annexion der Krim im Jahr 2014 und dem zunehmenden Agieren von Staaten in völkerrechtlichen Grauzonen und unter Nutzung hybrider Mittel wurde auch die schützenswerte kritische Infrastruktur sicherheitspolitisch neu bewertet. Seit etwa 2018 ist das Thema kritische maritime Infrastruktur auch verstärkt in den Fokus der Verteidigungsplanung der Nato gerückt.

Vorrangig wurde zu diesem Zeitpunkt nach wie vor nur jene Infrastruktur als kritisch betrachtet, die unmittelbar für die Wahrnehmung des militärischen Auftrags der Allianz von besonderer Bedeutung war. Dazu zählen Seewege (Sea Lines of Communication, SLOCs), die für die alliierten Truppen- und Logistikbewegung relevant waren; Häfen, die auch als Umschlagplätze für militärische Güter dienen sollten; Datenkabel, bei denen zivile und militärische Nutzung kaum mehr trennscharf zu unterscheiden sind; Funkstationen für die militärische, terrestrische Kommunikation sowie Einrichtungen zur Satellitenkommunikation. Vor allem die Rolle dieser Infrastruktur für Transport, Kommunikation und Logistik machte sie militärisch so relevant.

Diese Infrastrukturen werden auch zivil genutzt und besitzen daher einen »Dual-use«-Charakter. In diesem Zusammenhang ergibt sich daraus auch ein regulatorisches Spannungsfeld zwischen den verschiedenen rechtlichen Regelungen und Verantwortlichkeiten für Hoheitsgewässer, ausschließliche Wirtschaftszonen und Hohe See.[18] In Anwendung von Artikel 3 des Nato-Vertrags[19] belässt die Allianz die Verantwortung für den Schutz kritischer maritimer Infrastruktur innerhalb der Hoheitsgewässer bei den einzelnen Staaten. Dieser Schutz sei eine innerstaatliche Aufgabe sowie gleichzeitig ein zu erbringender Beitrag zur alliierten Sicherheit.

16 Die bekanntesten Beispiele hierfür sind: Anschlag auf die *USS Cole* vor dem Jemen am 12. Oktober 2000: FBI, »USS Cole Bombing«, o.D., <https://www.fbi.gov/history/famous-cases/uss-cole-bombing>, sowie die Vorbereitungen und die Logistik der Anschläge in Mumbai vom 26. bis 29. November 2008: »Mumbai Terror Attacks Fast Facts«, *CNN*, 29.11.2008, <https://edition.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/index.html>.

17 Nato, *Allied Maritime Strategy, Maritime Security*, Brüssel, 18.3.2011, Paragraph 14—15, <https://www.nato.int/cps/en/natohq/official_texts_75615.htm>.

18 Siehe dazu den Beitrag von Christian Schaller in dieser Studie, S. 14ff.

19 *The North Atlantic Treaty*, 4.4.1949, <https://www.nato.int/cps/en/natolive/official_texts_17120.htm>.

Im letzten Jahrzehnt, insbesondere infolge der illegalen Annexion der Krim durch Russland, hat sich in diesem Rahmen der Fokus der Allianz enorm erweitert.[20] Bei einer sich abzeichnenden oder wahrgenommenen Krise können etwa zum Zwecke der Abschreckung durch verstärkte Präsenz bestimmte in Bereitschaft gehaltene Truppen, Schiffe und Flugzeuge kurzfristig im geografischen Verantwortungsbereich der Allianz verlegt werden. Nach Beginn der russischen Aggression gegen die gesamte Ukraine im Februar 2022 hatten die Alliierten ihre Fähigkeiten, Einheiten und Verbände zu Land und zur See im Rahmen der sogenannten »enhanced Vigilance Activities« (eVA) mobilisiert.[21] Im maritimen Verantwortungsraum der Nato ist seit Beginn des Krieges eine intensivere Nutzung von Seeversorgungswegen und Häfen, aber auch von Kommunikationseinrichtungen zu beobachten. Dies bringt auch jenseits eines möglichen Konflikts mit einem Aggressor ein erhöhtes Potential an Gefährdungen für diese Infrastrukturen mit sich. Neben einem direkten konventionellen Angriff auf diese Infrastrukturen sind vor allem hybride Bedrohungen, zum Beispiel Sabotageakte, zur Störung der Truppen- bzw. Aufmarschbewegungen oder Spionageaktivitäten vorstellbar.

Parallel wurde in der Allianz spätestens seit 2019 wahrgenommen, dass Russland seine Forschungen im Unterwasserbereich intensiviert. Innerhalb der Nato analysierte man die Erprobungen und Aktivitäten russischer Drohnen, die oft im Tiefwasserbereich und im Verbund von Forschungs- und Kriegsschiffen stattfanden.[22] Mögliche Sabotageakte an Datenkommunikationsverbindungen wurden in diesem Kontext unter dem Begriff »seabed warfare«[23] ein zusehends intensiver betrachtetes Szenario. Spätestens seit dem Sabotageakt an den Pipelines Nord Stream 1 und 2 im September 2022 erweiterte sich der Fokus der Bedrohungswahrnehmung auf alle maritimen Infrastrukturen. Vermehrt wurden immer häufigere Versuche staatlicher russischer Schiffe[24] beobachtet, maritime Infrastruktur auszuspähen. Vertreter der Nato äußern mittlerweile auch die Vermutung, dass bereits vielfach Zündvorrichtungen an maritimen Infrastrukturen angebracht wurden, um diese bei Bedarf in einer vorausgeplanten Aktion zerstören zu können.[25]

Im Zusammenhang mit der Erarbeitung des neuen Strategischen Konzepts der Nato im Jahr 2022 und der Überarbeitung alliierter Verteidigungsplanung, die durch den russischen Angriffskrieg gegen die Ukraine beschleunigt wurden, ist das Verständnis von kritischer Infrastruktur innerhalb der Allianz noch einmal erweitert worden. Neben den rein militärischen Aspekten, die für den Schutz und die Verteidigung der Allianz von Belang sind, wird auch auf das Potential zur Destabilisierung von Staaten, Gesellschaften und somit auch der Allianz verwiesen, das mit kritischer Infrastruktur verbunden ist.[26] Schon im Vorfeld des Gipfeltreffens in Madrid wurde eine sogenannte »Reflection Group Nato 2030« beauftragt, Vorschläge für die künftige Ausrichtung der Allianz angesichts des veränderten Bedrohungsumfeldes zu erarbeiten. In ihrem Abschlussbericht stellt die Reflection Group fest,[27] dass Infrastruktur als kritisch zu gelten hat, wenn deren Störung oder ein Angriff auf sie einem bewaffneten Angriff entspricht und den Bestand sowie die Stabilität eines einzelnen Mitglieds, dessen Gesellschaft oder der Allianz gefährdet. Dazu zählen unter anderem maritime Infrastruktur, die für die

20 Nato, »Nato Warsaw Summit Communiqué«, Pressemitteilung, Warschau, 9.7.2016, Para. 35 bis 37, <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>.

21 Nähere Erläuterungen dazu auf der Internetseite der Bundeswehr: »Slowakei — eVA«, 2023, <https://www.bundeswehr.de/de/einsaetze-bundeswehr/anerkannte-missionen/slowakei-enhanced-vigilance-activities>.

22 Michael Paul/Göran Swistek, *Russland in der Arktis. Entwicklungspläne, Militärpotential und Konfliktprävention*, Berlin: Stiftung Wissenschaft und Politik, Oktober 2021 (SWP-Studie 19/2021), doi: 10.18449/2021S19v02.

23 Gemeinhin versteht man unter dem Begriff »seabed warfare« einen Teil der Unterwasserseekriegführung, ergänzend zur U-Boot-Seekriegführung und zur Minenkriegführung. Dabei geht es um vorrangig militärische Operationen und Einsatzverfahren, die nahe oder auf dem Meeresboden durchgeführt werden und dabei verschiedene Mittel und Technologien nutzen, um in einem Konflikt einen militärischen Vorteil zu erlangen.

24 Hierzu veröffentlichte ein dänisch geführtes Journalistenteam in Form einer Podcast-Reihe umfangreiche Recherchen: »Cold Front«, Podcast, *Deutschlandradio*, 26.4.2023, <https://www.dr.dk/lyd/p1/cold-front>.

25 Siehe u. a. Moritz Eichhorn, »Verdacht der Nato: Russland vermint Pipelines und Kabel in der Ostsee«, in: *Berliner Zeitung*, 5.5.2023, <https://www.berliner-zeitung.de/politik-gesellschaft/verdacht-der-nato-russland-vermint-pipelines-und-kabel-in-der-ostsee-li.345567>.

26 *NATO 2022 Strategic Concept*, Brüssel, 29.6.2022, Para. 26, <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf>.

27 *NATO 2030: United for a New Era*, 25.11.2020, <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf>.

Energiesicherheit oder die Klimasicherheit relevant sind, aber auch solche im Informations- und Cyberraum sowie die Seewege. Die Vorschläge wurden zu großen Teilen im Strategischen Konzept der Allianz übernommen und konkretisiert. Hybride Aktivitäten in den Sektoren Wirtschaft und Energieversorgung sowie im Informationsraum können nunmehr Auslöser einer Beistandspflicht nach Artikel 5 des Nordatlantikvertrags sein.[28] Dies wurde in der Gipfelerklärung der Staats- und Regierungschefs der Nato im Juli 2023 in Vilnius noch einmal bekräftigt.[29]

Im Strategischen Konzept der Allianz wird zusätzlich ein Zusammenhang zwischen dem Agieren staatlicher Akteure und der langfristigen strategischen Sicherheit der Mitglieder der Allianz durch Beeinflussung von außen herausgestellt. Mit Blick auf China heißt es darin etwa: »Die Volksrepublik China versucht Schlüsseltechnologien sowie bestimmte Industriesektoren, kritische Infrastruktur, strategische Ressourcen und Versorgungswege zu kontrollieren.«[30] Dementsprechend besitzen kritische Infrastrukturen auch eine militärische Relevanz, da sie für die Alliierten von sowohl großer strategischer als auch wirtschaftlicher Bedeutung sind. Häfen, See- und Binnenwasserstraßen sowie Pipelines sind wichtig für den Transport von Gütern, auf die die nationale Wirtschaft angewiesen ist. Dazu zählen unter anderem Rohstoffe, Energieträger, Lebensmittel, aber auch militärisches Material wie Waffen und Munition. Im Falle militärischer Operationen dienen sie aber auch der Versorgung und dem Truppentransport. Der Schutz maritimer kritischer Infrastrukturen ist daher nicht nur ein wichtiger Bestandteil der nationalen Sicherheitsstrategie vieler Länder, sondern auch zentrales Element alliierter Sicherheit und folglich der Verteidigungsplanung der Nato.

Zielgerichtete feindliche Aktivitäten dürften sich zunehmend in den Bereich des Hybriden verlagern.

Vielfach wird angenommen, dass sich zielgerichtete feindliche Aktivitäten zunehmend in den Bereich des Hybriden verlagern. In der Allianz werden infolgedessen auch Seekabel, Offshore-Windparks, Öl- und Gasplattformen, Pipelines sowie Seewege und Häfen zur maritimen kritischen Infrastruktur gezählt. Wo immer diese Infrastruktur vitale gesamtstaatliche und militärische Bedeutung hat, muss ihr Schutz auch durch Streitkräfte gewährleistet werden. Insofern bietet sich eine Qualifizierung als verteidigungsrelevante maritime Infrastruktur an.

Im Strategischen Konzept 2022 wurden die Allianz und ihre Mitglieder aufgefordert, Pläne zur Abschreckung und Verteidigung zu erstellen. Zu den potentiellen Bedrohungen zählen auch Angriffe auf maritime kritische Infrastruktur. Im November 2022 wurde auf gemeinsame norwegische und deutsche Initiative hin die Etablierung eines Nato-Instrumentariums zum Schutz von Unterwasserinfrastruktur angestoßen.[31] Auf ihren Nato-Ratstreffen im Februar 2023 einigten sich die Verteidigungsminister darauf, eine entsprechende Koordinierungszelle einzurichten.[32] Diese ist seither im Nato-Hauptquartier in Brüssel angesiedelt. Sie soll Schwachstellen beim Schutz von Unterwasserinfrastruktur identifizieren, die Zusammenarbeit mit den privatwirtschaftlichen Betreibern erleichtern und generell wesentliche zivile und militärische Akteure zusammenbringen. Daraus ergibt sich ein Akteursdreieck zwischen der Allianz, den nationalen Regierungen und den zivilen Betreibern entsprechender Infrastruktur.

Auf dem Gipfeltreffen der Allianz in Vilnius im Juli 2023 wurde außerdem bekanntgegeben, dass ein maritimes Zentrum für den Schutz kritischer Unterwasserinfrastruktur am maritimen Hauptquartier der Nato in Northwood, UK, eingerichtet werden soll. Dieses Zentrum soll zum einen ein Unterwasserlagebild erstellen und zum anderen als direkte Ansprechstelle ziviler Betreiber fungieren, für den Austausch sicherheitsrelevanter Daten und Informationen. Für die Erstellung eines Unterwasserlagebilds sollen nach Ansicht der Allianz zukünftig Informationen aus verschiedensten Quellen gebündelt werden, seien es Nachrichtendienste, militärische Sensoren (Radar, Sonar, Hdrophone etc.), Satelliten, das Schiffsidentifikationssystem AIS oder die privatwirtschaftlichen Betreiber kritischer Infrastruktur und deren existie-

28 *NATO 2022 Strategic Concept* [wie Fn. 26], Para. 27.

29 »NATO Vilnius Summit Communiqué«, Pressemitteilung, Vilnius, 11.7.2023, <https://www.nato.int/cps/en/natohq/official_texts_217320.htm>.

30 »The PRC seeks to control key technological and industrial sectors, critical infrastructure and strategic material and supply chains.« (zit in ebd., Para. 23; deutsche Übersetzung des Autors).

31 Lisa-Martina Klein, »Wie sich die Nato für Krieg am Meeresgrund rüstet«, *Table Media*, 14.8.2023, <https://table.media/security/analyse/wie-sich-die-nato-fuer-krieg-am-meeresgrund-ruestet/>.

32 Ebd.

rende Sicherheitseinrichtungen oder -unternehmen. Das Augenmerk gilt vor allem der Hohen See sowie den ausschließlichen Wirtschaftszonen, es können — auf freiwilliger Basis — aber auch Daten aus den Territorialgewässern der Alliierten beigesteuert werden. Das zu erstellende Lagebild soll eine umfassende Überwachung kritischer Infrastruktur auf und unter See in Echtzeit ermöglichen und folglich jedwede Anomalie schnell erkennen lassen. Abschreckung durch Attribuierbarkeit, also die Fähigkeit, verdeckte feindliche Aktivitäten eindeutig zuordnen zu können, entfaltet bereits eine abschreckende Wirkung und erhöht dadurch die Sicherheit kritischer Infrastruktur.

Parallel zu den genannten neuen Strukturen hat die Nato weitere Arbeitsprozesse angestoßen. In einem Expertenforum will man mit internationalen Völkerrechtsexperten und den 31 Alliierten das geltende Seevölkerrecht in den Blick nehmen, um zumindest innerhalb der Allianz zu einer einheitlichen Auslegung zu kommen. Gleichzeitig sollen Netzwerke zwischen der Industrie, den Betreibern maritimer Infrastruktur, den jeweiligen Regierungen sowie der Nato und den Militärs aufgebaut werden, um den gemeinsamen Austausch sowie den Informationsfluss zu verbessern.

