Studies in International Law of the Sea and Maritime Law
Internationales Seerecht und Seehandelsrecht 18

Katharina Reiling | Till Markus (Hrsg.)

Rechtsfragen zur Resilienz maritimer Infrastrukturen

Nomos

Studies in International Law of the Sea and Maritime Law
Internationales Seerecht und Seehandelsrecht

Herausgegeben von

Prof. Dr. Doris König
Prof. Dr. Nele Matz-Lück
Prof. Dr. Alexander Proelß
Prof. Dr. Wolfgang Wurmnest

Band 18

Katharina Reiling | Till Markus (Hrsg.)

Rechtsfragen zur Resilienz maritimer Infrastrukturen

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-3039-2
ISBN (ePDF): 978-3-7489-5349-4

DOI: https://doi.org/10.5771/9783748953494

Onlineversion
Nomos eLibrary

Vorwort

Der vorliegende Band publiziert die Ergebnisse der 7. Bremer Konferenz zum Maritimen Recht, die am 27. Oktober 2023 in den Räumlichkeiten der Bremer Handelskammer stattfand. Thema der Konferenz war die Resilienz der maritimen Infrastrukturen. Vor dem Hintergrund aktueller Herausforderungen widmete sich die Konferenz der Frage, was die (Krisen)Resilienz maritimer Infrastrukturen ausmacht und mit welchen Instrumenten sie gestärkt werden kann. Antworten darauf sollten Referate aus der Wissenschaft und aus der Praxis liefern. Die Ergebnisse der Konferenz wurden im Nachhinein durch Beiträge ergänzt und abgerundet, die Aspekte des Themas beleuchten, die auf der Konferenz nur am Rande behandelt werden konnten.

Die Resilienz maritimer Infrastrukturen ist ein junges und höchst dynamisches Forschungsfeld. Der Sammelband versteht sich vor diesem Hintergrund im Kern als Impuls für weitere Forschungsanstrengungen.

Die Herausgeber danken den Autoren der Beiträge herzlich für ihre Bereitschaft zur Mitwirkung an der Konferenz und diesem Sammelband. Besonderer Dank gilt der Manfred und Ursula Fluß-Stiftung für die finanzielle Unterstützung dieser Veröffentlichung. Des Weiteren danken wir dem Bremer Rhederverein, der Handelskammer Bremen sowie dem Forschungsverbund für Maritimes Recht für die vielfältige Unterstützung bei der Organisation der 7. Bremer Konferenz zum Maritimen Recht. Schließlich möchten wir uns bei den Herausgeberinnen und Herausgebern für die Aufnahme des Werks in die Schriftenreihe Internationales Seerecht und Seehandelsrecht ganz herzlich bedanken.

Bremen, Januar 2025 *Till Markus* und *Katharina Reiling*

Inhaltsverzeichnis

Einleitung: Rechtsfragen der Resilienz maritimer Infrastrukturen

Katharina Reiling und Till Markus

Maritime Infrastrukturen sind für das Funktionieren unserer Wirtschaft und die Versorgung unserer Gesellschaft von entscheidender Bedeutung. Sie können daher als Grundfeste unseres Staates betrachtet werden. Zugleich ist das Netz maritimer Infrastrukturen Ausdruck weltweiter Wertschöpfung und Voraussetzung der Globalisierung. In den letzten Jahren haben der Angriffskrieg Russlands auf die Ukraine, aber auch die COVID-19-Pandemie sowie die Auswirkungen des Klimawandels indes gezeigt, wie anfällig maritime Infrastrukturen auf Krisenlagen reagieren. Um nur einige Beispiele zu nennen: Die Überlastungen der Häfen und des Seeverkehrs infolge der COVID-19-bedingten Personalengpässe waren gerade überwunden, als im Herbst 2022 Stränge der beiden Gaspipelines Nord Stream 1 und 2 durch mehrere Sprengstoffexplosionen beschädigt und unterbrochen wurden. Indizien wiesen auf einen Sabotageanschlag im Gefolge des Ukrainekonflikts hin. Nur zwei Jahre später hat der Bruch des Ostsee-Datenkabels C-Lion 1 zwischen Deutschland und Finnland erneut einen Sabotageverdacht aufkommen lassen. Neben physischen Angriffen fordern Cyberattacken auf Häfen und Offshore-Windparks Anlagenbetreiber heraus. Beispielsweise wurde 2022 die Deutsche Windtechnik AG, die für die Wartung, Überwachung und die Sicherheit von Dutzenden Windparks zuständig ist, Opfer eines Cyberangriffs. Verantwortlich für den Vorfall sind, so wird vermutet, Russland nahestehende Hacker. Die Auswirkungen des Klimawandels auf maritime Infrastrukturen werden am Beispiel des Panamakanals deutlich, der als eine der wichtigsten Schifffahrtsstraßen der Welt gilt. Aufgrund der abnehmenden Niederschläge in Mittelamerika sah sich die *Panama Canal Authority* im Jahr 2023 gezwungen, den Tiefgang der für die Durchfahrt zugelassenen Schiffe zu reduzieren. Nicht zuletzt sorgte im selben Jahr der Streit um den Einstieg des chinesischen Staatskonzerns COSCO beim Container-Terminal Tollerort des Hamburger Hafenbetreibers HHLA für europaweite Aufmerksamkeit.

Vor diesem Hintergrund wurde in den vergangenen Jahren in der Politik die Forderung nach mehr Resilienz maritimer Infrastrukturen laut. Sie bildet den Gegenstand der 2023 überarbeiteten Strategie der Europäischen

Union zur maritimen Sicherheit (EUMSS) sowie der letzten Nationalen Maritimen Konferenz (13. NMK) der Bundesregierung. Aus juristischer Sicht bleibt allerdings nach wie vor unklar, was die (Krisen)Resilienz maritimer Infrastrukturen ausmacht, insbesondere wie ihr Verhältnis zu den verwandten Anliegen Sicherheit und Risikovorsorge aussieht, welche Rechtsfragen sie aufwirft und mit welchen rechtlichen Instrumenten sie gestärkt werden kann.

Eine zentrale Herausforderung des juristischen Zugriffs auf das Thema bildet die Gemengelage verschiedener Akteure und Normschichten im maritimen Bereich. Gerade der maritime Bereich ist durch ein Zusammentreffen verschiedener Rechtsphären gekennzeichnet, die sich typischerweise dem Zugriff eines Hoheitsträgers entziehen. Darüber hinaus erschwert das Aufkommen hybrider Angriffe auf maritime Infrastrukturen, wie sie auch bei Sabotageakten auf Pipelines vermutet werden, die rechtliche Zuordnung der Verantwortung zu einzelnen Akteuren. Die Stärkung der Resilienz maritimer Infrastrukturen umfasst daher Aspekte des überstaatlichen Rechts, des Verwaltungsrechts und des Privatrechts. Neben der grundsätzlichen Frage nach der Zulässigkeit einzelner Resilienzmaßnahmen spielt das übergreifende Anliegen von mehr Koordination und Kooperation, das auch die EUMSS und die 13. NMK stark machen, eine zentrale Rolle.