Militärischer Schutz von ziviler maritimer kritischer Infrastruktur in Deutschland – ein Spannungsfeld

Infolge des Sabotageaktes an den Nord-Stream-Pipelines entstand in der breiteren Öffentlichkeit die Erwartung, dass die Streitkräfte solche kritischen Infrastrukturen schützen sollten. Dabei handelt es sich ganz überwiegend um zivile Einrichtungen, die von privatwirtschaftlichen Unternehmen betrieben werden. Zwar dürften die Fähigkeiten der Streitkräfte für den Schutz von kritischer und insbesondere maritimer kritischer Infrastruktur geeignet sein, doch zählt ihr Schutz in Deutschland nicht zum verfassungsrechtlichen Auftrag der Streitkräfte.[33]

Rechtliche Grenzen eines Einsatzes der Streitkräfte

Die Frage, welche Maßnahmen zur Kontrolle und zum Schutz kritischer Infrastruktur oder zur Eingrenzung destruktiver Aktivitäten gegen diese Struktur geeignet sind, ist im maritimen Umfeld komplex und nicht leicht zu beantworten, sind hier doch zunächst einmal verschiedene Bereiche rechtlicher Vorgaben und Verantwortlichkeiten berührt.[34]

Maritime Infrastruktur, ob physischer oder nichtphysischer Natur, kann sich in den Territorialgewässern, der anschließenden ausschließlichen Wirtschaftszone, auf Hoher See oder über alle diese Räume hinweg befinden. In jedem dieser Räume gilt ein anderes Regelungs- und Verantwortungsregime. Wird eine Infrastruktur privatwirtschaftlich betrieben, liegt die Verantwortung für den Schutz der Objekte gegen natürliche oder kriminelle Gewalten zunächst beim Betreiber. Ginge es aber um maritime *kritische* Infrastruktur, bestünde die Möglichkeit, dass neben dem privaten Eigentümer auch staatliche Hoheitsorgane eine relevante Rolle für den Schutz dieser Infrastruktur spielen. Je nachdem, in welchem maritimen Rechtsraum sich die Infrastruktur konkret befindet, sind Maßnahmen zu deren Schutz aufgrund divergierender Zuständigkeiten von unterschiedlichen Hoheitsorganen zu koordinieren.

In der Überschneidung verschiedenster Regelungs- und Verantwortungsräume und den unterschiedlichen Zuständigkeiten nationaler Dienststellen liegt eine der großen Herausforderungen, die mit der Koordination und dem Einsatz von Kräften zum Schutz maritimer kritischer Infrastruktur verbunden sind. Staatliche sowie nichtstaatliche Akteure können diese komplexe Gemengelage gezielt für schädigende Aktivitäten ausnutzen.

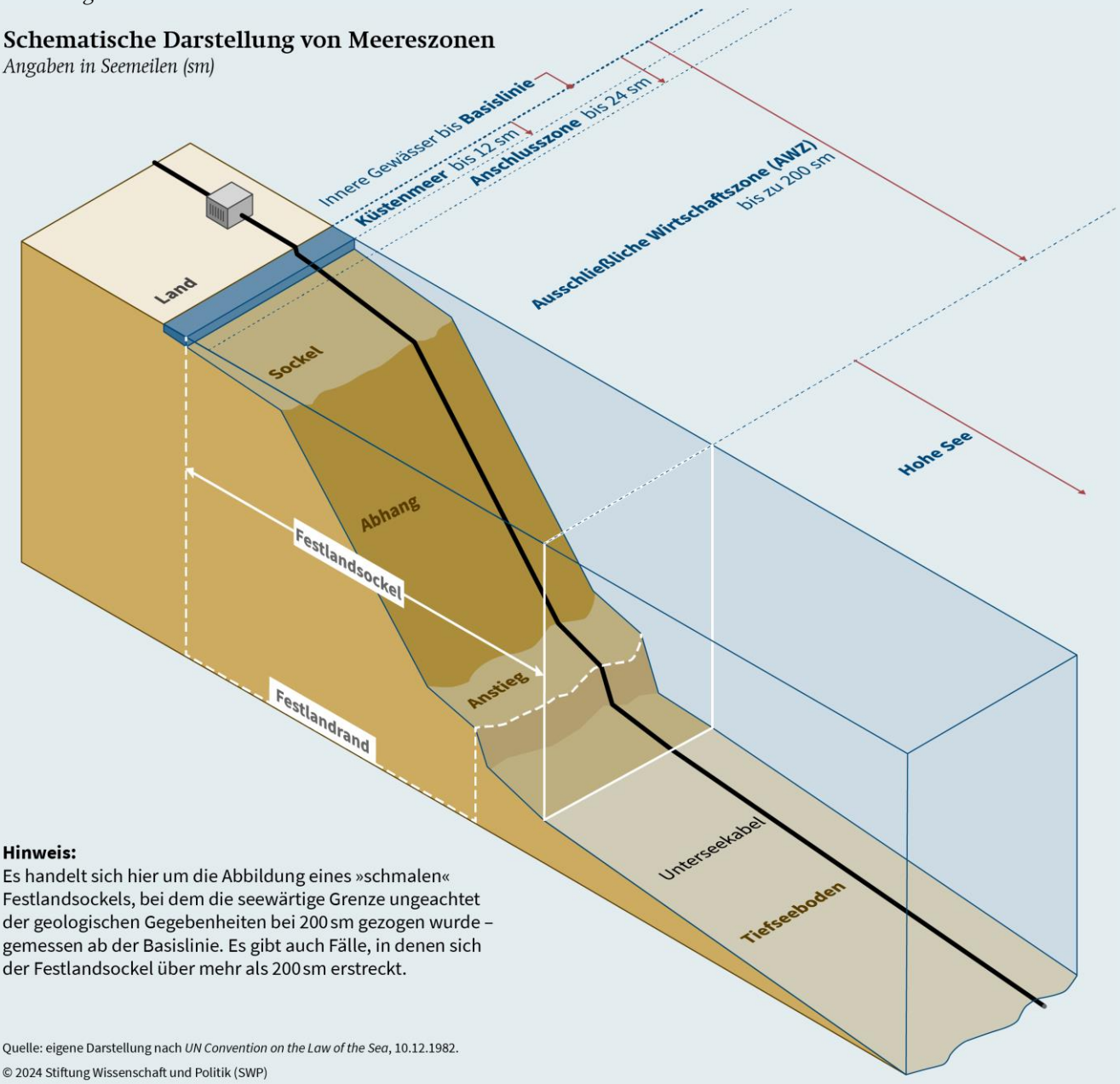
Was nun die Frage nach einem möglichen Schutzauftrag deutscher Hoheitsorgane für maritime kritische Infrastruktur angeht, sind zunächst die gesetzlichen und insbesondere grundgesetzlichen Vorgaben eingehend zu betrachten, die sowohl für den Einsatz der Streitkräfte als auch für den Schutz kritischer Infrastruktur gelten.

33 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Joachim Wundrak, Stefan Keuter, Markus Frohnmaier, weiterer Abgeordneter und der Fraktion der AfD*, Bundestags-Drucksache 20/6304, Berlin, 26.4.2023, <https://dserver.bundestag.de/btd/20/065/2006564.pdf>.

34 Eine detaillierte Auseinandersetzung hierzu findet sich in dem Beitrag von Christian Schaller in dieser Studie, S. 14ff.

Abbildung

Schematische Darstellung von Meereszonen
Angaben in Seemeilen (sm)



Hinweis:
Es handelt sich hier um die Abbildung eines »schmalen« Festlandsockels, bei dem die seewärtige Grenze ungeachtet der geologischen Gegebenheiten bei 200 sm gezogen wurde – gemessen ab der Basislinie. Es gibt auch Fälle, in denen sich der Festlandsockel über mehr als 200 sm erstreckt.

Quelle: eigene Darstellung nach *UN Convention on the Law of the Sea*, 10.12.1982.

Ein ausschlaggebendes Kriterium für die Entscheidung, eine bestimmte Infrastruktur als kritisch und damit als besonders schutzwürdig einzustufen, ist die Gefährdung der öffentlichen Sicherheit in Deutschland. Die öffentliche Sicherheit ist allgemein definiert als die Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen sowie der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger der Hoheitsgewalt.[35] Träger der öffentlichen Sicherheit und als solche verantwortlich für deren Schutz sind nach dem Grundgesetz zunächst die Landespolizeibehörden.[36] Gefährdet eine etwaige Störung, ein Unglücksfall oder eine Naturkatastrophe die öffentliche Sicherheit in einem Gebiet, das über die Grenzen eines einzelnen Bundesstaates hinausgeht, können Bundesbehörden wie die Bundespolizei oder, wenn nötig, auch die Streitkräfte zur Unterstützung anderer Hoheitsorgane eingesetzt wer-

35 Siehe §§ 2 Nr. 2 des Bremischen Polizeigesetzes.

36 Siehe u. a. Art. 35(2) GG.

den.[37] Letzteres erfolgt in Friedenszeiten im Rahmen der sogenannten subsidiären Amtshilfe, nach Antrag der Landes- oder Bundesbehörden an die Streitkräfte.

Eine für den Schutz und die Aufrechterhaltung der öffentlichen Sicherheit geltende Ausnahme ist der Einsatz von Streitkräften im Innern, nachdem das Parlament einen Spannungs- und Verteidigungsfall festgestellt hat. Dabei könnten Streitkräfte auch zum Schutz von Infrastruktur und insbesondere kritischer Infrastruktur eingesetzt werden, sofern die Bundeswehr dies in ihren Planungen zum Kräfte- und Fähigkeitsdispositiv vorgesehen hat.

Da ein direkter, konventionell geführter Angriff eines staatlichen Gegners in der gegenwärtigen Bedrohungslage wohl eher ein extremes, wenig wahrscheinliches, wenn auch nicht gänzlich auszuschließendes[38] Szenario darstellt, dürfte eine solche Feststellung des Spannungs- und Verteidigungsfalls die Ausnahme bleiben. Die derzeit wahrscheinlichste Entwicklung wird absehbar eine Fortsetzung der oben aufgezeigten feindlichen Aktivitäten in der Grauzone und im Hybriden darstellen.

Aus dem rechtlichen Rahmengerüst, das im Friedenszustand gilt, ergibt sich im Falle einer umfassenden Gefährdung somit ein erstes Spannungsfeld: Auf der einen Seite hat der privatwirtschaftliche Eigentümer die grundlegende Verpflichtung, seine maritime kritische Infrastruktur im Rahmen seiner Möglichkeiten zu schützen, auf der anderen soll die öffentliche Sicherheit durch Landes- und Bundesorgane sowie nötigenfalls durch die Streitkräfte und deren partielle Einbindung im Rahmen subsidiärer Amtshilfe aufrechterhalten und geschützt werden.

Praktische Grenzen eines Einsatzes der Streitkräfte

Die subsidiäre Amtshilfe, der Einsatz der Bundeswehr auch im Innern, ist primär für entsprechende Unfalllagen und Naturkatastrophen vorgesehen. Geführt werden die benötigten Kräfte und Fähigkeiten der Bundeswehr in diesem Fall durch das im Oktober 2022 aufgestellte Territoriale Führungskommando in Berlin. Dazu werden Kräfte entsprechend ihrer Verfügbarkeit und Bereitschaft und entsprechend der Lage dem Territorialen Führungskommando unterstellt. Das Spektrum reicht bei Notlagen oder Katastrophen oftmals von Pionier- und medizinischen Kräften bis hin zu speziellen Fähigkeiten zur Bekämpfung biologischer, chemischer oder gar atomarer Bedrohungen. Aber auch Fähigkeiten zur Aufklärung und Lagebilderstellung wurden in der Vergangenheit bereits angefordert und eingesetzt.

Im maritimen Raum könnten Fähigkeiten zur Beseitigung von Gefahr- und Kampfstoffen, Über- und Unterwassersensoren zur Lagebilderstellung, spezielle Drohnen oder Tauchkapazitäten betroffen sein. Fest vorgesehene Kräfte, Einheiten oder Pläne zur Nutzung militärischer Fähigkeiten in solchen Szenarien gibt es bisher nicht. Dazu müssten eigens designierte Kräfte zur Landesverteidigung und zum Einsatz im Innern und demgegenüber solche für den Einsatz außerhalb der Territorialgrenzen im Rahmen der Bündnisverteidigung und Krisenreaktion vorhanden sein. Derzeit würde eine etwaige Nutzung von Kräften der Bundeswehr im Rahmen der Amtshilfe im Innern unter Umständen mit bestehenden Bereitschaften und Verfügbarkeiten kollidieren, die für Aufgaben im Rahmen der Bündnisverteidigung vorgesehen sind, und zwar vor der Feststellung einer Beistandspflicht gemäß Artikel 5 des Nato-Vertrages.

In dem hypothetischen Szenario einer hybrid herbeigeführten großen Unfalllage innerhalb Deutschlands, bei der nur die Streitkräfte die geeigneten Mittel zur Beseitigung besäßen, und einer gleichzeitigen konventionellen Bedrohung eines Alliierten, ergäbe sich ein Zielkonflikt für die in Bereitschaft gehaltenen Kräfte und Fähigkeiten im Rahmen von Nato-Planungen: Die Streitkräfte könnten jedenfalls nicht beide Notlagen gleichzeitig abdecken.

Eine Klärung der Zuständigkeiten staatlicher Sicherheitsorgane durch das KRITIS-Dachgesetz[39] oder auch im Rahmen eines Seesicherheitsgesetzes analog zum Luftsicherheitsgesetz und der daraus resultierenden Konzentration von Ressourcen könnte hier Abhilfe schaffen. Dies ließe sich dann auch in einem interministeriell geführten Operationsplan, dem sogenannten OPLAN Deutschland, zur Landesverteidigung und zum Schutz im Innern mit einer Zuordnung von Kräften fortführen. Darüber hinaus könnte man jene Bereiche in deutschen Hoheitsgewässern, in denen verschiedenste Infrastrukturen gehäuft vorkommen,

37 Siehe Art. 35(3) GG.

38 Siehe hierzu u. a. die Bedrohungsanalyse in *NATO 2022 Strategic Concept* [wie Fn. 26], Para. 6.

39 BMI, *Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen*, Berlin, 25.7.2023, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG.pdf?__blob=publicationFile&v=3j>.

aufgrund ihrer besonders hohen Kritikalität auch als besonders verteidigungsrelevante Infrastruktur qualifizieren. Das würde dabei helfen, vorbezeichnete Fähigkeiten und Kräfte auch der Bundeswehr und der Deutschen Marine bei den Planungen zum Schutz besser zu berücksichtigen und entsprechend notwendige Ressourcen bereitzustellen.[40] Schließlich können gerade in solchen Ballungsräumen maritimer kritischer Infrastruktur gesteuerte Anschläge substantielle und sich kaskadenartig auswirkende Folgen haben.

Die Bedrohung und Gefährdung maritimer kritischer Infrastrukturen wird absehbar Bestandteil von Strategien staatlicher Akteure bleiben.

Praktisch-operativ birgt die Zusammenführung verschiedener technischer Überwachungssensoren der Betreiber mit den Daten und Informationen hoheitlicher Sicherheitsorgane in einem agglomerierten Lagebild das Potential, die derzeitige Situation zu verbessern. Auf dieser Basis könnten Entscheidungen zum Schutz von Infrastruktur schneller und ebenengerechter getroffen werden.

Schlussfolgerungen und Empfehlungen

Die Bedrohung und Gefährdung maritimer kritischer Infrastrukturen wird absehbar Bestandteil von Strategien staatlicher Akteure bleiben, die das Ziel verfolgen, andere Staaten und Gesellschaften zu destabilisieren. Infrastrukturen im maritimen Raum werden an Zahl weiter zunehmen und in bestimmten geografischen Regionen konzentriert auftreten. Aufgrund der Charakteristika maritimer kritischer Infrastruktur ist deren Schutz in Deutschland durch Betreiber und polizeiliche Kräfte kaum zu gewährleisten. Eine Bereitstellung militärischer Kräfte für diese Aufgabe ist nur in den im Grundgesetz genannten Fällen subsidiärer Hilfeleistungen im Sinne einer Amtshilfe zulässig. Da ein solcher Einsatz jedoch weder originär im Fähigkeitsspektrum der Streitkräfte vorgesehen ist noch den Bedarf an eigenen Haushaltsmitteln begründet, verfügen die Streitkräfte derzeit weder über explizite Fähigkeiten noch über vorbestimmte Kräfte zur Sicherung kritischer Infrastruktur, abgesehen von Kräften zum Schutz eigener Liegenschaften oder militärischer Operationsgebiete.

Um die potentiellen Bedrohungen und deren Auswirkungen zu minimieren, bedarf es eines Vorgehens auf unterschiedlichen Ebenen: bei den Betreibern, den Landes- und Bundesbehörden sowie zwischen betroffenen Staaten. Betreiber maritimer Infrastruktur müssen ihre Verantwortung besser wahrnehmen und zugleich den Informationsaustausch mit den Sicherheitsbehörden verbessern. Außerdem müssen sie Sicherheitsmaßnahmen wie Zugangskontrollen, Überwachungs- und Alarmsystemen forciert implementieren. Zugleich sind Schulungen für das Personal der Betreiber erforderlich, um es in die Lage zu versetzen, auf potentielle Bedrohungen zu achten und angemessen zu reagieren.

Auf nationalstaatlicher Ebene sollten alle am Schutz von Infrastrukturen beteiligten Akteure zusammen mit den privatwirtschaftlichen Betreibern eine umfassende Risikoanalyse und -bewertung erarbeiten. Ziel sollte es sein, die signifikanten Bedrohungen zu identifizieren und entsprechende präventive Maßnahmen zu entwickeln. Sowohl für die Prävention etwaiger Vorfälle wie auch für die Reaktion darauf bedarf es einer verbesserten Zusammenarbeit von Regierungs- und Strafverfolgungsbehörden sowie anderen relevanten Organen.

Ein wichtiger Aspekt des Schutzes maritimer kritischer Infrastrukturen ist außerdem die internationale Zusammenarbeit und Koordination. Denn viele Infrastrukturen sind über die verschiedenen maritimen Zonen hinweg international vernetzt, Bedrohungen können zumal grenzüberschreitend sein. Obwohl die Sabotageakte gegen die Pipelines Nord Stream 1 und 2 die Bedeutung und Verwundbarkeit der Meeresgebiete und der darin befindlichen kritischen Infrastrukturen deutlich aufgezeigt haben, haben die Partner und Verbündeten im Ostseeraum sie bisher nur in begrenztem Maße zum Anlass für eine engere Zusammenarbeit genommen.

Aufgrund der Beschlüsse der Nato beim Gipfel in Madrid im Juni 2022 und der Implementierung des regional ausgerichteten New Force Models (NFM) der Allianz ist es für Deutschland zwingend notwendig geworden, nach Jahrzehnten wieder eine eigene Verteidigungsplanung aufzustellen. Diese muss die Fähigkeiten, Kräfte und Maßnahmen im Falle der Landes- und der Bündnisverteidigung im Frieden sowie in sich entwickelnden Krisen und Kriegen aufzeigen. Einzubeziehen als Mindestansatz ist auch der Schutz identifizierter alliierter kritischer Infrastruk-

40 Vgl. hierzu auch die Ausführungen im Schlusskapitel dieser Studie, S. 79ff.

tur — von Seewegen und Häfen über Datenkabel und Pipelines bis hin zu Offshore-Installationen innerhalb des eigenen Hoheitsgebietes und in der ausschließlichen Wirtschaftszone. Darüber hinaus muss in einem umfassenderen Ansatz der Beitrag zum Schutz kritischer Infrastruktur auf Hoher See — vorzugsweise in einem bi- bis multilateralen Vorgehen oder zur Unterstützung einzelner Alliierter innerhalb der Territorialgewässer — in die Gesamtplanung aufgenommen werden. Im Herbst 2022 hat die Deutsche Marine bereits einen Alliierten beim Schutz maritimer kritischer Infrastruktur unterstützt, indem drei deutsche Fregatten mit Fähigkeiten zur Über- und Unterwasserlagebilderstellung in Norwegen eingesetzt wurden, vor allem entlang der Gas- und Ölplattformen.

Zur Abschreckung könnten die Streitkräfte zukünftig in verstärkten Präsenzoperationen eingesetzt werden.

Zur Abschreckung ließen sich die Streitkräfte zukünftig in verstärkten Präsenzoperationen einsetzen. Über das Jahr synchronisierte Fahrten alliierter Kriegsschiffe und Übungen in der Umgebung besonders kritischer Infrastruktur hätten nicht nur abschreckende Wirkung, sie würden auch das ständige Lagebild verbessern. Dies wäre sowohl als Maßnahme der EU wie auch der Nato vorstellbar. Ein besonderer Fokus sollte dabei auf Ballungsräume maritimer Infrastruktur gelegt werden, insbesondere auf jene, die als verteidigungsrelevant gelten. Die zunehmend regionale Organisation von Abschreckungs- und Verteidigungsmaßnahmen der Allianz, insbesondere durch die Bestimmung von Kräften und Fähigkeiten mit unterschiedlicher Bereitschaft im Rahmen des NFM, erlaubt es, solche geografischen Schwerpunkte zu setzen.[41] Auf dem Gipfeltreffen in Vilnius 2023 haben die Staats- und Regierungschefs der Nato-Mitgliedstaaten die regionalen Verteidigungspläne bestätigt,[42] die ihre zahlenmäßigen Kräfte und Fähigkeiten aus dem NFM ziehen. Diese scheinen eine ideale Voraussetzung dafür zu sein, regionale Sicherheitsstrukturen und Verfahren auch mit Blick auf die Überwachung bestimmter relevanter kritischer Infrastruktur zu etablieren.

Schließlich ist vorstellbar, dass einzelne Mitgliedsnationen sogar bi- oder minilaterale Strukturen jenseits der Allianz ausbilden, die Aufgaben wie Präsenz, Abschreckung und Schutz maritimer kritischer Infrastruktur übernehmen. Der dänisch-deutsche Aktionsplan[43] vom August 2022 bietet hierfür eine gute Grundlage. Zwischen Anrainern einer bestimmten Region mit sicherheitsrelevanten Infrastrukturen könnten beispielsweise in einem rotierenden System sogenannte Bereitschaftsschiffe zum Einsatz kommen, die über einen festgelegten Zeitraum für die beteiligten Staaten Präsenz- und Schutzaufgaben wahrnehmen. Im Interesse des Schutzes maritimer Infrastruktur und somit auch maritimer Sicherheit sollte ferner ein verbessertes maritimes Lagebild angestrebt werden, das aus komplementären Sensoren besteht, unter anderem aus akustischen Unterwassersensoren, Satellitenbildern, elektrooptischen sowie elektromagnetischen Sensoren.

41 Claudia Major/Göran Swistek, *Die Nato nach dem Gipfel von Madrid. Norderweiterung, neues Strategisches Konzept und militärische Neuaufstellung*, Berlin: Stiftung Wissenschaft und Politik, Juli 2022 (SWP-Aktuell 49/2022), doi: 10.18449/2022A49.

42 »NATO Vilnius Summit Communiqué« [wie Fn. 29].

43 *Gemeinsamer Aktionsplan für die künftige deutsch-dänische Zusammenarbeit*, 26.8.2022, <https://www.auswaertiges-amt.de/de/newsroom/deutsch-daenischer-aktionsplan/2548528>.

Raphael Bossong

Vorhaben und Mehrwert der EU zum Schutz kritischer maritimer Infrastrukturen

Grundsätzliche Bedeutung und aktuelle EU-Pläne

Der Schutz maritimer kritischer Infrastrukturen hat eine besonders ausgeprägte transnationale und europäische Komponente. Deutschland hat im Vergleich zu anderen großen europäischen Staaten wie Frankreich oder Spanien eine kürzere Küstenlinie, ist aber im Binnenmarkt tief integriert und auf stabile wie weitläufige Versorgungswege angewiesen. Auf den gesamten EU-Binnenmarkt bezogen, verlaufen knapp unter 50 Prozent des innereuropäischen Handels und 75 Prozent des Handels mit außereuropäischen Partnern über maritime Verkehrswege.[1] Insbesondere Ein- und Ausfuhr von Nahrungsmitteln werden primär über Seewege abgewickelt.[2] Der maritime Raum ist außerdem für die Energieversorgung (fossil wie regenerativ)[3] und für die globale Internet-Infrastruktur[4] entscheidend. Ein europäischer Rahmen für den Schutz maritimer Infrastrukturen ist somit im zentralen Interesse Deutschlands, wenn es darum geht, grenzüberschreitende Versorgungs- und Wertschöpfungsketten abzusichern und die nationalen Vorsorgemaßnahmen auszubauen.

Angesichts der besonders schwerwiegenden Anschläge auf die Nord-Stream-Pipelines[5] bleibt es prioritär, den Ausbau militärischer Fähigkeiten zur Seeraumüberwachung voranzutreiben.[6] Die Nato beschäftigt sich bereits seit über zehn Jahren mit der Thematik wachsender feindlicher Aktivitäten, die sich gegen maritime Infrastrukturen richten.[7] Im Jahr 2021 wurde mit Blick auf die Verwundbarkeit von Unterseekabeln die militärische Bedrohungslage neu gewichtet.[8] Für die sichere Versorgung Deutschlands mit Erdgas über die Nordsee ist es von besonderer Bedeutung, dass Norwegen und Großbritannien im Rahmen der Nato eng eingebunden sind. Die Erweiterung der Nordatlantischen Allianz um Finnland und demnächst Schweden unterstreicht die zentrale Rolle des Bündnisses in der Ostsee. Die Nato gründete zusammen mit der EU im Frühjahr 2023 eine gemeinsame Task Force zum Schutz kritischer Infrastrukturen, die bislang aber keine greifbaren Ergebnisse vorgelegt hat.[9]

1 Eurostat, *International Trade in Goods by Mode of Transport*, Dezember 2022, <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_goods_by_mode_of_transport> (eingesehen am 20.7.2023).

2 Vgl. den Beitrag von Bettina Rudloff in dieser Studie, S. 37ff.

3 Vgl. den Beitrag von Jacopo Maria Pepe in dieser Studie, S. 27ff.

4 Vgl. den Beitrag von Daniel Voelsen in dieser Studie, S. 48ff.

5 Eine offizielle Stellungnahme zu Hergang und Verursacher steht aus, trotz weitreichender öffentlicher Diskussionen und Mutmaßungen, vgl. Liliana Botnariuc u. a., »Investigating the Nord Stream Attack. All the Evidence Points to Kyiv«, in: *Der Spiegel* (online), 26.8.2023, <https://www.spiegel.de/international/investigating-the-attack-on-nord-stream-all-the-clues-point-toward-kyiv-a-124838c7-992a-4d0e-9894-942d4a665778> (eingesehen am 1.9.2023).

6 Vgl. den Beitrag von Göran Swistek in dieser Studie, S. 61ff.

7 Nato, *Alliance Maritime Strategy*, Brüssel, 18.3.2011, <https://www.nato.int/cps/en/natohq/official_texts_75615.htm> (eingesehen am 20.7.2023); Nato, *NATO's Maritime Activities*, Brüssel, 20.7.2023, <https://www.nato.int/cps/en/natohq/topics_70759.htm> (eingesehen am 20.7.2023).

8 Nato, »Brussels Summit Communiqué«, Pressemitteilung, Brüssel, 14.6.2021, <https://www.nato.int/cps/en/natohq/news_185000.htm> (eingesehen am 20.7.2023).

9 Nato, *NATO and European Union Launch Task Force on Resilience of Critical Infrastructure*, Brüssel, 16.3.2023, <https://www.nato.int/cps/en/natolive/news_212874.htm> (eingesehen am 20.7.2023). Ein erster gemeinsamer Bericht liegt seit Juni vor, genaue operative Maßnahmen und eine klare Arbeitsteilung zwischen der EU und Nato finden sich darin jedoch nicht, vgl. European Commission, *EU-NATO Task Force on the Resilience of Critical Infrastructure Final Assessment Report*, Brüssel, Juni 2023, <https://commission.europa.eu/system/files/2023-06/EU-NATO_Final Assessment Report Digital.pdf> (eingesehen am 20.7.2023).

Vor diesem Hintergrund konzentriert sich der vorliegende Beitrag vorrangig auf die zivile Dimension des Schutzes kritischer maritimer Infrastrukturen und auf die diesbezügliche Rolle der EU. Unter dem Eindruck des Anschlags auf die Nord-Stream-Pipelines einigte sich der Rat der Union auf eine Empfehlung, laufende Maßnahmen zum Schutz kritischer Infrastrukturen auszubauen und zu beschleunigen.[10] Dazu gehören etwa die Umsetzung neuer europäischer Rechtsakte, mit denen die Resilienz (einschließlich der im Cyberraum) gestärkt werden soll, neue Risikobewertungen und »Stresstests« kritischer Infrastrukturen auf nationaler Ebene sowie ein intensivierter und vertraulicher europäischer Informationsaustausch zu diesen Punkten. Zusätzlich will die EU eine Blaupause für eine koordinierte europäische Reaktion auf schwerwiegende Störungen kritischer Infrastrukturen erarbeiten.[11]

Insbesondere wurden eine neue Mitteilung samt Aktionsplan zur Maritimen Sicherheitsstrategie der EU von 2014 vorgestellt.[12] Ergänzend zur europäischen Präsenz in Küstengewässern und strategisch wichtigen Seegebieten, bei der auch die militärische Zusammenarbeit im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) eine Rolle spielt, soll ein Akzent auf den zivilen Schutz maritimer Infrastrukturen gelegt werden. Vorgesehen sind unter anderem Maßnahmen wie der Ausbau europäischer Fähigkeiten zur »maritimen Raumüberwachung« *(maritime domain awareness)*, Übungen zur Abwehr hybrider Bedrohungen (einschließlich Cyberangriffen) und eine verbesserte Risikokartierung.[13]

Angesichts der vielfältigen Ankündigungen gilt es systematisch zu erfassen, welche wesentlichen Beiträge die EU tatsächlich leisten kann. Die Komplexität des Themenfelds verlangt nach einer differenzierten Betrachtung.[14] Für die EU, die in verschiedenen wirtschaftlichen Sektoren und sicherheitspolitischen Fragen über jeweils unterschiedliche Kompetenzen und Handlungsressourcen verfügt, sollten drei Arbeitsfelder unterschieden werden:

- Erstens kann die EU durch Rechtssetzung für kritische Infrastrukturen bzw. durch regulative Auflagen für deren Betreiber strukturelle Schwachstellen identifizieren und Marktverzerrungen im Binnenmarkt reduzieren. Dabei sind in jüngerer Zeit vor allem drei Rechtsakte mit übergreifender Bedeutung zu beachten: die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, die Richtlinie über die Resilienz kritischer Einrichtungen und die Investitionsschutzverordnung.
- Zweitens verfügt die EU über diverse Mechanismen und EU-Agenturen, die einen operativen Beitrag zum Krisenmanagement leisten könnten. In Reaktion auf schwerwiegende Vorfälle und Anschläge kann die EU den gemeinsamen Katastrophenschutzmechanismus aktivieren. Im Bereich der Vorsorge sind die maritime Raumüberwachung und der Informationsaustausch über EU-Agenturen wie etwa die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) von Relevanz.
- Drittens könnte die EU mittels eigener finanzieller Investitionen in kritische Infrastrukturen mögliche Schwachstellen oder Abhängigkeiten von Drittstaaten verringern. Für den maritimen Bereich könnte insbesondere die EU-Initiative Global Gateway, das europäische Förderprogramm für Infrastrukturausbau in Drittstaaten, in Betracht gezogen werden; allerdings sollten Investitionsentscheidungen dann überlegter und strategischer erfolgen, als dies bisher der Fall ist.

10 Council of the European Union, *Council Recommendation of 8 December 2022 on a Union-wide Coordinated Approach to Strengthen the Resilience of Critical Infrastructure (Text with EEA Relevance)*, 2023/C 20/0, Brüssel, 20.1.2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023H0120(01)> (eingesehen am 20.7.2023).