Diesem Konvolut von Gegenständen und Rechtsfragen widmete sich die 7. Bremer Konferenz des Forschungsverbundes für Maritimes Recht im Oktober 2023. Das Ziel des Forschungsverbunds besteht darin, die wissenschaftliche und praktische Expertise im Nordwesten zu maritimen Angelegenheiten zu bündeln und ihr einen institutionellen Rahmen zu geben. Als Forum des Austauschs dienen in erster Linie die alle zwei Jahre stattfindenden Bremer Konferenzen zum Maritimen Recht. Hauptanliegen der 7. Konferenz war es, einerseits zentrale Rechtsfragen der Resilienz maritimer Infrastrukturen zu vertiefen und diese andererseits in einen interdisziplinären Kontext einzubinden.

Die Erträge der 7. Konferenz, die im Nachgang um weitere Erkenntnisse ergänzt wurden, werden in diesem Sammelband zusammengeführt. Den Auftakt macht ein Beitrag von Dr. Ing. Frank Sill Torres vom Institut für den Schutz maritimer Infrastrukturen in Bremerhaven, das Teil des Deutschen Zentrums für Luft- und Raumfahrt ist. Er führt aus einer nicht-juristischen Perspektive in das Thema der Resilienz maritimer Infrastrukturen ein und diskutiert Möglichkeiten der Erhöhung dieser Resilienz, die von multidimensionaler Überwachung und Situationsbewusstsein bis hin zu Schutzmaßnahmen und systemischen Ansätzen reichen. Er betont

die Unterscheidung von Resilienz und Vorsorge und mahnt an, Resilienzmaßnahmen umfassend und ganzheitlich zu betrachten und umzusetzen, um eine nachhaltige Sicherheit und Widerstandsfähigkeit der maritimen Infrastrukturen zu gewährleisten.

Der erste Themenblock widmet sich der Resilienz von Offshorekabeln und sonstigen Einrichtungen auf See. Prof. Dr. Dr. h. c. mult. Peter Ehlers analysiert die Möglichkeiten des Völkerrechts und des deutschen Rechts zum Schutz von Einrichtungen auf See. Er kommt zum ernüchternden Ergebnis eines „rechtlichen Seenebels". Insbesondere auf nationaler Ebene sei das Ordnungsrecht auf See unvollkommen und inkohärent geregelt, was er historisch erklärt. Zumindest für den Bereich der deutschen AWZ fordert er daher eine Regelung durch ein in sich stimmiges Gesetz. Dr. Michael Stadermann, ebenfalls vom Institut für den Schutz maritimer Infrastrukturen in Bremerhaven, analysiert im Anschluss die völkerrechtlichen Hindernisse insbesondere im UN-Seerechtsübereinkommen und in der UN-Charta für einen effektiven Schutz von Datenkabeln in der Hohen See und identifiziert Lücken im geltenden internationalen Rechtsrahmen.

In einem zweiten Schritt weitet sich die Perspektive und der Blick wendet sich auch der maritimen Infrastruktur an Land zu, sprich den Hafenanlagen. Prof. Dr. Christian Tietje von der Martin-Luther-Universität Halle-Wittenberg und Dr. Philipp Reinhold von Universität des Saarlandes analysieren aus Anlass des umstrittenen Einstiegs des chinesischen Schiffskonzerns COSCO im Hamburger Hafen das deutsche und europäische Investitionskontrollrecht im Bereich maritimer Infrastrukturen. Sie kommen zum Ergebnis, dass Schutzlücken in diesem Bereich – von einzelnen Mitgliedstaaten abgesehen – eher innerhalb der behördlichen Praxis bestehen und weniger den Anwendungsbereich des Investitionskontrollrechts betreffen. Prof. Dr. Katharina Reiling von der Universität Bremen adressiert hingegen den Schutz von Seehäfen vor Cyberattacken. Ihre Kernthese lautet, dass sich die Herstellung von Cyberresilienz in besonderem Maße als ein Problem der Orchestrierung erweist, was sich im regulatorischen Zugriff widerspiegelt. Unter Orchestrierung versteht sie in Anlehnung an die Global Governance-Forschung die Lenkung internationalisierter Regelungsstrukturen ohne zentralen Akteur. Sie zeigt Perspektiven einer internationalisierten Cyberresilienz auf, indem ausgehend von dem Konzept der Orchestrierung zentrale Rechtsinstrumente und -prinzipien benannt werden, um diese zu stärken und abzusichern.

Abschließend nimmt Dr. Moritz Brake von der Rheinischen Friedrich-Wilhelms-Universität Bonn eine gesamtstrategische Bewertung der aktuel-

len Bedrohungslage für maritime Infrastrukturen vor. Maritime Sicherheit erfordere die Zusammenführung ressortübergreifender Informationen und Handlungsmöglichkeiten in einem Ansatz der „integrierten Sicherheit". Um Lücken in der Sicherheitsarchitektur zu schließen, brauche es klare Verantwortlichkeiten, einheitliche Führung, koordinierten zivilen und militärischen Fähigkeitsaufbau und nicht zuletzt eine Anpassung des Rechtsrahmens.

Resilienz maritimer Kritischer Infrastrukturen

Dr.-Ing. habil. Frank Sill Torres[*]

Eine größere Anzahl maritimer Infrastrukturen sind für die Versorgung und das Wohlergehen der Bevölkerung von wesentlicher Bedeutung und gelten daher aus Sicht des Gesetzgebers als Kritische Infrastruktur. Angesichts vielfältiger Bedrohungen wird die Resilienz dieser Systeme – die Fähigkeit, Störereignissen zu widerstehen und sich schnell zu erholen – zunehmend relevant. Der vorliegende Beitrag diskutiert Maßnahmen zur Verbesserung der Resilienz dieser Infrastrukturen.

A. Einleitung

Die Bedeutung maritimer Infrastrukturen für Deutschland ist vielseitig und teils essenziell. Als eine führende Exportnation spielt der Handel über See eine wesentliche Rolle für die deutsche Wirtschaft sowie die Weltwirtschaft insgesamt. Etwa 80 % des globalen Handelsvolumens werden über den Seeweg abgewickelt. Dabei erreichte der Exportwert der Bundesrepublik Deutschland im Jahr 2021 1.375 Milliarden Euro, während der Importwert 1.203 Milliarden Euro betrug[1]. Im Jahr 2023 wurden rund 270 Millionen Tonnen Güter mit einem erheblichen Volumen über das Meer verschifft, was einen wesentlichen Anteil des deutschen Handelsvolumens darstellt[2]. In diesem Kontext sind nicht nur die Häfen, sondern auch wichtige Schiffswege wie der Nord-Ostsee-Kanal von zentraler Bedeutung. Neben der Funktion als Handelsroute ist die maritime Infrastruktur auch wichtiger Teil der Energieversorgung Deutschlands. Ein signifikanter Anteil der Energieproduktion wird durch Offshore-Windparks gewährleistet. Deren ins deutsche Stromnetz einspeisende Anlagen wiesen im Jahr 2022 eine

* Der Verfasser ist Institutsdirektor (komm.) am Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR), Institut für den Schutz maritimer Infrastrukturen in Bremerhaven.