11 European Commission, *Proposal for a Council Recommendation on a Blueprint to Coordinate a Union-level Response to Disruptions of Critical Infrastructure with Significant Cross-border Relevance,* Brüssel, 6.9.2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0526> (eingesehen am 22.12.2023).

12 European Commission, *Joint Communication on the Update of the EU Maritime Security Strategy and Its Action Plan: An Enhanced EU Maritime Security Strategy for Evolving Maritime Threats*, Brüssel, 10.3.2023, <https://oceans-and-fisheries.ec.europa.eu/publications/joint-communication-update-eu-maritime-security-strategy-and-its-action-plan-enhanced-eu-maritime_en> (eingesehen am 20.7.2023).

13 European Commission, *Annex to the Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strategy and Its Action Plan ›An Enhanced EU Maritime Security Strategy for Evolving Maritime Threats‹*, Brüssel, 10.3.2023, vgl. S. 9 (Punkt 3.1) und S. 12 (Punkt 4.2), <https://oceans-and-fisheries.ec.europa.eu/system/files/2023-03/join-2023-8-annex_en.pdf> (eingesehen am 20.7.2023).

14 Vgl. die Einleitung dieser Studie von Daniel Voelsen und Göran Swistek, S. 7ff.

EU-Regulierung für kritische Infrastrukturen und deren maritimer Bezug

Ende 2022 konnten die Novellierungen der EU-Richtlinien für den Schutz kritischer Infrastrukturen (CER-Richtlinie, EU 2022/2557) und für kritische Informationsinfrastrukturen (NIS-2-Richtlinie, EU 2022/2555) abgeschlossen werden. Diese Novellierungen basieren auf langjährigen Diskussionen über die Umsetzung des geltenden EU-Rechts, wurden seit Beginn der aktuellen EU-Legislaturperiode (2019) angestrebt und konnten in Reaktion auf den Nord-Stream-Anschlag beschleunigt werden. Beide Richtlinien müssen bis 2024 in nationales Recht überführt und umgesetzt werden. Vorrangig sind hierbei die Erweiterung des Anwendungsbereichs auf elf wirtschaftliche Sektoren, die Absenkung von Schwellenwerten für relevante Infrastrukturbetreiber und grenzüberschreitende europäische Infrastrukturen, außerdem inhaltlich erweiterte Sicherheitsauflagen und eine umfassende Betrachtung der »cyber-physikalischen« Komponenten oder Abhängigkeiten. Mitgliedstaaten müssen nun innerhalb von drei Jahren eine nationale Resilienzstrategie erstellen, während die EU-Ebene eine neue Critical Entities Resilience Group (CERG) einrichtet, um die zwischenstaatliche Sicherheitskooperation verbindlicher zu gestalten.

In Deutschland wird die Erwartung geäußert, dass damit ein breiterer Impuls für nationale Reformen einhergehen sollte. Bisher verfügt Deutschland über kein einheitliches Bundesgesetz zum Schutz kritischer Infrastrukturen. Die Umsetzung der CER-Richtlinie soll zum Anlass dienen, im Jahr 2024 ein KRITIS-Dachgesetz zu verabschieden; ein Referentenentwurf zu diesem Gesetz, der im Juli 2023 vorgelegt wurde, sieht insbesondere eine Bedrohungslagenanalyse und eine Erhöhung des Schutzniveaus vor.[15] Die weiteren Auflagen der NIS-2-Richtlinie sollen im deutschen IT-Sicherheitsgesetz aufgenommen werden. Insgesamt müssen deutlich mehr Akteure eingebunden werden, da nun kleinere Betriebe ab 50 Mitarbeitern und einem Jahresumsatz von 10 Millionen Euro als kritische Infrastrukturen oder Dienstleister gelten können.[16]

Der Schwerpunkt der rechtlichen Novellierungen liegt nicht im maritimen Bereich. In der EU-Richtlinie von 2008 sind Verkehrs- und Energiesektor bereits erfasst worden.

Der Schwerpunkt dieser rechtlichen Novellierungen liegt aber nicht im maritimen Bereich, da der Verkehrs- und der Energiesektor bereits in der ursprünglichen EU-Richtlinie aus dem Jahr 2008 erfasst wurden. Häfen, Schiffsverkehr, Passagier- und Frachtbeförderungsunternehmen sowie Betreiber von Schiffsverkehrsdiensten, Erdöl- und Erdgasleitungen sowie Fernleitungsnetzbetreiber können also schon seit längerem in einem europäischen Rahmen als kritische Infrastrukturen deklariert werden. Die jeweiligen nationalen Einstufungen sowie Mitteilungen zu Infrastrukturen mit besonderer europäischer grenzüberschreitender Bedeutung sind vertraulich. Der langjährige Diskussionsprozess zur Novellierung zeigt jedoch, dass vorhandene Risikokartierungen Lücken aufweisen. Deshalb sind auch die bestehenden Einstufungen von kritischen Infrastrukturen im Energie- und Verkehrssektor zu überprüfen.

Unterseekabel als kritische Infrastrukturen finden allerdings auch nach der Novellierung EU-rechtlich keine angemessene Berücksichtigung. Die ursprüngliche NIS-Richtlinie von 2016 »über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen«[17] konnte je nach Auslegung des Begriffs »Netzsystem« solche Kabel zwar umfassen. Diese wurden jedoch etwa im Gegensatz zu Internetknotenpunkten nicht explizit benannt. Auch wenn in den Verhandlungen zur Neufassung ein deutlich geschärftes Bewusstsein für die Verwundbarkeit von Unterseekabeln zum Ausdruck kam, findet sich in der novellierten NIS-2-Richtlinie nur ein kleiner Verweis auf Unterseekabel.

15 Bundesministerium des Innern und für Heimat, *Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen*, Berlin, 25.7.2023, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG.pdf?__blob=publicationFile&v=3j> (eingesehen am 19.12.2023).

16 Rund 73.000 Unternehmen in Deutschland haben zwischen 50 und 250 Mitarbeiter. Statista, *Unternehmen in Deutschland: Anzahl der rechtlichen Einheiten in Deutschland nach Beschäftigtengrößenklassen im Jahr 2021*, 28.2.2023, <https://de.statista.com/statistik/daten/studie/1929/umfrage/unternehmen-nach-beschaeftigtengroessenklassen/> (eingesehen am 21.7.2023). Eine genauere Aufschlüsselung für den Bereich maritimer Infrastrukturen ist nicht verfügbar.

17 Europäisches Parlament/Rat der Europäischen Union, *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*, Brüssel, 19.7.2016, vgl. Annex, <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L1148&from=EN> (eingesehen am 21.7.2023).

Danach sollen diese in der Neufassung nationaler Cybersicherheitsstrategien[18] und in der Meldung von Cybersicherheitsvorfällen an die EU stärker berücksichtigt werden. Ansonsten bleibt es bei allgemeinen Begriffen von elektronischen Kommunikationsnetzwerken bzw. einem Querverweis auf die EU-Richtlinie 2018/1972,[19] die einen allgemeinen Rahmen unter anderem für Glasfaserkabel aufspannt, dabei aber nicht auf die zentrale Bedeutung und die Verwundbarkeit von Unterseekabeln eingeht.[20]

Die Ratsempfehlungen von Ende 2022 zum verbesserten Schutz kritischer Infrastrukturen enthalten demgegenüber einen Arbeitsauftrag zur Überprüfung der Sicherheit von Unterseekabeln.[21] Ob dies wirklich effektiv durch die EU verfolgt werden kann, ist zweifelhaft. Mit Blick auf militärische Bedrohungen und die mögliche nachrichtendienstliche Bedeutung von Unterseekabeln bleiben die Nato und bilaterale Formate vorrangig.

Investitionsschutz und kritische Infrastrukturen

Die EU-Investment-Screening-Verordnung 2019/452, die seit Oktober 2020 gilt, zielt darauf ab, die Zusammenarbeit zwischen den Mitgliedstaaten und der Europäischen Kommission bei der Prüfung ausländischer Direktinvestitionen zu vertiefen. Mitgliedstaaten müssen die europäische Ebene notifizieren, wenn nationale Verfahren zur Genehmigung sensibler Investitionen durchgeführt werden. Allerdings sind mögliche Stellungnahmen der Europäischen Kommission zu einem Investitionsvorhaben von gemeinsamem europäischem Interesse für nationale Entscheidungen weiterhin nicht verbindlich.

Im maritimen Bereich haben vor allem Investitionen aus China in europäische Häfen Bedenken hervorgerufen.

Im maritimen Bereich haben vor allem Investitionen aus China in europäische Häfen Bedenken geweckt. Der zentrale Referenzpunkt ist der Erwerb des Hafens von Piräus durch China im Jahr 2008. Damals wurde im Schatten der Finanzkrise der Verkauf noch begrüßt. Seit Mitte der 2010er Jahre hat sich die Wahrnehmung jedoch verändert. Die globalen Investitionen Chinas im Rahmen der sogenannten Belt-and-Road-Initiative werden häufig als scharfe Konkurrenz zu europäischen Wirtschaftsinteressen verstanden. Der Hafen von Piräus selbst wurde mehrfach ausgebaut, galt zeitweise als der weltweit am schnellsten wachsende Containerhafen und stellt einen starken Wettbewerber zu anderen europäischen Seehäfen dar.[22] 2022 verweigerte ein griechisches Gericht allerdings einen weiteren Ausbau von Piräus mit Verweis auf fehlende Umweltprüfungen.[23] Vor diesem Hintergrund löste die Zustimmung der Bundesregierung zum Verkauf eines Anteils am Hamburger Hafen an das chinesische Unternehmen COCSO scharfe Kritik aus.[24] Der Abschluss des Geschäfts stand zeitweise infrage, da der Hamburger Terminal nach dem Auf-

18 Europäisches Parlament/Rat der Europäischen Union, *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union*, Brüssel, 27.12.2022, vgl. Präambel 97 und Art. 7, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.DEU&toc=OJ%3AL%3A2022%3A333%3ATOC> (eingesehen am 20.12.2023).

19 Europäisches Parlament/Rat der Europäischen Union, *Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung)*, Brüssel, 17.12.2018, Art. 2, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L1972> (eingesehen 21.7.2023).

20 Vgl. den Beitrag von Daniel Voelsen in dieser Studie, S. 48ff.

21 Council of the European Union, *Council Recommendation of 8 December 2022* [wie Fn. 10].

22 Andere Länder ließen in den 2010er Jahren punktuell auch chinesische Hafenbeteiligungen zu, siehe European Parliamentary Research Service, *Chinese Strategic Interests in European Ports*, 28.2.1023, <https://epthinktank.eu/2023/02/28/chinese-strategic-interests-in-european-ports/> (eingesehen am 21.7.2023).

23 Eleni Stamatoukou, »Greek Court Blocks Expansion of Major Port under Chinese Deal«, in: *BalkanInsight* (Athen), 15.3.2022, <https://balkaninsight.com/2022/03/15/greek-highest-administrative-court-blocked-coscos-master-plans-of-investments-in-piraeus/> (eingesehen am 21.7.2023).

24 Nadia Clark, »EU Outrage Clouds Hamburg Port Deal«, *Council on Foreign Relations*, 2.12.2022, <https://www.cfr.org/blog/eu-outrage-clouds-hamburg-port-deal> (eingesehen am 21.7.2023). Andere chinesische Investitionen in Hochtechnologiefirmen wie den deutschen Chiphersteller Elmos hat die Bundesregierung jedoch abgelehnt. Bundesregierung, »Erwerb von Chipfabrik Elmos durch chinesischen Investor untersagt«, Berlin, 9.11.2022, <https://www.bundesregierung.de/breg-de/suche/investitionspruefung-elmos-2141794> (eingesehen am 21.7.2023).

flammen der Kritik neu überprüft und anschließend als kritische Infrastruktur definiert wurde. Deshalb musste eine erneute Investitionsschutzprüfung durchgeführt werden.[25] Die Bundesregierung bekräftigte letztlich die Entscheidung, einen Anteil des Terminals unterhalb einer Beteiligungsschwelle von 25 Prozent zu erlauben. Angesichts dieser Entwicklungen wurde nun auch bereits der Prozess der Überarbeitung der Nationalen Hafenstrategie von 2015 in Gang gesetzt, der eigentlich erst 2025 eingeleitet werden sollte. Dabei stehen gemäß der bisherigen offiziellen Kommunikation vorrangig wirtschaftspolitische und technologische Erwägungen im Vordergrund.[26] Insgesamt kann die Debatte über den Hamburger Hafen als Beleg dafür gelten, dass der EU-Rahmen noch nicht ausreicht, um eine gemeinsame europäische Perspektive zu Investitionen in kritischen Infrastrukturen zu schaffen. Zusätzlich zu Häfen gilt es im maritimen Bereich auf Eigentümerstrukturen bei Unterseekabeln und Energienetzwerken zu achten.

Operative Fähigkeiten – Krisenreaktion und Lagebild

Im Jahr 2006 wurden der europäische Katastrophenschutzmechanismus und angebundene Satellitensysteme im kleinen Maßstab eingesetzt, um die ökologischen Folgen eines israelischen Bombenangriffs an der libanesischen Mittelmeerküste einzudämmen.[27] Seither wurde der Mechanismus aber primär an Land genutzt — sowohl innerhalb der EU als auch in Drittstaaten. Im Zentrum standen dabei insbesondere die Bekämpfung von Waldbränden, die Reaktion auf Erdbeben und zuletzt die Unterstützung bei der Pandemiebekämpfung und bei der Bewältigung von großen Flüchtlingsströmen wie nach der Öffnung der türkischen Grenze zu Griechenland im März 2020.[28]

Grundsätzlich ist es denkbar, diesen Mechanismus, wie von der EU-Kommission nach dem Nord-Stream-Anschlag vorgeschlagen,[29] für die zivile Krisenreaktion auf Vorfälle zu nutzen, die kritische Infrastrukturen betreffen. Das Zentrum für die Koordination von Notfallmaßnahmen (ERCC) und das europäische Satellitenüberwachungssystem Copernicus bzw. die Fähigkeiten des Europäischen Satellitenzentrums (SatCen) könnten beispielsweise zur Lagebewertung einbezogen werden. Die rechtlich begrenzte Möglichkeit, militärische Reaktionsfähigkeiten[30] bei privatwirtschaftlichen Einrichtungen einzusetzen, kann als weiteres Argument für eine entsprechende Rolle der EU angeführt werden. Allerdings verfügt der EU-Katastrophenschutzmechanismus auch nach seiner letzten Aufwertung im Jahr 2019 über keine eigenständigen Einsatzfähigkeiten im maritimen Raum. Die damals geschaffene sogenannte rescEU-Reserve umfasst eine Flotte von Löschflugzeugen und -hubschraubern, medizinische Evakuierungsflugzeuge, Notfallmedizinteams, Ausrüstung zum Umgang mit ABC-Gefahren sowie diverse landbasierte Transport- und Logistikkapazitäten. Eigene Schiffe sind gemäß den bisher bekannten Informationen nicht vorgesehen[31] und angesichts der für die gesamten Bedarfe knapp bemessenen Finanzierung dieses EU-Politikfelds frühestens im nächsten mehrjährigen EU-Finanzrahmen denkbar. Gleichwohl könnte evaluiert werden, ob Schiffe, die auf die Reparatur von Unterseekabeln oder anderen Infrastrukturen (Windturbinen, Öl- und Gasförderstätten) spezialisiert sind, im

25 Manuel Bewarder/Stefan Buchen/Volkmar Kabisch/Florian Flade, »Kippt der Einstieg beim Hamburger Hafen?«, *Tagesschau.de*, 19.4.2023, <https://www.tagesschau.de/investigativ/ndr-wdr/bundesregierung-hamburg-hafen-containerterminal-101.html> (eingesehen am 21.7.2023).

26 Bundesministerium für Digitales und Verkehr, »Die Nationale Hafenstrategie«, Berlin, 7.7.2023, <https://bmdv.bund.de/DE/Themen/Mobilitaet/Wasser/Hafenstrategie/hafenstrategie.html> (eingesehen am 1.9.2023).

27 European Commission, *Lebanon and Cyprus Emergencies 2006*, Brüssel, o. D., <https://ec.europa.eu/echo/files/civil_protection/leb_cy_2006.htm> (eingesehen am 21.7.2023).

28 Council of the European Union, *Infographic – The EU Civil Protection Mechanism in Numbers*, 1.3.2023, <https://www.consilium.europa.eu/en/infographics/civil-protection/> (eingesehen am 21.7.2023); »EU kündigt Sofortmaßnahmen und Härte gegen ›illegale Grenzübertritte‹ an«, in: *Handelsblatt*, 5.3.2020, <https://www.handelsblatt.com/politik/international/fluechtlinge-eu-kuendigt-sofortmassnahmen-und-haerte-gegen-illegale-grenzuebertritte-an/25612214.html> (eingesehen am 20.12.2023).

29 European Commission, »Proposal for a Council Recommendation« [wie Fn. 11].

30 Vgl. den Beitrag von Göran Swistek in dieser Studie, S. 61ff

31 Bislang besteht nur eine mitgliedstaatliche Ressourcenteilung (Modul) für Boote, die bei Hochwasserlagen eingesetzt werden können: DLRG Bundesverband, »Das EU-Modul FRB«, o. D., <https://www.dlrg.de/mitmachen/auslandseinsaetze/> (eingesehen am 21.7.2023).

europäischen Verbund sinnvoll geteilt und als Einsatzreserve vorgehalten werden sollten.[32] Stattdessen wird auf EU-Ebene diskutiert, neue Reaktionsteams für hybride Bedrohungen einzurichten. Als Aufgaben für diese Teams wird aber primär an die Reaktion auf Desinformation und Cyberangriffe gedacht.[33]

Der EU-Katastrophenschutzmechanismus für den maritimen Bereich ist als politischer und administrativer Rahmen zu verstehen.

Somit ist der EU-Katastrophenschutzmechanismus für den maritimen Bereich zum aktuellen Stand als politischer und administrativer Rahmen zu verstehen, in dem weitere Risikokartierungen, Szenarien und gemeinsame Trainings entwickelt werden. Wie in anderen Einsatzfeldern können dazu künftig auch grenzüberschreitende Übungen von Großschadensereignissen auf See gehören.[34] Ohne neue verbindliche Entscheidungen sowie Investitionen ist die Zusammenarbeit zwischen den Mitgliedstaaten im Ernstfall aber nicht verlässlich. Derzeit ist offen, ob die Mitgliedstaaten eine Vorlage der Europäischen Kommission für eine Empfehlung des Rats verabschieden, die politische Krisenkoordinierung im Rat[35] um eine weitere thematisch fokussierte »Blaupause« zur Reaktion auf Vorfälle und Krisen in kritischen Infrastrukturen zu ergänzen.[36] Solche Blaupausen werden bereits in den Bereichen Cybersicherheit und Migration zur Koordination genutzt, schaffen aber für sich genommen noch keine neuen operativen Fähigkeiten. Die neue Vorlage zu kritischen Infrastrukturen betont die bereits bestehenden rechtlichen Verpflichtungen zum Informationsaustausch und zur Einrichtung nationaler Kontaktpunkte, die dem Infrastrukturschutz dienen. Bestenfalls bestärkt diese Blaupause die Kooperation zwischen EU-Institutionen, EU-Agenturen und EU-Mitgliedstaaten, beispielsweise im Rahmen von Übungen, sie bleibt aber grundsätzlich ein freiwilliger Mechanismus ohne dezidierte Ressourcen.

Verschiedene EU-Agenturen verfügen allerdings über relevante Kapazitäten im maritimen Sektor. Die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) mit rund 250 Mitarbeitern und Sitz in Lissabon stellt technische und operative Unterstützung in Bereichen wie Seesicherheit und Umweltschutz bereit, während die Europäische Fischereiaufsichtsagentur (EFCA) mit 56 Mitarbeitern ergänzend die Kontrolle maritimer Gebiete und von Schiffen begleitet. Die Europäische Agentur für die Grenz- und Küstenwache (Frontex) mit demnächst bis zu 10.000 Einsatzkräften unterstützt Mitgliedstaaten bei der allgemeinen Seeraumüberwachung. Frontex ist zudem die Zentralstelle für das europäische Überwachungssystem Eurosur und soll die Lagezentren aller Grenz- und Küstenschutzbehörden der Mitgliedstaaten vernetzen. Im Rahmen des Eurosur-Systems und weiterer relativ umfassender Fähigkeiten zur Luftüberwachung ist somit zumindest für den Mittelmeerraum eine engmaschige Erfassung von Schiffsbewegungen gewährleistet. Ergänzend sind die Europäische Verteidigungsagentur (EDA) und die Europäische Agentur für Cybersicherheit (ENISA) zu nennen, die einige Querschnittsbelange und Projekte mit maritimem Bezug betreuen. Beispielsweise veröffentlichte ENISA Berichte zu Cyberangriffen auf Hafenbetreiber und Logistikunternehmen.[37] Von insgesamt rund 60 Projekten zur europäischen Rüstungsbeschaffung und Entwicklung, die derzeit von der EDA koordiniert werden, sind acht im maritimen Sektor angesiedelt.[38] Seit den Angriffen auf Nord Stream 2 ist

32 Die britische Marine hat schon vor den Nord-Stream-Anschlägen begonnen, ein solches Spezialschiff auszurüsten, das 2024 einsatzbereit sein soll, vgl. Jonathan Beale, »New Royal Navy Ship to Protect ›Critical‹ Undersea Cables«, *BBC News*, 21.3.2021, <https://www.bbc.com/news/uk-56472655> (eingesehen 1.9.2023).

33 Vgl. Rat der Europäischen Union, »Moldau: EU richtet eine zivile Mission zur Stärkung der Widerstandsfähigkeit des Sicherheitssektors ein«, Pressemitteilung, 24.4.2023, <https://www.consilium.europa.eu/de/press/press-releases/2023/04/24/moldova-eu-sets-up-a-civilian-mission-to-strengthen-the-resilience-of-the-security-sector/> (eingesehen am 21.7.2023).

34 EU Modex, »Outlook: Baltic Sea Expansion«, o. D., <https://10years.eu-modex.eu/future-of-eu-modex/future/baltic-sea-expansion> (eingesehen am 21.7.2023).

35 Der sogenannte ICPR-Mechanismus (Integrated Political Crisis Response).

36 European Commission, »Proposal for a Council Recommendation« [wie Fn. 11].

37 European Union Agency for Cybersecurity (ENISA), »Maritime Sector«, o. D., <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/maritime/?tab=publications> (eingesehen am 21.7.2023).

38 Essential Elements of European Escort (4E), European Patrol Corvette (EPC), Harbour and Maritime Surveillance and Protection, Maritime (semi) Autonomous Systems for Mine Countermeasures, Medium size Semi-Autonomous

ein neues Vorhaben von sechs Mitgliedstaaten hinzugekommen, die militärischen Unterwasserfähigkeiten zum Schutz kritischer Infrastrukturen zu verbessern. Zu diesem Zweck soll aber zunächst der Bedarf genauer erhoben werden; eine gemeinsame Beschaffung wäre frühestens ab 2028 avisiert.[39]

Für eine baldige Stärkung des Schutzes maritimer kritischer Infrastrukturen ist das Vorhaben eines gemeinsamen operativen Lagebilds von besonderer Bedeutung.

Für eine zeitnahe Stärkung des Schutzes maritimer kritischer Infrastrukturen ist in der Schnittmenge der erwähnten EU-Agenturen das Vorhaben von besonderer Bedeutung, ein gemeinsames operatives Lagebild zu erstellen.[40] Gerade hier ließen sich die umfassenden Kompetenzen der EU im zivilen Sektor bündeln und im Gegensatz zu militärischen Akteuren offener und inklusiver handhaben. Das sogenannte Common Information Sharing Environment (CISE) soll demnach Überwachungssysteme der europäischen Agenturen sowie der korrespondierenden nationalen Behörden interoperabel gestalten und nach Bedarf zusammenführen. Die Entwicklung von CISE, die erstmals 2009 vorgeschlagen wurde, wird seither im Rahmen der Maritimen Sicherheitsstrategie der EU (EUMSS) genauer konzipiert. Seit 2019 soll die Umsetzung in einer gemeinsamen Stakeholder Group vorangebracht werden, die alle EU-/EWR-Mitgliedstaaten, die Europäische Kommission, den Europäischen Auswärtigen Dienst und die beteiligten EU-Agenturen (EDA, EFCA, EMSA, Frontex und SatCen) umfasst. Dieses Vorhaben kann bei Vorsorge, Risikoerfassung und Krisenreaktion einen deutlichen Mehrwert schaffen. Die Vielzahl fachlich spezialisierter Agenturen auf EU-Ebene spiegelt sich in zahlreichen nationalen Behörden, die für verschiedene Aspekte des Küstenschutzes und der Sicherung von Seeräumen zuständig sind.[41] Eine geteilte aktuelle Datenlage ist für unterschiedliche Zwecke sinnvoll, einschließlich des Schutzes kritischer Infrastrukturen.

Trotz jahrelanger Bemühungen ist CISE bisher allerdings nicht über das Stadium eines Pilotprojekts hinausgekommen. Vorerst ist nur das separate Programm der Europäischen Verteidigungsagentur für eine Informationsaustauschplattform für die Marine (MARSUR) im Zuge von GSVP-Operationen zur Anwendung gekommen.[42]

EU-Investitionen in maritime Infrastrukturen

Die »geoökonomische Union« und verwandte Konzepte der offenen strategischen Autonomie schlagen sich insbesondere seit der Pandemie in neuen Rechtsakten und Initiativen zur Diversifizierung von Lieferketten, Rohstoffen und kritischen Gütern wie etwa Medizinprodukten nieder. Die Mobilisierung neuer europäischer Finanzmittel und damit verbundener privatwirtschaftlicher Investitionen ist ein weiterer gewichtiger Trend. So wurden den EU-Mitgliedstaaten 750 Milliarden Euro an Direkthilfen und Krediten zur Wiederbelebung der Wirtschaft nach Corona bereitgestellt, während für die beschleunigte Abkoppelung von russischen Energielieferungen im Rahmen des REPowerEU-Plans weitere 33 Milliarden zur Verfügung gestellt wurden. Darüber hinausgehende nationale Subventionen sind als zeitlich begrenzte Ausnahmen vom EU-Recht genehmigt worden. Alle Mittel kommen zu jenen der langfristigen EU-Strukturfonds und anderen regulären Programmen der Europäischen Investitionsbank hinzu.

In dieser dynamischen Gemengelage lässt sich nicht eindeutig ausweisen, welche Investitionen tatsächlich zum Schutz oder zur Resilienz kritischer

Surface Vehicle (M-SASV), Upgrade of Maritime Surveillance (UMS).

39 Critical Seabed Infrastructure Protection (CSIP) project, vgl. European Defence Agency, *11 New PESCO Projects Focus on Critical Defence Capabilities and Interoperability*, 13.5.2023, <https://eda.europa.eu/news-and-events/news/2023/05/23/11-new-pesco-projects-to-focus-on-critical-defence-capabilities-and-interoperability> (eingesehen am 1.9.2023).

40 European Commission, *Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strategy and Its Action Plan*, Brüssel, 10.3.2023, vgl. S. 9f, <https://data.consilium.europa.eu/doc/document/ST-7311-2023-INIT/en/pdf> (eingesehen am 20.12.2023).

41 Wissenschaftliche Dienste des Deutschen Bundestages, *Seeschifffahrt und Seehäfen in Deutschland. Zuständigkeiten und Verwaltung*, Sachstand WD 5 — 3000 — 013/20, 13.2.2022, <https://www.bundestag.de/resource/blob/687984/0095fe54b1ac83321e6d4028413757c7/WD-5-013-20-pdf-data.pdf> (eingesehen am 21.7.2023).

42 Nathan Gain, »Europe's Maritime Surveillance Project Enters Third Phase«, *Naval News*, 3.12.2020, <https://www.navalnews.com/naval-news/2020/12/europes-maritime-surveillance-project-enters-third-phase/> (eingesehen am 25.7.2023).

Infrastrukturen beitragen. Allgemein stellt sich die Frage, ob Investitionen in Infrastrukturen grundsätzlich in diesem Sinne zu werten sind, also als Beitrag zur Redundanz wie auch zu einer verstärkten europäischen Eigentümerstruktur, oder ob vielmehr nur gezielte Sicherheitsmaßnahmen zum Infrastrukturschutz gezählt werden sollten.

Für den maritimen Bereich bietet es sich an, das Volumen der Investitionen in Infrastrukturen im Rahmen der EU-Initiative Global Gateway abzuschätzen.

Für den maritimen Bereich bietet es sich an, das Volumen der Investitionen in Infrastrukturen im Rahmen der EU-Initiative Global Gateway abzuschätzen. Diese wurde als Alternative zur chinesischen Belt-and-Road-Initiative angelegt und hat somit Bezüge zum geoökonomischen Wettbewerb sowie zu potentiellen hybriden Bedrohungen. Insgesamt sollen via Global Gateway über Garantien und Beteiligungen private Investitionen in Höhe von rund 300 Milliarden Euro mobilisiert werden. Diese Summen sind bislang nur projiziert und thematisch wie regional sehr weit gestreut. Für die Zwecke dieses Beitrags lässt sich anhand öffentlicher Mitteilungen der Europäischen Investmentbank und ergänzender nationaler Pressemitteilungen grob schätzen,[43] dass zum derzeitigen Stand Aufwendungen für maritime Infrastrukturen in Häfen oder Energienetzwerke unterhalb der Summe von etwa 10 Milliarden Euro verbleiben. In der südlichen und südöstlichen europäischen Nachbarschaft (Mittelmeer, Schwarzes Meer) sind für die folgenden Jahre Projekte mit europäischer Finanzierung oder Beteiligung an privaten Initiativen in Höhe von mindestens 8,5 Milliarden Euro geplant. Dazu gehören vor allem mehrere Elektrizitätsverbindungen in den Kaukasus, nach Zypern, Israel und Ägypten sowie Datenkabel nach Nordafrika, Georgien und Armenien. Innerhalb der EU sind Darlehen der Europäischen Investitionsbank oder Zuschüsse aus EU-Fonds von insgesamt rund einer Milliarde Euro für europäische Häfen in Italien, Griechenland, Portugal und Litauen erteilt oder geplant. Ergänzend wird derzeit geprüft, ob die EU sich an der Finanzierung eines neuen, über die Arktis verlaufenden Datenkabels nach Japan beteiligen will; eine bis Ende 2023 laufende Machbarkeitsstudie zu diesem Projekt (»Far North Fiber«) wird mit Mitteln aus dem EU-Förderprogramm für trans-europäischen Infrastrukturausbau Connecting Europe Facility gefördert.[44]

Die geplanten Investitionen können je nach Thema und Vergleichsmaßstab als unterschiedlich gewichtige Beiträge für resilientere maritime kritische Infrastrukturen gewertet werden. Insbesondere im Bereich von Datenkabeln können auch kleinere Summen neue Projekte ermöglichen, die zur gesamteuropäischen Diversifizierung beitragen. Bei Häfen und Energienetzen hingegen ist die geschätzte Summe von deutlich unter 10 Milliarden Euro kein bedeutender Hebel.

Ungleich größer dimensioniert sind dagegen beispielsweise die jüngst angekündigten minilateralen Pläne der Nordseeanrainer, einschließlich Großbritanniens und Norwegens, bis zum Jahr 2050 insgesamt 300 GW an Offshore-Installationen aufzubauen.[45] Die Europäische Union begleitet dieses Vorhaben auf politischer Ebene, bisher jedoch ohne eindeutige Finanzierungszusagen. Allgemein wächst die Unterstützung für eine aktive europäische Industrie- und Energiepolitik sowie die Finanzierung weiterer öffentlicher Güter zur Stärkung der europäischen Wettbewerbsfähigkeit. Die maritime Dimension ist dabei jedoch nicht explizit oder gesondert ausgewiesen.