1 Marinekommando, Jahresbericht 2022 – Fakten und Zahlen zur maritimen Abhängigkeit der Bundesrepublik Deutschland, Hrsg. Marinekommando Rostock, S. 147.

2 Statistisches Bundesamt, Seeverkehr 2023, Wiesbaden.

Nennleistung von rund 8,1 Gigawatt auf, was etwa 4 % der Bruttostromerzeugung Deutschlands entsprach[3]. Die Ausbauziele der Bundesregierung sehen bis 2045 eine Erhöhung der Leistung auf mindestens 70 Gigawatt vor, was mehr als 25 % der gesamten Bruttostromerzeugung ausmachen würde[4]. Zudem wird ein erheblicher Anteil des Erdgasverbrauchs über die Nordseepipelines importiert; im Jahr 2022 betrug dieser Anteil etwa 56 % des gesamten Erdgasverbrauchs in Deutschland[5]. Auch im Bereich der digitalen Infrastruktur sind maritime Systeme unverzichtbar. So werden über 95 % des weltweiten Datenverkehrs über Unterseekabel abgewickelt[6].

Aktuelle Ereignisse wie die Angriffe auf Nord Stream und den Baltic Connector verdeutlichen jedoch, dass physische Bedrohungen gegen maritime Infrastrukturen nicht nur theoretischer Natur sind, sondern reale und unmittelbare Risiken darstellen[7]. Der Schutz dieser Infrastrukturen ist daher von größter Relevanz für die Bevölkerung und die nationale Sicherheit. Diese Ereignisse zeigen jedoch auch, wie anspruchsvoll und komplex der Schutz dieser Infrastrukturen ist und dass eine 100%ige Sicherheit kaum erreichbar ist.

Aus diesem Grund gewinnt neben der Gefahrenabwehr das Thema Resilienz zunehmend an Bedeutung. Resilienz beschreibt in diesem Kontext die Fähigkeit von Systemen und Organisationen, Störereignissen zu widerstehen bzw. sich daran anzupassen und dabei die Funktionsfähigkeit zu erhalten oder möglichst schnell wiederzuerlangen.

Das Ziel dieses Beitrags ist es, fachfremden Lesern eine Einführung in das Thema Resilienz maritimer Infrastrukturen zu geben. Dazu wird zunächst ein Überblick über maritime Kritische Infrastrukturen präsentiert (B.), gefolgt von einer Diskussion zu den spezifischen Sicherheitsherausforderungen im maritimen Sektor (C.). Anschließend wird eine Einführung in die Resilienz sozio-technischer Systeme gegeben (D.), aus der Ansätze zur Erhöhung der Resilienz abgeleitet werden (E.).

3 Deutsche WindGuard, Status des Offshore-Windenergieausbaus in Deutschland – Jahr 2023, Varel, S. 3.
4 § 1 WindSeeG.
5 *Hilgers/Busch*, Energie und Rohstoff Erdgas: Verfügbarkeit, Engpässe und Alternativen, Angewandte Geowissenschaften, 2022, S. 27.
6 *Gorden/Jones*, Global Communications Infrastructure: Undersea and Beyond, Center for Space Policy and Strategy, 2022, S. 2.
7 *Liebetrau/Bueger,* International Journal of Critical Infrastructure Protection v. 46 2024, 100683 (100683).

B. Maritime Kritische Infrastrukturen

Kritische Infrastrukturen sind Einrichtungen, Systeme oder Teile davon, die für das Funktionieren einer Gesellschaft und ihrer Wirtschaft von entscheidender Bedeutung sind. Ihr Ausfall oder ihre Beeinträchtigung würden erhebliche Auswirkungen auf die öffentliche Sicherheit, das öffentliche und wirtschaftliche Wohl oder die öffentliche Gesundheit haben[8].

In der aktuellen Gesetzgebung zu Kritischen Infrastrukturen (KRITIS) in Deutschland werden acht primäre Sektoren identifiziert, die für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen entscheidend sind[9]. Diese Sektoren umfassen Energieversorgung, Wasserversorgung, Informations- und Kommunikationstechnologie, Finanz- und Versicherungswesen, Lebensmittelversorgung, Transport und Verkehr, Gesundheitswesen sowie Entsorgung. Innerhalb dieser Sektoren stellen die Betreiber spezifischer KRITIS-Anlagen grundlegende Dienstleistungen bereit, um die kontinuierliche Versorgung der Bevölkerung und deren Wohlergehen zu gewährleisten. Wenn ein Betreiber mit seinen Anlagen die in der KRITIS-Verordnung festgelegten, dienstleistungsbezogenen Schwellenwerte überschreitet, werden diese Anlagen gemäß der Verordnung als Kritische Infrastruktur eingestuft, wodurch der Betreiber zum KRITIS-Betreiber wird. Diese Klassifizierung zieht spezifische rechtliche Verpflichtungen nach sich, die unter anderem die Implementierung adäquater Sicherheitsmaßnahmen, die Meldepflicht von sicherheitsrelevanten Vorfällen und die Durchführung regelmäßiger Prüfungen umfassen. Auf den maritimen Bereich übertragen trifft eine solche Einstufung aktuell u. a. auf folgende Infrastrukturarten zu: Seekabel zur Daten- und Stromübertragung, Gaspipelines, Offshore-Windparks und -Konverterstationen, Liquefied-Natural-Gas-Anlagen, Hafenanlagen (z.B. Umschlaganlagen, Leitzentralen, Hafeninformationssystem) und Verkehrsleitzentralen.[10]

C. Bedrohungen und Vulnerabilitäten

Im Folgenden werden die grundsätzlichen Bedrohungen und Vulnerabilitäten maritimer Infrastrukturen überblicksartig vorgestellt.

8 Vgl. 2008/114/EG, Artikel 2
9 Vgl. §2 (10) BSIG
10 *Voelsen,* Maritime kritische Infrastrukturen, SWP-Studie 2024/S 03, 2024, 7.

I. Bedrohungen

Grundsätzlich können Bedrohungen für kritische maritime Infrastrukturen unterteilt werden in Naturgefahren und anthropogene Bedrohungen. Zu den Naturgefahren zählen im maritimen Raum bspw. Sturmfluten, Hochwasser, hoher Wellenschlag, Extremwetter, Blitzschlag oder Seebeben. Vom Menschen ausgehende Bedrohungen können wiederum unterteilt werden in unbeabsichtigte und beabsichtige Bedrohungen. Zu den Ersteren gehören bspw. Arbeitsunfälle und Fehlbedienungen. Das Feld der beabsichtigten anthropogenen Bedrohungen ist ungleich vielfältiger und umfasst Diebstahl, mutwillige Beschädigung, Sabotage, Cyber-Angriffe, Terrorismus und weitere.

II. Vulnerabilitäten

Die Herausforderungen für den Schutz kritischer Infrastrukturen unterscheiden sich im maritimen Raum teils signifikant von denen im terrestrischen Raum. Hierzu gehört insbesondere die räumliche Ausdehnung der zu überwachenden Gebiete. So beträgt die Größe der deutschen Meeresflächen[11] ca. 41.000 km² in der Nordsee und 15.400 km² in der Ostsee, was in etwa der Fläche der deutschen Bundesländer Niedersachsen (47.710 km²) sowie Schleswig-Hollstein (15.804 km²) entspricht. Des Weiteren verfügen auch die Infrastrukturen über eine große Ausbreitung. So können bspw. Offshore Windparks eine Flächengröße von mehr als 100 km² haben, während Pipelines eine Länge von über 1.000 km besitzen können.

Die räumliche Ausdehnung zusammen mit der Tatsache, dass Einsatzkräfte gewöhnlich in Küstennähe bzw. auf Inseln stationiert sind, führt zusätzlich zu langen Interventionszeiten. Diese umfassen bei Luftfahrzeugen oft über 30 min, während bei Wasserfahrzeugen in Stunden gerechnet wird[12]. Dies erschwert maßgeblich eine zeitnahe Reaktion auf bedrohliche Ereignisse.

Ein weiteres Merkmal des Schutzes maritimer Infrastrukturen ist die Multi-Dimensionalität. Das bedeutet, es müssen sowohl die Bereiche Meeresboden (bspw. für Pipelines, Datenkabel), Unterwasser (bspw. für Angriffe durch Unterwasserfahrzeuge), Wasseroberfläche (bspw. für Offshore

11 Jeweils Küstenmeer und Ausschließliche Wirtschaftszone i.S.d. Art. 2, Art. 55 ff. SRÜ

12 Hierbei ist die Vorbereitungszeit der Luftfahrzeuge, welche ebenfalls 30 – 60 min in Anspruch nehmen kann, nicht mit eingerechnet.

Windparks und Offshore Plattformen), Luftraum (bspw. für Angriffe durch bzw. gegen Luftwahrzeuge und Drohnen) und der Cyberraum überwacht und geschützt werden.

Weitere Herausforderungen sind die durch das internationale Seerecht grundsätzlich gewährte freie Zugänglichkeit der Meere sowie die schlechte Attributierbarkeit, welche die Identifikation und Verfolgung von Verantwortlichen für illegale oder schädliche Aktivitäten erschwert.

D. Resilienz

Dieser Abschnitt dient der Einführung in das Thema Resilienz sowie der Betrachtung von Fähigkeiten resilienter Systeme.

I. Begriffsdefinition

Es gibt vielfältige Verständnisse von Resilienz. Dies liegt an der langen Entwicklungsgeschichte des Konzepts[13], konstanten Diskussionen über seine Ausgestaltung, bspw. illustriert durch die unterschiedlichen Ansichten von Holling[14] und Pimm[15], sowie die fortlaufenden Anpassungen des Resilienzverständnisses in verschiedenen Forschungsbereichen wie Ökologie[16], Katastrophenmanagement[17] und dem Schutz von Kritischer Infrastrukturen[18]. Daher unterscheidet sich die genaue Bedeutung von Resilienz je nach Fachgebiet und spezifischem Anwendungsbereich. Zu nennen sind hier beispielsweise die Definitionen zur „seismischen Resilienz in Gemeinden"[19], die Hurrikanresilienz von Stromnetzen[20] oder die „Resilienz" i.S.d. Anpassungsfähigkeit von Städten an den Klimawandel[21]. Grundsätzlich ermöglicht jedoch die Resilienzdefinition des Büros der Vereinten Nationen für Katastrophenvorsorge eine grundlegende und weitakzeptierte An-

13 *Alexander*, in Nat. Hazards Earth Syst. Sci. v. 13 2013, 2707 (2708).
14 *Holling*, Annual Review of Ecology, Evolution, and Systematics v. 4 1973, 1 (3).
15 *Pimm*, Nature v. 307 1984, 321 (324).
16 *Carpenter*, Ecosystems v. 4 2001, 765 (770).
17 *Cutter*, Global Environ. Change v. 18 2018, 598 (600).
18 *Poulin*, *Kane*, Reliability Engineering and System Safety v. 216 2021, 107926 (107928).
19 *Bruneau*, Earthquake Spectra v. 19 2003, 733 (740).
20 *Ouyang/Duenas-Osorio*, Structure Safety v. 48 2014, 15 (18).
21 *Brown*, Environmental Urbanization v. 24 2012, 531 (538).

näherung[22]. Sie definiert Resilienz als „die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, sich rechtzeitig und effizient den Auswirkungen einer Gefährdung widersetzen, diese absorbieren, sich an sie anpassen, sie umwandeln und sich von ihnen erholen zu können. Eine wichtige Voraussetzung dafür ist die Erhaltung und Wiederherstellung ihrer wesentlichen Grundstrukturen und Funktionen durch Risikomanagement".[23]

II. Fähigkeiten resilienter Systeme

Zentrale Aspekte bei der Betrachtung der Resilienz eines Systems sind dessen Fähigkeiten und die Anwendung von Resilienzprinzipien[24]. Letztere umfassen grundlegende Regeln, Richtlinien oder Ziele, die entscheidend sind, um die Entwicklung und Gestaltung resilienter Systeme zu steuern und eine wesentliche Orientierung für die Auswahl effektiver resilienzsteigernder Maßnahmen bieten[25]. In der Fachliteratur gibt es verschiedene Ansichten zu den essenziellen Systemfähigkeiten eines resilienten Systems[26]. Insbesondere im Bereich kritischer Infrastrukturen werden jedoch häufig drei Systemfähigkeiten hervorgehoben, welche im Folgenden beschrieben werden.