Empfehlungen

Der Anschlag auf die Nord-Stream-Pipelines in der Ostsee hat die längerfristige politische Dynamik auf EU-Ebene verstärkt, den Schutz kritischer Infrastrukturen und die europäischen Krisenreaktionsfähigkeiten zu verbessern. Diverse sicherheits- und wirtschaftspolitische Strategien der EU haben seither vermehrt die maritime Dimension in den Fokus gerückt und das Bewusstsein für grenzüberscheitende Abhängigkeiten in diesem Bereich geschärft. Die EU kann dabei auf diverse, seit Ende der 2000er Jahre

43 Online-Datenrecherche Stand 2023, gesammelte Belege auf Anfrage vorlegbar.

44 European Commission, *Planning of Development of the Autonomous Digital Backbone and Connecting Europe with Global Strategic Partners*, Brüssel, Januar 2023, <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43251567/101089599/CEF2027> (eingesehen am 26.7.2023).

45 Government of the Netherlands/Alexander De Croo, *Ostend Declaration on the North Seas as Europe's Green Power Plant*, 24.4.2023, <https://www.premier.be/en/north-sea-summit-23-declaration> (eingesehen am 21.7.2023).

geleistete Vorarbeiten aufbauen, als erstmalig ein politischer und rechtlicher Rahmen für den Schutz kritischer Infrastrukturen aufgespannt wurde. Dagegen ist Deutschland noch damit befasst, die Koordination und Vorsorge zwischen den Ebenen der Länder und des Bundes zu verbessern. Eine grenzüberschreitende bis paneuropäische Risikobewertung und eine ebensolche Planung müssen in diesem breiten Themenfeld konsequent weiterverfolgt werden.

Bei genauerer Betrachtung zeigt sich allerdings, dass der Mehrwert für den maritimen Sektor bislang eher gering ausfällt. Die größten Neuerungen durch die novellierten EU-Rechtsakte für den Schutz kritischer Infrastrukturen fallen jenseits der bereits seit 2008 regulierten Bereiche Energie und Verkehr an, konkret für landbasierte Infrastrukturen (u. a. Trink- und Abwasser, Gesundheitswesen, Finanzdienstleister und öffentliche Verwaltung). Die Diskussion über die chinesische Beteiligung an europäischen Häfen weist widersprüchliche Tendenzen auf. Einerseits ist hier in den letzten Jahren eine deutliche Änderung der europäischen Bedrohungswahrnehmung zu beobachten. Andererseits verbleibt die Entscheidung über die Zulassung ausländischer Beteiligungen letztlich bei den einzelnen Mitgliedstaaten. Eine weitergehende Europäisierung und eine größere Verbindlichkeit bei der Prüfung ausländischer Investitionen in kritische Infrastrukturen — ob landbasiert oder maritim — wären in jedem Fall erstrebenswert.

Die bisher verfügbaren Daten lassen keine strategische europäische Investitionspolitik in Bezug auf Häfen oder andere kostenintensive maritime Infrastrukturen erkennen. Eine Erklärung hierfür wäre die Vielzahl an konkurrierenden und drängenden Anforderungen im Kontext einer Verbesserung der europäischen Wettbewerbsfähigkeit und Versorgungssicherheit — etwa im Bereich der kritischen Technologien (Künstliche Intelligenz) und Produkte (Chips, Medikamente). Dennoch sollte eine regelmäßige, bessere Koordinierung der unterschiedlichen europäischen Finanzierungs- und Investitionsprogramme im maritimen Sektor angestrebt werden. Voraussichtlich werden sich im Zusammenhang mit der Energiewende und dem Ziel der Klimaneutralität zwischen den EU-Staaten auch größere Schnittmengen bei Fragen der maritimen Sicherheit ergeben.

Der Schutz europäischer maritimer Infrastrukturen vor feindlichen Aktivitäten bleibt in der Zuständigkeit nationaler Sicherheitsorgane, militärischer Kräfte und der Nato.

Zusammengefasst bleibt somit der operative Schutz europäischer maritimer Infrastrukturen vor wachsenden feindlichen Aktivitäten, insbesondere im Unterwasserbereich, in der Zuständigkeit nationaler Sicherheitsorgane, militärischer Kräfte und der Nato. Eine regelmäßige und enge Koordination zwischen der EU und der Nato könnte zivile Daten für ein umfassendes Lagebild europäischer Küsten und angrenzender Gewässer beisteuern. Insofern sollte das Vorhaben des Common Information Sharing Environment (CISE) möglichst schnell umgesetzt und in die Praxis überführt werden. Es ist zu begrüßen, dass auch im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik ein militärisches Beschaffungsvorhaben zum Schutz kritischer Infrastrukturen im Unterwasserbereich in Aussicht steht. Dringlicher ist jedoch, dass im Rahmen des EU-Katastrophenschutzmechanismus nicht nur neue Szenarien und Übungen für den maritimen Raum entwickelt werden, sondern dass möglichst bald auch spezialisierte Einsatzreserven, insbesondere Reparaturschiffe, beschafft werden. Vergleichbar mit der europäischen Flotte von Löschflugzeugen ließen sich so Fähigkeiten aufbauen, die nicht jeder Mitgliedstaat vorhalten kann oder will, was wiederum für die EU einen deutlichen Mehrwert bedeuten würde.

Daniel Voelsen

Schlussfolgerungen

In den Weiten der Meere findet sich eine Vielzahl von Infrastrukturen, die zentrale Bedeutung haben für die globalen Energiebeziehungen, das Netz des weltweiten Handels mit Nahrungsmitteln und nicht zuletzt den Datenaustausch im Internet. Deutschland nutzt vom europäischen Kontinent aus viele dieser Infrastrukturen. Und auch wenn nicht jede einzelne davon gleichermaßen bedeutsam ist, so zeigen die Beiträge dieser Studie doch: Einige maritime Infrastrukturen sind in der Tat so wichtig, dass sie als kritische Infrastrukturen verstanden werden sollten. Und: Neben fixen physischen Infrastrukturen können auch Seewege oder Schiffe den Charakter von Infrastrukturen erlangen und sollten als solche ebenfalls berücksichtigt werden.

Das Identifizieren kritischer Infrastrukturen, auch jener im maritimen Raum, dient dazu, spezifische Risiken zu erkennen und entsprechend gezielte Schutzmaßnahmen vorzusehen. Die Fokussierung auf *kritische* Infrastrukturen trägt insofern auch dazu bei, einer »Versicherheitlichung« des maritimen Raums vorzubeugen, sprich: das pauschale Übergreifen einer primär sicherheitspolitischen Logik auf das gesamte Geschehen im maritimen Raum zu vermeiden.

Die mittel- und langfristige Entwicklung der Bedrohungslage

In diesem Sinne lassen sich zum heutigen Stand einige maritime Infrastrukturen als besonders bedeutsam — eben *kritisch* — ausweisen (vgl. hierzu die folgende Karte). Ihre Kritikalität ergibt sich aus der Kombination einer herausgehobenen Bedeutung für den Zugang zu den entsprechenden Gütern und einer besonderen Bedrohungslage. Dabei zeigt die Analyse, dass neben fixen physischen Infrastrukturen auch Containerschiffe als bewegliche Einrichtungen oder Seewege als immaterielle Strukturen relevante kritische Infrastrukturen darstellen können.

Heute und auf absehbare Zeit ist die Bedrohungslage in besonderem Maße durch den Angriff Russlands auf die Ukraine geprägt. Vertreter der russischen Regierung haben explizit damit gedroht, maritime Infrastrukturen westlicher Staaten anzugreifen.[1] In Kombination mit den in jüngerer Zeit beobachteten Aktivitäten russischer Schiffe in Nord- und Ostsee ist hier in der Tat von einer ernstzunehmenden Bedrohung auszugehen. Wie sich diese in Zukunft entwickelt, wird wesentlich vom weiteren Verlauf des Krieges in der Ukraine abhängen.

Mittel- bis langfristig ist damit zu rechnen, dass die Bedeutung maritimer Infrastrukturen groß bleiben und in einigen Bereichen wie der Energieversorgung möglicherweise sogar noch zunehmen wird. Veränderungen gehen dabei zum einen von der technischen Entwicklung aus: So wird sich, wie im Beitrag von Jacopo Maria Pepe skizziert, mit dem verstärkten Umstieg auf Wasserstoff als Energiequelle auch das Portfolio der relevanten maritimen Infrastrukturen verschieben. Mit Blick auf die Kommunikationsnetze wird sich über die kommenden Jahre zeigen, inwieweit neue Satellitenkonstellationen Datenströme abwickeln können, die heute über Unterseekabel laufen. Falls erdnahe Satelliten tatsächlich vor allem für besonders sensible oder zeitsensitive Datenströme eine redundante Infrastruktur bereitstellen können, dürfte dies die Kritikalität von Unterseeverbindungen vermindern. Hinzu kommen perspektivisch möglicherweise neue Nutzungen des maritimen Raums, etwa zur Speicherung von CO_2 oder zur Gewinnung von Rohstoffen (siehe dazu die Infoboxen in diesem Kapitel, S. 82 und S. 83).

1 Dmitry Medvedev, »Based on the Proof of western countries' complicity in blowing up the Nord Stream pipelines, we have none, not even moral limitations left to refrain from destroying our enemies' undersea communications cables«, *Social Media Post*, *X*, 14.6.2023, <https://twitter.com/MedvedevRussiaE/status/1668908185229426688> (eingesehen am 25.9.2023).

Energie – Ernährung – Kommunikation: maritime kritische Infrastrukturen von besonderer Bedeutung für Deutschland und Europa

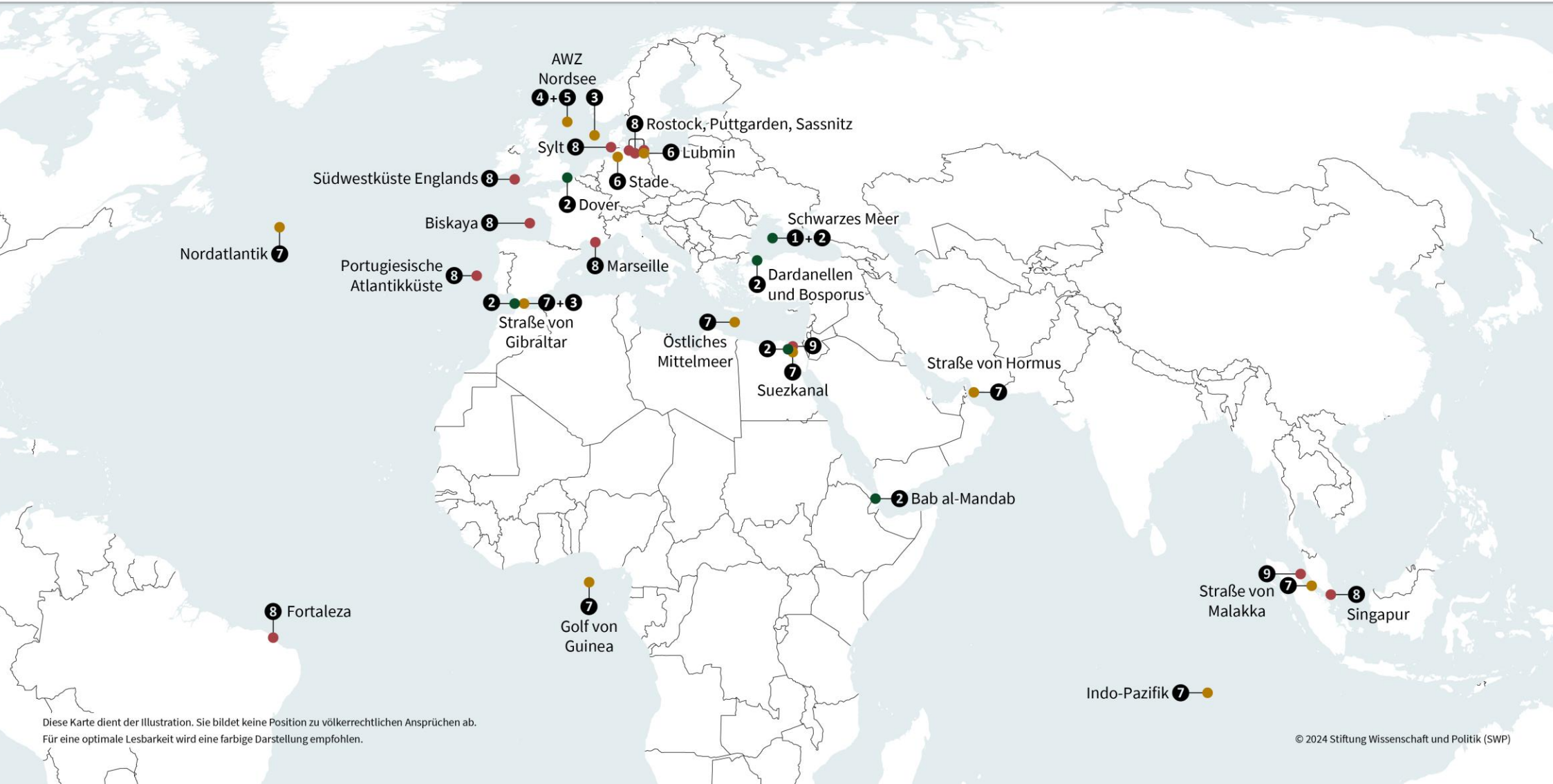
Diese Karte zeigt, wo sich maritime kritische Infrastrukturen von besonderer Bedeutung für die drei Sektoren Ernährung, Energie und Kommunikation befinden. Sie basiert auf den Analysen in den Kapiteln zu maritimem Nahrungstransport, maritimen Energieinfrastrukturen und Untersee-Datenkabeln.

- Kritische Knotenpunkte Nahrung und nahrungsrelevante Produkte (Fokus auf Getreide und Dünger)
- Kritische Knotenpunkte maritime Energieinfrastrukturen (Fokus auf Deutschland)
- Kritische Knotenpunkte Untersee-Datenkabel

Quellen: Beiträge von Jacopo Maria Pepe, Bettina Rudloff und Daniel Voelsen in: Daniel Voelsen (Hg.), *Maritime kritische Infrastrukturen. Strategische Bedeutung und geeignete Schutzmaßnahmen*, Berlin: Stiftung Wissenschaft und Politik, Februar 2024, DOI: 10.18449/2024S03

Kategorien von Infrastrukturen

- **Nahrung**
  - 1 Häfen
  - 2 Seewege
- **Energie**
  - 3 Pipelines
  - 4 Offshore-Windanlagen
  - 5 Stromtrassen
  - 6 Terminals
  - 7 LNG-(und Wasserstoff-)Schiffe
- **Kommunikation**
  - 8 Anlandestellen
  - 9 Untersee-Datenkabel



Diese Karte dient der Illustration. Sie bildet keine Position zu völkerrechtlichen Ansprüchen ab.
Für eine optimale Lesbarkeit wird eine farbige Darstellung empfohlen.

Mögliche Zukünfte: Tiefseebergbau (Lisa Voigt)

In den letzten Jahren hat der Abbau mineralischer Rohstoffe in der Tiefsee verstärkt Aufmerksamkeit erfahren. Die drei Rohstoffarten Manganknollen, Kobaltkrusten und Massivsulfide enthalten Metalle wie Kupfer, Kobalt, Nickel und Seltene Erden. Neben Vorkommen in der Hohen See, vor allem im Indischen Ozean und in der Clarion-Clipperton-Bruchzone im Zentralpazifik, sind hier auch die Küstenmeere und ausschließlichen Wirtschaftszonen einiger Staaten relevant, in Europa besonders norwegische Gewässer.[a]

Die Internationale Meeresbodenbehörde (ISA) wurde im Rahmen des UN-Seerechtsübereinkommens mit dem Auftrag gegründet, die Ressourcen auf dem Meeresboden und im Meeresuntergrund jenseits der Grenzen des Bereichs nationaler Hoheitsbefugnisse (»Gebiet« gem. Art. 1 Abs. 1 SRÜ) zu verwalten. Bisher hat sie 31 Explorationslizenzen an Staaten und von diesen gesponserte[b] Unternehmen vergeben, darunter an die EU-Mitgliedstaaten Belgien, Bulgarien, die Tschechische Republik, Slowakei, Polen und Frankreich. Deutschland besitzt über die Bundesanstalt für Geowissenschaften und Rohstoffe jeweils eine Lizenz im Pazifik und im Indischen Ozean.