1. Absorptionsfähigkeit

Unter Absorbtionsfähigkeit mag man die Fähigkeit eines Systems verstehen, die initialen negativen Effekte einer Störung zu mindern und dennoch funktionsfähig zu bleiben. Diese Fähigkeit dient der Aufrechterhaltung der Systemkontinuität und umfasst Maßnahmen, die entweder automatisch oder mit minimalem Aufwand wirksam werden können. Dies steht im Gegensatz zu Wiederherstellungs- und Anpassungsfähigkeit, die oft spezifische Maßnahmen erfordern. Im Unterschied zu gezielten Schutzmaßnahmen, die für bestimmte Szenarien konzipiert sind, erhöhen Absorptions-

22 *United Nations Office for Disaster Risk Reduction*, Sendai Framework Terminology on Disaster Risk Reduction, 2016.
23 *Bundesregierung*, Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, 2022, 17.
24 *Woods*, Reliability Engineering and System Safety v. 141 2015, 5 (6).
25 *Jackson/Ferris*, Systems Engineering v. 16 2013, 152 (155).
26 *Rehak*, International Journal of Critical Infrastructure Protection v. 25 2019, 125 (130).

maßnahmen die allgemeine Widerstandsfähigkeit eines Systems gegenüber verschiedenen Störungen.

2. Wiederherstellungsfähigkeit

Die Fähigkeit eines Systems, seine Funktionsleistung nach einer Störung rasch zu regenerieren, ist ein zentrales Element vieler Resilienzdefinitionen. Die Wiederherstellungsfähigkeit bezieht sich auf Maßnahmen, die durchgeführt werden, um die Auswirkungen einer Störung rückgängig zu machen. Dazu gehören bspw. der Einsatz von Reparaturteams, die Instandsetzung beschädigter Komponenten unter Verwendung von Ersatzteilen oder die Beschaffung benötigter Teile. Weitere wesentliche Aspekte sind effektive Notfallpläne, kompetente Notfallreaktionen und die effiziente Zuweisung von Personal und Ressourcen.[27]

3. Anpassungsfähigkeit

Unter Anpassungsfähigkeit versteht man weithin die Fähigkeit eines Systems, sich selbst zu modifizieren, um zukünftigen Störungen effektiv zu begegnen. Dies impliziert, dass das System seine aktuellen Praktiken oder Strategien ändert und aus vergangenen Störungen lernt. Zu den Maßnahmen, die die Anpassungsfähigkeit fördern, gehören die Überarbeitung von Plänen, die Modifikation von Verfahren sowie die Implementierung neuer Werkzeuge, Technologien und Schulungen, die zur Optimierung vor der nächsten Krise erforderlich sind. Die Anpassungsfähigkeit eines Systems wird primär durch soziale Faktoren, insbesondere durch menschliche Handlungen, und weniger durch technische Eigenschaften beeinflusst. Ein hochgradig anpassungsfähiges System kann seine Leistung im Vergleich zu vor der Störung entweder steigern oder stabil halten, selbst wenn der Druck auf das System zunimmt. Besonders relevant ist, dass in einem solchen System die Resilienz selbst als Reaktion auf Störungen zunimmt. Im Gegensatz zur Absorptions- und Wiederherstellungsfähigkeit, die sich auf aktuelle Störungen konzentrieren, fokussiert sich die Anpassungsfähigkeit darauf, die Kompetenz des Systems zu erhöhen, zukünftige Herausforderungen zu bewältigen[28]. Darüber hinaus spielt die Anpassungsfähigkeit auch bei

27 *Ouyang,* Structural Safety v. 36 2012, 23 (27).
28 *Rehak*, International Journal of Critical Infrastructure Protection 25 2019, 125, (126).

anhaltenden, intensiven Störungen eine entscheidende Rolle, indem sie das System an neue Bedingungen anpasst.

4. Resilienzprinzipien

Den oben genannten grundlegenden Fähigkeiten resilienter Systeme lassen sich verschiedene Resilienzprinzipien zuordnen, wobei diese Zuordnung nicht immer eindeutig ist. Oft betrifft ein spezifisches Resilienzprinzip nicht ausschließlich eine der drei Systemfähigkeiten. Beispielsweise kann eine modulare Struktur zunächst die Verbreitung initialer Schadensauswirkungen innerhalb eines Systems begrenzen und somit die Absorptionsfähigkeit erhöhen, später jedoch auch den Wiederaufbau des ursprünglichen Leistungsniveaus unterstützen.

Tabelle 1 stellt die Beziehungen zwischen ausgewählten Resilienzprinzipien und den drei Fähigkeiten resilienter Systeme dar.[29] Dabei wird verdeutlicht, wie multifunktionale und interdisziplinäre Ansätze zur Verbesserung der Resilienz beitragen. Verbreitete Resilienzprinzipien sind beispielsweise Diversität, Modularität, Redundanz und Flexibilität. Diese Prinzipien können je nach Kontext und Art des Störereignisses unterschiedliche Rollen spielen. Beispielsweise trägt Diversität zur Anpassungsfähigkeit bei, indem sie eine Vielzahl von Reaktionsmöglichkeiten auf neue Herausforderungen bietet, während Redundanz die Absorptionsfähigkeit durch zusätzliche Kapazitäten stärkt.

29 *Mentges*, International Journal of Disaster Risk Reduction v. 96 2023, 103893 (103912).

Tabelle 1: Der Zusammenhang zwischen Resilienzprinzipien und den drei Systemfähigkeiten (adaptiert).

		Systemfähigkeiten		
		Absorptions-fähigkeit	Wiederherstel-lungsfähigkeit	Anpassungs-fähigkeit
Ausgewählte Resilienzprinzipien	Robustheit	X		
	Redundanz	X		
	Diversität	X	X	X
	Modularität	X	X	
	Situationsbewusstsein	X	X	
	Überwachung	X	X	
	Ressourcenvielfalt	X	X	
	Wiederherstellbarkeit		X	
	Schnelligkeit		X	
	Graduelle Verschlechterung		X	
	Flexibilität	X	X	X
	Vorbereitungsfähigkeit	X	X	X
	Antizipationsvermögen	X	X	X
	Graduelle Erweiterbarkeit	X	X	X

III. Bewertung

Die Bewertung der Resilienz eines Systems ermöglichet die Bestimmung der Notwendigkeit von Anpassungen bzw. die Einschätzung deren Auswirkungen. Hierbei können generell die drei Methodenarten qualitativ, quantitativ und semi-quantitativ unterschieden werden. Qualitative Methoden konzentrieren sich auf das Verstehen sozialer Phänomene aus der Perspektive der beteiligten Akteure und nutzen unstrukturierte oder halbstrukturierte Daten wie Interviews und Beobachtungen, um tiefere Einblicke in menschliches Verhalten und soziale Prozesse zu gewinnen. Quantitative Methoden basieren auf der systematischen Sammlung und Analyse numerischer Daten, mit dem Ziel, Muster, Beziehungen und Kausalitäten zu identifizieren sowie Hypothesen zu testen. Semi-quantitative Methoden kombinieren qualitative und quantitative Ansätze, erfassen Daten, die so-

wohl numerisch als auch beschreibend sein können, und verwenden häufig Skalen oder Rangordnungen, um schwer messbare Daten zu klassifizieren.

Verbreitet sind vor allem semi-quantitative und quantitative Methoden. Beispiele für Ersteres sind Resilience Assessment Grids[30] und Resilienzmatrizen[31]. Resilience Assessment Grids analysieren die zentralen Systemfähigkeiten anhand vorgegebener Kriterien und Skalen. Der Prozess umfasst die Identifikation relevanter Resilienzprinzipien, die Datenerhebung durch Interviews, Umfragen oder Beobachtungen und die Analyse der gesammelten Daten. Dabei werden sogenannte Resilienzprofile erstellt, wobei es sich um eine grafische Darstellung in Form von Spinnendiagrammen handelt, die eine visuelle Bewertung ermöglichen.

Eine Resilienzmatrix organisiert die Systemfähigkeiten in verschiedenen Domänen (z.B. physisch, informationell und kognitiv) über die zeitlichen Phasen einer Störung (z.B. Vorbereitung, Absorption, Erholung und Anpassung). Die Benutzer bewerten das System und seine kritischen Funktionen, indem sie verschiedene Resilienzprinzipien anhand von Indikatoren einschätzen, und tragen diese Werte in normalisierter Form die Resilienzmatrix ein. Abschließend können die entsprechenden Werte aggregiert werden, so dass ein initialer und oberflächlicher Vergleich der Resilienz verschiedener Systeme und Systemkonfigurationen ermöglich wird.

Ein Großteil der quantitativen Methoden zur Resilienzbewertung zielt darauf ab, den zeitlichen Verlauf der Performance des untersuchten Systems bzw. einzelner Systemfunktionen vor, während und nach einer Störung zu quantifizieren[32]. Dies reicht von einer eher simplen Bestimmung des Integrals der Performanz über die Zeit[33] bis hin zu umfangreichen Ansätzen, welche die verschiedenen zeitlichen Phasen formell beschreiben[34]. Andere

30 *Hollnagel*. RAG-the resilience assessment grid. Safety-II in practice: developing the resilience potentials: Routledge, 2017, 50.

31 *Rand/Kurth/Fleming/Linkov*, International Journal of Disaster Risk Reduction v. 42, 2020, 101310 (101312).

32 *Hosseini/Barker/Ramirez-Marquez*, Reliability Engineering and System Safety v. 145 2016, 47, (51).

33 *Zobel*, Int. Conf. on Information Systems for Crisis Response and Management 2010, 1, (3).

34 *Guillouët/Keszöcze, Sill Torres*, Resilience Week 2021, 1 (4).

Ansätze verfolgen eine system-orientierte Sicht und erfassen das Systemverhalten bspw. über Simulationsmodelle[35] oder Fuzzy-Logik.[36]

IV. Vergleich Risiko und Resilienz

Ein zentraler Punkt beim Verständnis von Resilienz liegt in der Unterscheidung zwischen Ansätzen, die Risiken reduzieren, und solchen, die Resilienz aufbauen. Hierbei spielt die Unvorhersehbarkeit von Ereignissen eine maßgebliche Rolle: Risikominderungsstrategien zielen darauf ab, auf vorhersehbare Ereignisse zu reagieren, während Resilienzstrategien darauf fokussieren, ein System so zu stärken, dass es flexibel auf jegliche, auch unerwartete, Situationen reagieren kann[37]. Tatsächlich hat das wachsende Bewusstsein für unvorhersehbare und einzigartige Herausforderungen maßgeblich zur steigenden Bedeutung des Resilienzdenkens in der politischen Diskussion beigetragen[38].

Die unterschiedlichen Schwerpunkte dieser Ansätze bestimmen die verfolgten Strategien. Risikominderungsstrategien lassen sich in Prävention, d.h. die Reduzierung der Eintrittswahrscheinlichkeit schwerwiegender Gefahren, Vermeidung, d.h. die Vermeidung der Aussetzung gegenüber Gefahrenquellen, und Schutz, d.h. die Verringerung der Anfälligkeit von Systemen, unterteilen. Prävention und Vermeidung konzentrieren sich auf vorhersehbare Gefahren, und versuchen die Wahrscheinlichkeit des Eintritts dieser zu verringern. Damit werden beiden nicht zu den resilienzfördernden Strategien gezählt. Im Gegensatz dazu gibt es beim Schutz Überschneidungen mit Resilienzansätzen: In beiden Fällen zielen die jeweiligen Maßnahmen darauf ab, die Auswirkungen von Störereignissen zu verringern, indem Maßnahmen ergriffen werden, die die Systemfähigkeiten stärken[39]. Aus der Risikoperspektive wird gezielt die Verwundbarkeit gegenüber bestimmten Ereignissen reduziert, während aus der Resilienzperspektive die Fähigkeit zur Bewältigung beliebiger Ereignisse im Mittelpunkt steht. Es bleibt festzuhalten, dass Resilienzmaßnahmen, die darauf abzielen, ein Sys-

35 *Niemi/Skobiej/Kulev, Sill Torres*, Reliability Engineering and System Safety v. 242 2024, 109719 (109721).

36 *Gote*, Fuzzy-Logik basierte Methodik zur Vulnerabilitätsbewertung eines Containerterminals, Hochschule, Bremerhaven, 2022, 20.

37 *Park/Sharman/Rao,* MIS Quarterly, v. 39, 2013, 317, (320).

38 *Petersen/Lange/Theocharidou*, Reliability Engineering and System Safety, v. 199, 2020 106872 (106873).

39 *Mentges*, Fn. 30 (103930)

tem gegen unvorhersehbare Störungen zu schützen, gleichzeitig auch den Schutz vor bekannten Risiken erhöhen. Im gleichen Sinne steigern risikozentrierte Schutzmaßnahmen, die auf bestimmte Bedrohungen abzielen, im Allgemeinen auch die Fähigkeit eines Systems, mit unvorhergesehenen Störungen umzugehen. Letztlich wird die Wirksamkeit beider proaktiven Maßnahmen in der Reaktion des Systems auf ein auftretendes Störereignis zusammenwirken.

Der konzeptionelle Unterschied zwischen Risiko- und Resilienzmanagement zeigt sich jedoch in den angewandten Methoden. Das Risikomanagement fokussiert sich auf spezifische Risiken, während das Resilienzmanagement die Aufrechterhaltung und Stärkung der Systemfähigkeiten in den Vordergrund stellt. Trotz ihrer unterschiedlichen Schwerpunkte und Ansätze verfolgen Risikominderung und Resilienzaufbau ein gemeinsames Ziel: die negativen Folgen von Störungen zu minimieren. Kombinierte Maßnahmen, die sowohl Risikominderung als auch Resilienzaufbau integrieren, sind daher besonders effektiv, da sie sowohl bekannte als auch unvorhersehbare Herausforderungen bewältigen, indem sie die Eintrittswahrscheinlichkeit von Risiken reduzieren und gleichzeitig die Fähigkeit zur Reaktion auf diese stärken.