Die Exploration umfasst neben der Forschung das Testen neuer Infrastrukturen, etwa von ferngesteuerten oder autonomen Tiefseebergbaugeräten und hydraulischen Schlauchsystemen für den Transport der Mineralien an die Oberfläche. Im Falle eines Abbaus kämen zudem Plattformen und Schiffe zur Trennung der Metalle von dem Sediment bzw. zu ihrem Transport zum Einsatz. Die Lizenzen beinhalten ein Vorrecht auf zukünftigen Abbau, der aber aufgrund hoher Kosten, mangelnder Regulierungen und fehlender marktreifer Technologien bislang gar nicht stattfindet.[c] Die ISA-Mitgliedstaaten einigten sich im Juli 2023 darauf, die Verabschiedung der Regulierung für Tiefseebergbau auf dem Meeresboden jenseits nationaler Hoheitsbefugnisse auf voraussichtlich 2025 zu verschieben.[d]

Im Zuge der steigenden Bedeutung strategischer Rohstoffsicherung könnten durch Tiefseebergbau geförderte Metalle zukünftig eine kritische Dimension erhalten.[e] Derzeit verfolgt die EU mit dem Critical Raw Material Act etwa das Ziel, durch Diversifizierung die Abhängigkeit von China zu reduzieren.[f] Aufgrund des Risikos von irreversiblen Umweltschäden und Menschenrechtsverletzungen hat sie einen Abbau jedoch vorerst ausgeschlossen.[g] Die Bundesregierung forderte jüngst international eine »precautionary pause« (vorsorgliche Pause), da die Umweltfolgen auf Basis des jetzigen Wissensstandes nicht abzusehen seien.[h] In Norwegen stimmte eine Mehrheit des Parlaments kürzlich für kommerziellen Tiefseebergbau auf dem Festlandsockel.[i]

Sollte Tiefseebergbau durchgeführt werden, wären Infrastrukturschäden insbesondere bei kostenintensiven Reparaturen am Meeresgrund mit wirtschaftlichen Verlusten verbunden. Gleichzeitig sind gezielte Angriffe in großen Meerestiefen unwahrscheinlich. Plattformen und Schiffe könnten dagegen ein potentielles Ziel von Piraterie und Terrorismus werden. Auch Aktionen von Umweltaktivistinnen und -aktivisten, die auf die Folgen des Tiefseebergbaus aufmerksam machen, sind denkbar.[j] Außerdem könnte der Wettbewerb um Ressourcen zwischenstaatliche Territorialkonflikte verschärfen.[k] Nicht zuletzt können die neuen Infrastrukturen und die Folgen des Tiefseebergbaus negative Auswirkungen auf Fischerei, Schifffahrt und Unterseekabel als bereits bestehende kritische Infrastrukturen haben.[l]

a John Childs, »Extraction in Four Dimensions: Time, Space and the Emerging Geo(-)politics of Deep-Sea Mining«, in: *Geopolitics*, 1 (2020), S. 189–213.

b Nach Art. 153 SRÜ ist die Befürwortung eines Vertragsstaates (sog. »Sponsorship«) eine notwendige Voraussetzung für die Genehmigung eines bergbaulichen Vorhabens durch die ISA. Der Staat ist für die Sicherstellung der Einhaltung des Regelwerks der ISA verantwortlich. Siehe Umweltbundesamt, »Der ›Mining Code‹ der Internationalen Meeresbodenbehörde (IMB)«, 18.8.2021, <https://bit.ly/3HwvTeQ> (eingesehen am 23.10.2023).

c Das bisher einzige Abbauprojekt, SOLWARA 1 vor der Küste Papua-Neuguineas, wurde 2019 vor Beginn des Abbaus wegen fehlender Finanzierung beendet. Siehe Seas at Risk, *At a Crossroads: Europe's Role in Deep-sea Mining*, Brüssel 2021, <https://bit.ly/47MQgyX> (eingesehen am 20.4.2023).

d Im Jahr 2024 werden die ISA-Mitgliedstaaten über eine vorsorgliche Pause für den Schutz des marinen Ökosystems diskutieren. Siehe Karen McVeigh, »International Talks End without Go-ahead for Deep-sea Mining«, in: *The Guardian* (online), 29.7.2023, <https://bit.ly/4b8uGrC> (eingesehen am 20.9.2023).

e Tom LaTourrette, »Is Seabed Mining an Opportunity to Break China's Stranglehold on Critical Minerals Supply Chains?«, 21.11.2022 (Blog-Beitrag), <https://bit.ly/3SqEoOJ> (eingesehen am 20.4.2023).

f Vgl. den Beitrag von Raphael Bossong, S. 71ff.

g Europäische Kommission, *EU Biodiversity Strategy for 2030. Bringing Nature Back into Our Lives*, 20.5.2020, <https://bit.ly/3UgcjuP> (eingesehen am 25.4.2023); Europäische Kommission, *Setting the Course for a Sustainable Blue Planet – Joint Communication on the EU's International Ocean Governance Agenda*, 24.6.2022, <https://bit.ly/47HgrXS> (eingesehen am 25.4.2023).

h Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, »Schutz der Meere: Deutschland unterstützt bis auf Weiteres keinen Tiefseebergbau«, Pressemitteilung, Berlin, 1.11.2022, <https://bit.ly/3SewxlU> (eingesehen am 20.7.2023).

i Miranda Bryant, »Norway Votes for Deep-sea Mining Despite Environmental Concerns«, in: *The Guardian* (online), 9.1.2024, <https://bit.ly/3uffiZM> (eingesehen am 17.1.2024).

j Edwin Egede, »Maritime Security and Deep Seabed beyond National Jurisdiction«, in: Catherine Banet (Hg.), *The Law of the Seabed. Access, Uses, and Protection of Seabed Resources*, Leiden: Koninklijke Brill N.V., 2020, S. 185–210.

k Uwe K. Jenisch, »Old Laws for New Risks at Sea: Mineral Resources, Climate Change, Sea Lanes, and Cables«, in: *WMU Journal of Maritime Affairs*, 11 (Januar 2012), S. 169–185.

l UN Environment Programme's Sustainable Blue Economy Finance Initiative, *Harmful Marine Extractives: Understanding the Risks & Impacts of Financing Non-renewable Extractive Industries*, Genf 2022, <https://bit.ly/3u8gHl1> (eingesehen am 24.4.2023).

Mögliche Zukünfte: CO_2-Transport- und Speicheranlagen im maritimen Raum (Miranda Böttcher/Oliver Geden)

Nachdem sich die Europäische Union und Deutschland verpflichtet haben, bis 2050 bzw. 2045 Netto-Null-Emissionsziele zu erreichen, entwickeln sie nun Strategien, wie sie schwer vermeidbare fossile CO_2-Emissionen mittels Carbon Capture and Storage (CCS) abscheiden und verbleibende Restemissionen mittels CO_2-Entnahme (Carbon Dioxide Removal, CDR) aus der Atmosphäre ausbalancieren könnten. CCS umfasst Prozessketten, bei denen CO_2 abgetrennt und verdichtet wird. CDR umfasst eine Reihe von Methoden, die CO_2 aus der Atmosphäre entziehen, darunter auch solche, die CCS mit CO_2 aus Biomasse (BECCS) oder aus der Umgebungsluft (DACCS) kombinieren.[a] Bei allen CCS-Varianten muss das CO_2 anschließend vom Ort der Abscheidung oder Entnahme wegtransportiert und in geologischen Formationen gespeichert werden. Wegen gesellschaftlicher Bedenken gegen die CO_2-Speicherung an Land wird die Speicherung unter dem Meeresboden zunehmend als praktikable Alternative angesehen.[b]

Zukünftige maritime CO_2-Transport- und Speicherinfrastruktur könnte Häfen und küstennahe »Hubs« für die Zwischenlagerung und Verladung, CO_2-Containerschiffe, Unterwasserpipelines, Verpressungsanlagen auf künstlichen Inseln oder Plattformen sowie Einrichtungen zur Injektion und zum Monitoring umfassen. Derzeit gibt es Pläne für Hubs in Wilhelmshaven und Rostock sowie für den Export von deutschem CO_2 zur Speicherung in der ausschließlichen Wirtschaftszone (AWZ) Norwegens und Dänemarks, aber auch längerfristige Untersuchungen zur Möglichkeit einer CO_2-Speicherung unter dem Meeresboden in der deutschen AWZ.[c]

Es ist eher unwahrscheinlich, dass ein anderer Staat die deutsche Infrastruktur zur Kohlenstoffspeicherung sabotieren wollen würde — es sei denn, es ginge darum, die deutsche Industrie, die gegebenenfalls auf CCS oder CDR angewiesen wäre, in wirtschaftliche Schwierigkeiten zu bringen. Alternativ könnten radikale Umweltorganisationen versuchen, solche Anlagen aus Protest zu sabotieren.

Eine Pipeline zur Explosion zu bringen ist vergleichsweise einfach. Auch das Abfangen oder Beschädigen von Schiffen ist denkbar. Die Sprengung eines geologischen CO_2-Speichers wiederum ist im Grunde unmöglich — diese Speicher befinden sich mehrere Kilometer unter dem Meeresboden, und CO_2 ist nicht explosiv. Es wäre jedoch technisch möglich, eine Explosion während der CO_2-Verpressungsphase an der Injektionsstelle herbeizuführen, wenn ein hoher Druck im Spiel ist. Eine weitere Möglichkeit, den Transport und/oder die Verpressung zu sabotieren, bestünde darin, eine Ladung CO_2 mit korrosiven Stoffen zu verunreinigen. Denkbar wären auch Cyberangriffe auf die digitale Infrastruktur, die für den Betrieb und die Überwachung von CO_2-Speicheranlagen erforderlich ist.

Auf der Basis der EU-Definition kritischer Infrastrukturen (siehe Einleitung) ließe sich argumentieren, dass der mit der Sabotage von CO_2-Infrastrukturen verbundene wirtschaftliche Schaden diese Infrastrukturen als »kritisch« qualifiziert. Wirtschaftlicher Schaden könnte etwa dann entstehen, wenn EU-Mitgliedstaaten bzw. -Unternehmen infolge eines Angriffs auf eine CO_2-Pipeline oder eine Injektionsstelle hohe Ausgleichszahlungen für das dabei entwichene — und damit faktisch emittierte — CO_2 aufbringen müssten. Oder wenn industrielle Produktionsprozesse mit »schwer vermeidbaren« Emissionen (etwa bei Stahl oder Zement) eingestellt werden müssten, weil die Schäden an der Infrastruktur den Transport und die Speicherung des abgeschiedenen CO_2 für einige Zeit unmöglich machen würden. Das gleiche Szenario wäre auch für die »blaue« Wasserstoffproduktion auf Erdgasbasis denkbar.

a Mustafa Babiker u. a., »Cross-sectoral Perspectives«, in: IPCC, *Climate Change 2022: Mitigation of Climate Change. Contribution of Working Group III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*, Cambridge/New York: Cambridge University Press, 2022, S. 1245—1354.

b Miranda Böttcher/Felix Schenuit/Oliver Geden, *Die Rolle des Ozeans in der Klimapolitik*, Berlin: Stiftung Wissenschaft und Politik, März 2023 (SWP-Aktuell 20/2023), doi: 10.18449/2023A20; Felix Schenuit/Miranda Böttcher/Oliver Geden, »*Carbon Management«: Chancen und Risiken für ambitionierte Klimapolitik*, Berlin: Stiftung Wissenschaft und Politik, Mai 2023 (SWP-Aktuell 30/2023), doi: 10.18449/2023A30.

c Zum Beispiel ein vom BMBF gefördertes Projekt zur Erforschung des Potentials für die CO_2-Speicherung unter der Nordsee: GEOSTOR, <https://geostor.cdrmare.de/> (eingesehen am 28.9.2023).

Mittel- bis langfristige Veränderungen werden zum anderen aber auch von politischen Entscheidungen geprägt sein: Ganz unmittelbar betrifft dies die Handelsrouten für die Nahrungsversorgung und entsprechend die Frage, welche Seewege und Häfen in Zukunft besonders kritisch sein werden. Nicht zuletzt wird sich hier aber auch zeigen, ob es politisch gelingt, Maßnahmen zum Schutz kritischer Infrastrukturen zu implementieren.

Schließlich wird zu beobachten sein, ob sich die maritimen Ambitionen Chinas zu einer Gefahr für die deutsche und die europäische Infrastruktur im maritimen Raum entwickeln. Die Beteiligung chinesischer Unternehmen am Betrieb europäischer Häfen illustriert, dass China hier Europa durchaus im Blick hat. Neben solchen staatlichen Akteuren gilt es mittel- bis langfristig zudem im Blick zu behalten, wie sich die Strategien nichtstaatlicher Akteure im Spek-

trum von terroristischen Gruppierungen bis hin zu modernen Formen der Piraterie weiterentwickeln. Immerhin war man noch vor einigen Jahren überzeugt, dass gerade von diesen Akteuren die größte Bedrohung für kritische Infrastrukturen ausgeht.

Zivile und militärische Maßnahmen zum Schutz europäischer maritimer Infrastrukturen

Die Analyse der einzelnen Sektoren zeigt, dass sich die Bedeutung maritimer Infrastrukturen nur sinnvoll im kontinentalen Maßstab erfassen lässt: Wegen des hohen Grads der Vernetzung innerhalb Europas können Infrastrukturen an der Küste eines Landes von besonderer Bedeutung für ganz Europa sein. Das gilt insbesondere für ein Land wie Deutschland, das zentral in Europa gelegen ist und nur über eine vergleichsweise kurze eigene Küstenlinie verfügt.

Darum bietet die europäische Ebene aus deutscher Sicht den wichtigsten Ansatzpunkt, um die Sicherheit maritimer kritischer Infrastrukturen zu erhöhen. Wie der Karte auf S. 81 zu entnehmen ist, stechen dabei einige Räume im unmittelbaren Umfeld Europas besonders hervor, weil es dort jeweils zu einer Verdichtung kritischer Infrastrukturen kommt.

Für deren Schutz bietet sich eine Kombination ziviler und militärischer Maßnahmen an.[2]

Diversität und Resilienz

Der Schutz kritischer Infrastrukturen verlangt einen kontinuierlich hohen Einsatz von Ressourcen und kann dabei doch nie perfekt sein. Dies gilt insbesondere mit Blick auf die besonderen Eigenschaften des maritimen Raums, seine Weite und bisweilen noch immer schwere Zugänglichkeit. Eine attraktive Alternative zum aufwendigen Schutz kritischer Infrastrukturen besteht folglich darin, durch Redundanz und Varianz die Bedeutung und damit letztlich auch die Kritikalität einzelner Anlagen zu reduzieren. Gerade hier ist eine gesamteuropäische oder zumindest kontinental abgestimmte Vorgehensweise notwendig.

Das betrifft im Küstenbereich die Häfen und weitere Infrastrukturen wie Kabelanlandestellen oder Gasterminals. Je mehr etwa die maritime Struktur auf verschiedene Orte verteilt ist, umso geringer sind die Folgen von Ausfällen einzelner Anlagen bzw., positiv gewendet, umso höher ist die Resilienz des Gesamtsystems, also dessen Fähigkeit, auf Schocks flexibel zu reagieren und möglichst schnell wieder einsatzbereit zu sein. Neben der räumlichen Verteilung gehören zur Resilienz auch der Aufbau und das Vorhalten von Fähigkeiten zur Reparatur ausgefallener Anlagen. Die fortgeschrittene Integration des europäischen Binnenmarktes macht es dabei notwendig, eine solche Politik der gezielten Diversifizierung und des Aufbaus von Resilienz europäisch anzulegen.