E. Ansätze zur Erhöhung der Resilienz maritimer Kritischer Infrastrukturen

Maßnahmen zur Erhöhung der Resilienz maritimer Kritischer Infrastrukturen gegenüber physischen Bedrohungen orientieren sich an den im vorherigen Kapitel eingeführten Resilienzprinzipien und lassen sich in die Bereiche Multidimensionale Seeraumüberwachung, Lagebewusstsein, Schutzmaßnahmen und systemische Ansätze unterteilen.

I. Multi-dimensionale Seeraumüberwachung

Folgend dem Resilienzprinzip Überwachung bildet die multidimensionale Seeraumüberwachung eine wichtige Säule für eine resiliente maritime Kritische Infrastruktur. Dies beinhaltet eine Mischung aus Sensorsystemen und -plattformen, die der Überwachung aller maritimen Dimensionen (Meeresboden, Unterwasser, Wasseroberfläche, Luftraum, Cyberraum) dienen. Ziel ist es, Objekte, Personen, Umweltparameter (bspw. Wetter, Meeresdaten), Veränderungen an den Komponenten der Infrastrukturen sowie

den Ablauf der Prozess in den Infrastrukturen (bspw. Wartung, Logistik) zu erfassen. Die Sensorsysteme lassen sich grob nach ihrem Einsatzraum einordnen, d.h. Wasseroberfläche/Luftraum, Unterwasser/Meeresboden und Cyberraum.

Im Bereich Wasseroberfläche/Luftraum existiert eine Vielzahl von Sensoren, welche vor allem im elektromagnetischen Spektrum arbeiten[40]. Hierzu gehören optische Sensoren, insbesondere optische Kameras und Lidar-Sensoren, Radar-Systeme, inklusive Over-The-Horizon-Radar und Synthetic Aperture Radar, sowie Hyper- und Multispektrale Sensorsysteme[41]. Ein im maritimen Raum weithin verbreitetes System ist das Automatic-Identification-System, ein automatisches Tracking-System, das in der Schifffahrt zur Identifizierung und Positionsbestimmung von Schiffen verwendet wird. Darüber hinaus werden auch kontextbezogene Informationsquellen verwendet. Hierzu gehören Human-Intelligence, d.h. die Informationsgewinnung durch menschliche Quellen, Signals-Intelligence, d.h. die Fernmelde- und Elektronische Aufklärung, sowie Open-Source-Intelligence, d.h. die Informationsgewinnung aus frei verfügbaren und offenen Quellen[42].

Im Unterwasserbereich sind auf Grund starker Dämpfungseffekte Sensoren aus dem elektromagnetischen Spektrum nur sehr begrenzt einsetzbar[43]. Daher kommt es in diesem Bereich vor allem zum Einsatz akustischer Systeme, insbesondere von Sonar-Systemen[44]. Diese umfassen aktive und passive Sonare, Seitensichtsonare, Fächerecholot und Synthetic-Aperture-Sonar. Von steigender Bedeutung sind Systeme, die Lichtwellenleiterkabel, welche zur Datenkommunikation verwendet werden, als Sensor einsetzen. Hierbei sind vor allem Distributed-Temperature-Sensing- und Distributed-Acoustic-Sensing -Systeme zu nennen[45].

Sensorsysteme zu Überwachung der Bereiche Wasseroberfläche/Luftraum sowie Unterwasser/Meeresboden können entweder fest installiert sein oder auf Sensorplattformen eingesetzt werden. Klassische Plattformen sind im maritimen Bereich Satelliten, bemannte Luftfahrzeuge (bspw. Flugzeuge, Hubschrauber) und bemannte Über- und Unterwasserfahrzeuge.

40 *Briguglio/Crupi*, Journal of Marine Science and Engineering v. 12 2024, 353 (354).
41 *Thombre*, IEEE Transactions on Intelligent Transportation Systems 23.1 2022, 64 (67).
42 *Crosston/Valli*, Cyber-Intelligence, and Security 2017, 68 (70).
43 *Wright,* International Journal on Marine Navigation and Safety of Sea Transportation v. 13 2019, 503 (505).
44 *Blondel/Murton*, Handbook of Seafloor Sonar Imagery, 1997, 5 ff.
45 *Duckworth/Ku.*, Society for Optics and Photonics Conference 2013, 87110G (87112G).

Von zunehmender Bedeutung werden jedoch auch unbemannte Luftfahrzeuge (bspw. Drohnen und High-Altitude Platforms) sowie Über- und Unterwasserfahrzeuge.[46]

II. Lagebewusstsein

Das Lagebewusst folgt den Resilienzprinzipien Situationsbewusstsein und Antizipationsvermögen und umfasst vor allem Lösungen zur Sensordatenfusion und -analyse sowie zur Lagebilderstellung[47]. Ziel ist es, zum einen die Informationen der eingesetzten Sensorsysteme zusammenzuführen und die aktuelle Lage darzustellen. Darüber hinaus sollen durch die automatische Detektion, Klassifizierung und Identifikation von Objekten, weiterführende Informationen gewonnen werden. Hierbei kommt es vor allem zum Einsatz von Methoden des maschinellen Lernens. Dies ermöglicht unteranderem die Erkennung von Anomalien, bspw. untypischen Schiffsverhalten oder auffällige Objekte in der Nähe von Infrastrukturen. Von zunehmender Bedeutung sind antizipative Ansätze, welche eine Prognose darüber liefern, wie sich eine Situation entwickelt und ob es notwendig wird, auf diese Lage reagieren zu müssen.

III. Schutzmaßnahmen

Schutzmaßnahmen folgen im weitesten Sinn dem Resilienzprinzip Robustheit und dienen der Verhinderung eines Störereignisses bzw. der Reduzierung der Auswirkungen eines solchen Ereignisses. Wie in Abschnitt B dargelegt, schränkt die räumliche Ausdehnung im maritimen Raum solche Schutzmaßnahmen signifikant ein, insbesondere im Hinblick auf den proaktiven und reaktiven Einsatz von Sicherheitskräften, welche in vielen Fällen lange Interventionszeiten haben.

Im Falle von Schiffen, welche ein auffälliges Verhalten zeigen, erfolgt gewöhnlich ein Ansprechen per Funk. Durch diese Maßnahme können vor allem anthropogene Bedrohungen abgewendet werden, bei denen die Angreifer unerkannt bleiben möchten, bspw. im Falle von unrechtmäßigen Aktivitäten staatlicher oder privater Akteure (z.B. Spionage oder Diebstahl).

46 *Soldi*, IEEE Aerospace and Electronic Systems Magazine v. 38 2013, 4 (5).
47 *Flenker/Stoppe*, Workshop on Maritime Systems Resilience and Security 2021, 1 (3).