Diversifizierung und Resilienz sind allerdings mit Kosten verbunden, die unter Umständen jene für Maßnahmen zum Schutz kritischer Infrastrukturen übersteigen, auf jeden Fall aber schwer mit der kurz- bis mittelfristig angelegten Effizienzlogik privater Unternehmen zu vereinbaren sind. Um das öffentliche Interesse an einer durch Diversifizierung sicheren Infrastruktur zur Geltung zu bringen, bedarf es daher öffentlicher Interventionen, nicht zuletzt in Form von finanziellen Anreizen. Diese sollten so gestaltet werden, dass sie den marktwirtschaftlichen Wettbewerb nicht zu stark verzerren. Trotz der spezifischen Eigenheiten der jeweiligen Märkte bietet hierfür der sektorenübergreifende Blick einen guten Ausgangspunkt. Denn letztlich stellt sich die grundsätzliche Frage nach der Balance zwischen öffentlichen Sicherheitsinteressen und privatem Effizienz- und Profitstreben ganz ähnlich auch in Bezug auf Energie, Ernährung und Kommunikation.

Jenseits der übergreifenden regulatorischen Fragen lassen sich zudem in operativer Hinsicht Synergien nutzen. Dies betrifft etwa den europaweiten Informationsaustausch, möglicherweise aber auch das von den europäischen Staaten gemeinsam finanzierte Vorhalten von zivilen Fähigkeiten zur Reparatur maritimer Infrastrukturen.

Nicht zuletzt erscheint es sinnvoll, als Teil einer Diversifizierungsstrategie auch die Eigentümerstrukturen der Betreiber maritimer kritischer Infrastrukturen sektorenübergreifend und im europäischen Maßstab zu betrachten.[3] Praktisch relevant wird dies insbesondere beim Investitionsscreening, bei dem problematische Marktkonzentrationen möglicherweise erst dann sichtbar werden, wenn der Blick auf

2 Vgl. hierzu die Beiträge von Raphael Bossong, S. 71ff, und Göran Swistek, S. 61ff, in dieser Studie.

3 Bundesregierung, *China-Strategie der Bundesregierung*, Berlin, Juli 2023, S. 40, <https://www.auswaertiges-amt.de/blob/2608578/810fdade376b1467f20bdb697b2acd58/china-strategie-data.pdf> (eingesehen am 4.9.2023).

den gesamten Kontinent mit der gleichzeitigen Analyse verschiedener Sektoren kombiniert wird.

Ergänzende militärische Maßnahmen

Wenn zu befürchten ist, dass Staaten gezielt maritime Infrastrukturen angreifen könnten und eine weitere Diversifizierung nicht möglich ist, reichen rein zivile Schutzmaßnahmen nicht mehr aus. Um hier angemessen reagieren zu können, bedarf es in einzelnen Fällen des ergänzenden Schutzes durch militärische Maßnahmen. Im Wesentlichen zielen diese auf Abschreckung. Eine möglichst umfassende Aufklärung gegnerischer Aktivitäten sowie eine verstärkte Präsenz signalisieren die Fähigkeit und die Bereitschaft zu militärischem Handeln. Im besten Fall gelingt es damit, das Kalkül potentieller Angreifer so zu verändern, dass sie von Angriffen absehen.

Das größte Hindernis bildet in diesem Zusammenhang die enorme räumliche Ausdehnung maritimer Infrastrukturen. So dürfte es kaum möglich sein, sämtliche als kritisch verstandene maritime Infrastrukturen dauerhaft militärisch zu schützen. Abgesehen vom Schutz einzelner Anlagen bei konkreten Hinweisen auf Bedrohungen erscheint es daher sinnvoll, den kontinuierlichen Schutz auf jene Orte an den Küsten Europas zu konzentrieren, an denen mehrere kritische Infrastrukturen zusammenkommen.

Darüber hinaus setzen die Vorgaben des Seerechts[4] einem aktiven und vor allem präventiven Eingreifen enge Grenzen. Diese ergeben sich aus dem besonderen Wert, den das Seerecht der freien Durchfahrt auf Hoher See einräumt, sowie aus den unterschiedlichen Zuständigkeiten in den verschiedenen Seegebieten von der Küste über die AWZ bis zur Hohen See. Hinzu kommen im Fall Deutschlands die verfassungsrechtlichen Hürden für einen Einsatz der Bundeswehr im Innern, also auch im Küstenbereich. Um den Schutz maritimer kritischer Infrastrukturen an den Küsten Europas militärisch zu ergänzen, sind daher schon im Vorfeld solcher Aktivitäten die rechtlichen Voraussetzungen für eine effektive Zusammenarbeit zwischen militärischen Einheiten und zivilen Sicherheitsbehörden zu schaffen.

Den wichtigsten Bezugsrahmen bildet für Europa dabei bislang noch immer die Nato. Die Allianz hat etwa im Februar 2023 ein Zentrum zum Schutz kritischer Infrastruktur auf dem Meeresboden eingerichtet, das vom Generalleutnant a. D. Hans-Werner Wiermann geleitet wird.[5] Die Nato kann insbesondere auch den Rahmen bieten, um im europäischen Umfeld mit Staaten wie Großbritannien und Norwegen zusammenzuarbeiten und um den Austausch zu diesen Fragen mit den USA zu intensivieren.[6]

Diplomatische Ansätze zum Schutz globaler Chokepoints

Die für Deutschland und Europa bedeutsamen maritimen Infrastrukturen sind eingebunden in ein globales Netz. Wie beschrieben, liegen einige Verdichtungen von kritischen Infrastrukturen in weiter Entfernung zu den europäischen Küsten, wie etwa der Suezkanal oder die Straße von Malakka. Störungen an Orten wie diesen können sich auch in Deutschland und Europa negativ bemerkbar machen. Auch wenn hier die direkten Handlungsmöglichkeiten deutlich eingeschränkter sind, liegt es im Interesse Europas, Formen der internationalen Kooperation zu finden, die zum Schutz dieser weiter entfernten Infrastrukturen beitragen. Grundlage hierfür ist der strategische Austausch mit relevanten Partnern in den entsprechenden Regionen im Rahmen der bestehenden diplomatischen Beziehungen. Eine solche politisch-strategische Verständigung kann den Rahmen für verstärkten Informationsaustausch oder sogar weiterreichende Formen der militärischen Kooperation bilden.[7]

Neben der militärischen Komponente bildet die internationale Entwicklungszusammenarbeit einen weiteren Ansatzpunkt. In ihrem Rahmen ließen sich etwa gezielt Programme auflegen, die es den Partnerländern ermöglichen, die Sicherheit maritimer Infrastrukturen in ihren Gewässern zu erhöhen. Dies würde unmittelbar diesen Ländern zugutekommen, zumindest in einigen Fällen aber auch einen Beitrag dazu leisten, den Schutz globaler Chokepoints zu ver-

4 Vgl. den Beitrag von Christian Schaller in dieser Studie, S. 14ff.

5 »NATO Stands Up Undersea Infrastructure Coordination Cell«, Brüssel, 15.2.2023, <https://www.nato.int/cps/en/natohq/news_211919.htm> (eingesehen am 25.9.2023).

6 Amanda Kraley, »Securing the Deep: Undersea Cables and National Security«, *49Security*, 12.4.2023, <https://fournine security.de/en/2023/04/12/securing-the-deep-undersea-cables-and-national-security> (eingesehen am 25.9.2023).

7 Ein Beispiel für den institutionalisierten globalen Informationsaustausch zu Fragen maritimer Sicherheit ist das in Singapur angesiedelte »Information Fusion Center«, an dem sich auch Deutschland beteiligt, <https://www.ifc.org.sg>.

bessern. Außerdem könnte beispielsweise das EU-Programm Global Gateway in diesem Sinne noch expliziter auf solche Infrastrukturen von globaler Bedeutung ausgerichtet werden.

Deutschlands nationaler Beitrag

Schließlich stellt die Debatte um maritime kritische Infrastrukturen auch für die deutsche Politik eine Herausforderung dar, und dies in mindestens drei Hinsichten: Konzeptionell und strategisch gilt es zu klären, wie Deutschland in diesem Bereich seine Interessen und Ziele versteht. Dabei geht es, wie beschrieben, insbesondere darum, über die eigenen Küstengebiete auch die Bedeutung maritimer Infrastrukturen rund um Europa in den Blick zu nehmen. Konkret führt dies zu der Frage, welchen Beitrag Deutschland zu einem kontinentaleuropäisch angelegten Schutz maritimer Infrastrukturen leisten kann. Die im Sommer 2023 veröffentlichte nationale Sicherheitsstrategie bietet hierfür einen Ausgangspunkt, indem sie das Thema maritimer kritischer Infrastrukturen explizit aufgreift — allerdings noch ohne vertiefte strategische Einordnung.[8] Neben dem KRITIS-Dachgesetz wird es auch bei der geplanten nationalen Hafenstrategie darauf ankommen, ein konsistentes strategisches Verständnis zu entwickeln.[9]

Im Zuge der strategischen Klärung stellen sich für die deutsche Politik zudem rechtliche Fragen der Zuständigkeiten. Sie betreffen das Verhältnis von öffentlichen Stellen und privaten Betreibern, das Zusammenspiel von Bundes- und Landesbehörden sowie die verfassungsrechtlich heikle Option einer Beteiligung der Marine am Schutz ziviler Infrastrukturen in Friedenszeiten.[10]

Verbunden mit den rechtlichen Fragen sind schließlich auch operative Fragen, nicht zuletzt mit Blick auf die materielle Ausstattung der zuständigen Stellen und deren Koordinierung. Hier gilt es etwa zu klären, ob und gegebenenfalls wie das Zentrum für maritime Sicherheit in Cuxhaven aufgewertet werden könnte, um verstärkt auch den Schutz maritimer kritischer Infrastrukturen zu begleiten.

8 Bundesregierung, *Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie*, Berlin, 14.6.2023, S. 25, <https://www.bmvg.de/resource/blob/5636374/38287252c5442b786ac5d0036ebb237b/nationale-sicherheitsstrategie-data.pdf> (eingesehen am 4.9.2023).

9 Bundesministerium für Digitales und Verkehr, »Die Nationale Hafenstrategie«, 7.7.2023, <https://bmdv.bund.de/DE/Themen/Mobilitaet/Wasser/Hafenstrategie/hafenstrategie.html> (eingesehen am 19.9.2023).

10 Vgl. den Beitrag von Göran Swistek in dieser Studie, S. 61ff.

Anhang

Abkürzungen

4E	Essential Elements of European Escort
ABC	Atomar, Biologisch, Chemisch
AGEB	Arbeitsgemeinschaft Energiebilanzen
AIS	Automatic Identification System (Automatisches Identifikationssystem)
AMIS	Agricultural Market Information System
AWG	Außenwirtschaftsgesetz
AWV	Außenwirtschaftsverordnung
AWZ	Ausschließliche Wirtschaftszone
BBC	British Broadcasting Corporation
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BECCS	Bio-Energy with Carbon Capture and Storage
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern und für Heimat
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik (Bonn)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
CCS	Carbon Capture and Storage
CDR	Carbon Dioxide Removal
CERG	Critical Entities Resilience Group
CER-Richtlinie	Critical Entities Resilience Directive (EU-Richtlinie über die Resilienz kritischer Einrichtungen)
CISE	Common Information Sharing Environment (Gemeinsamer Informationsraum)
CO_2	Kohlendioxid
CSIP	Critical Seabed Infrastructure Protection (Projekt)
DACCS	Direct Air Carbon Capture and Storage
EDA	European Defence Agency (Europäische Verteidigungsagentur)
EFCA	European Fishery Control Agency (Europäische Fischereiaufsichtsagentur)
EFSCM	European Food Security Crisis preparedness and response mechanism (Europäischer Mechanismus zur Krisenvorsorge und Krisenreaktion im Bereich der Ernährungssicherheit)
EMSA	European Maritime Safety Agency (Europäische Agentur für die Sicherheit des Seeverkehrs)
ENISA	European Union Agency for Cybersecurity (Agentur der Europäischen Union für Cybersicherheit)
EPC	European Patrol Corvette
ERCC	Emergency Response Coordination Centre (Zentrum für die Koordination von Notfallmaßnahmen)
EU	Europäische Union
EUMSS	European Union Maritime Security Strategy (Maritime Sicherheitsstrategie der Europäischen Union)
Eurosur	European Border Surveillance System (Europäisches Grenzkontrollsystem)
eVA	enhanced Vigilance Activities
EWG	Europäische Wirtschaftsgemeinschaft
EWI	Energiewirtschaftliches Institut an der Universität zu Köln
EWR	Europäischer Wirtschaftsraum
FAO	Food and Agriculture Organization (Ernährungs- und Landwirtschaftsorganisation der Vereinten Nationen)
Frontex	Europäische Agentur für die Grenz- und Küstenwache
G7	Gruppe der Sieben
G20	Gruppe der Zwanzig
GATT	General Agreement on Tariffs and Trade (Allgemeines Zoll- und Handelsabkommen)
GCHQ	Government Communications Headquarters
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
GW	Gigawatt
ICPC	International Cable Protection Committee
ICPR	Integrated Political Crisis Response
IEA	International Energy Agency (Internationale Energieagentur)
IEEFA	Institute for Energy Economics and Financial Analysis (Lakewood, OH)
IRENA	International Renewable Energy Agency
ISA	International Seabed Authority (Internationale Meeresbodenbehörde)
IT	Informationstechnologie
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
LNG	Liquefied Natural Gas (Flüssigerdgas)
MARSUR	Maritime Surveillance Project
MROSS	Multi-Role Ocean Surveillance Ships
M-SASV	Medium size Semi-Autonomous Surface Vehicle
Nato	North Atlantic Treaty Organization (Nordatlantische Vertragsorganisation)
NFM	New Force Model

NIS-2-Richtlinie	Network and Information Security Directive (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union)
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
PESCO	Permanent Structured Cooperation (Ständige Strukturierte Zusammenarbeit)
PRC	People's Republic of China (Volksrepublik China)
SatCen	Satellitenzentrum der Europäischen Union
SLOC	Sea Lines of Communication (Seeverbindungslinien)
sm	Seemeilen
SMEI	Single Market Emergency Instrument (Notfallinstrument für den Binnenmarkt)
SRÜ	Seerechtsübereinkommen
Tbps	Terabit pro Sekunde
UMS	Upgrade of Maritime Surveillance
UN	United Nations (Vereinte Nationen)
ÜNB	Übertragungsnetzbetreiber
UNCLOS (SRÜ)	United Nations Convention on the Law of the Sea (Seerechtsübereinkommen der Vereinten Nationen)
UNCTAD	United Nations Conference on Trade and Development
UNTS	United Nations Treaty Series (Vertragssammlung der Vereinten Nationen)
WTO	World Trade Organization (Welthandelsorganisation)

Die Autorinnen und Autoren

Dr. Raphael Bossong
Stellvertretender Leiter der Forschungsgruppe
EU/Europa

Dr. Miranda Böttcher
Wissenschaftlerin in der Forschungsgruppe
EU/Europa

Dr. Oliver Geden
Senior Fellow in der Forschungsgruppe EU/Europa

Dr. Jacopo Maria Pepe
Wissenschaftler in der Forschungsgruppe
Globale Fragen

Dr. agr. Bettina Rudloff
Wissenschaftlerin in der Forschungsgruppe
EU/Europa

Dr. Christian Schaller
Wissenschaftler in der Forschungsgruppe
Globale Fragen

Fregattenkapitän Göran Swistek
Bis Ende 2023 Gastwissenschaftler in der Forschungsgruppe Sicherheitspolitik

Dr. Daniel Voelsen
Leiter der Forschungsgruppe Globale Fragen

Lisa Voigt
Forschungsassistentin der Forschungsgruppe
Globale Fragen