Im maritimen Raum gewinnen semi-automatische und automatische Drohnenabwehrsysteme in den drei Dimensionen Unterwasser, Wasseroberfläche und Luft an Bedeutung[48]. Unterwasserabwehrsysteme schützen vor unbemannten Unterwasserfahrzeugen, die bspw. Kabel und Anlagen angreifen könnten. Auf der Wasseroberfläche und in der Luft bieten Anti-Drohnen-Technologien Schutz vor maritimen Drohnen und Luft-Drohnen, die für Spionage, Sabotage oder Angriffe genutzt werden können. Diese integrierten Systeme ermöglichen die Echtzeit-Erkennung und ggf. Neutralisierung von Bedrohungen.

Eine weitere Maßnahme sind schwimmende Barrieren und Unterwassernetze[49]. Erstere sind kettenartige Strukturen aus Stahl, Beton und anderen Materialien, die über Schäkeln und Drehgelenke miteinander verbunden sind und Schutz vor Booten oder U-Booten bieten. Unterwassernetze, aus haltbarem Stahldraht und am Meeresboden verankert, dienen als physische Barrieren mit Sensoren zur Erkennung von Eindringlingen. Auf Grund der räumlichen Ausdehnung vieler maritimer Infrastrukturen, bspw. Offshore Windparks und Pipelines, sind solche Barrieren jedoch nur begrenzt einsetzbar.

IV. Systemische Ansätze

Systemische Ansätze zur Erhöhung der Resilienz maritimer Systeme gegenüber physischen Bedrohungen umfassen vor allem Maßnahmen mit dem Fokus auf Absorptionsfähigkeit, die im Vorfeld eines Ereignisses relevant sind, sowie auf Wiederherstellungsfähigkeit, die im Nachgang eines erfolgreichen Angriffs von Bedeutung ist. Hierzu gehören vor allem Redundanzmaßnahmen und Reparaturfähigkeiten. Erstere umfassen bspw. die Verlegung mehrere Unterseekabel, wobei eine räumliche Trennung angestrebt werden sollte, oder die redundante Auslegung zentraler Komponenten in Offshore Plattformen, so dass die Auswirkungen eines Ausfalls einzelner Elemente verringert werden können.

Die Reparaturfähigkeit zerstörter Systeme und Komponenten kann durch eine Vielzahl von Maßnahmen gesteigert werden. Bei Unterseekabeln ist es ratsam, Kabellegerschiffe bereitzuhalten, die abhängig von deren Verfügbarkeit, der Entfernung und Tiefe des beschädigten Kabels sowie den

48 *Yaacoub/Noura/Salman/Chehab*, Internet of Things v. 11 2020, 100218 (100241).
49 *Knysh*, Ocean Engineering v. 227 2021, 108707 (108710).

aktuellen Witterungsbedingungen eine Reparatur ermöglichen. Zusätzliche Maßnahmen umfassen die Vorratshaltung kritischer Ersatzteile sowie die Etablierung von Lieferketten und Vereinbarungen mit Herstellern und Lieferanten, um eine schnelle Beschaffung von Ersatzteilen zu gewährleisten. Es ist jedoch zu berücksichtigen, dass viele kritische Elemente maritimer Infrastrukturen groß und kostspielig sind, wie beispielsweise die Transformatoren von Offshore-Konverterstationen.

F. Fazit

Maritime Infrastrukturen sind von teils entscheidender Bedeutung für ein Land, sowohl für die Wirtschaft als auch für die Energieversorgung, so dass eine größere Anzahl dieser Systeme als Kritische Infrastruktur gelten. Der Schutz dieser Infrastrukturen ist aufgrund vielfältiger Bedrohungen, wie Naturkatastrophen und von Menschen ausgehende Gefahren, äußerst anspruchsvoll und komplex. Hinzu kommt die räumliche Ausdehnung der zu überwachenden Gebiete und die langen Interventionszeiten der Sicherheitskräfte. Resilienz, also die Fähigkeit von Systemen, Störereignissen standzuhalten und dabei ihre Funktionsfähigkeit entweder zu bewahren oder zeitnah wiederherzustellen, ist daher von entscheidender Bedeutung. Maßnahmen zur Erhöhung der Resilienz maritimer Infrastrukturen reichen von multidimensionaler Überwachung und Situationsbewusstsein bis hin zu Schutzmaßnahmen und systemischen Ansätzen. Dabei ist es wichtig, diese Maßnahmen ganzheitlich zu betrachten und umzusetzen, um eine nachhaltige Sicherheit und Widerstandsfähigkeit der maritimen Infrastrukturen zu gewährleisten.

Mayday, Mayday: Mangelnder Schutz von Einrichtungen auf See

Peter Ehlers, Hamburg[*]

A. Einführung

Mit den Anschlägen auf die Gas-Rohrleitungen Nord Stream 1 und 2 ist vielen erstmals bewusst geworden, wie verletzlich und ungeschützt Unterwasserleitungen und andere Einrichtungen[1] auf See sind und welche große Bedeutung sie für Versorgung und Kommunikation haben. Soweit Deutschland betroffen ist, handelt es sich zum einen um Gas-Rohrleitungen mit dazu gehörigen Verdichterstationen, die durch Nord- und Ostsee bis an die deutsche Küste führen, zum anderen um Unterwasser-Stromleitungen und zahlreiche Datenkabel. Hinzu kommen die immer zahlreicheren Offshore-Windkraftanlagen mit den erforderlichen Konverterplattformen. Anderenorts spielen außerdem Förderplattformen für Öl und Gas eine wichtige Rolle, während es vor der deutschen Küste nur eine Ölplattform im Küstenmeer gibt. Vieles spricht dafür, dass in Zukunft weitere Anlagen auf See errichtet werden, seien es Produktionsanlagen für Wasserstoff, gigantische Meerwasser-Wärmepumpen oder Unterwasser-Rechenzentren, wie sich das in anderen Ländern bereits abzeichnet. Inzwischen ist sogar ein schwimmender Weltraumbahnhof in der Nordsee in Planung.[2] Häufig sind diese Einrichtungen zur kritischen Infrastruktur zu zählen, kann ihr Ausfall doch zu erheblichen Beeinträchtigungen der Energieversorgung oder der Kommunikationsmöglichkeiten führen.

Errichtung und Betrieb derartiger Einrichtungen setzen umfangreiche Planfeststellungs- oder Genehmigungsverfahren voraus.[3] Damit soll sichergestellt werden, dass von den Einrichtungen keine Gefahren insbesondere

---

* Prof. Dr. Dr. h. c. mult. Peter Ehlers war vormals Präsident des Bundesamtes für Seeschifffahrt und Hydrographie; er ist Honorarprofessor der Universität Hamburg und Autor des Standardkommentars „Recht des Seeverkehrs".

1 Unter diesem Begriff werden im Folgenden Anlagen, Bauwerke, Rohrleitungen und Kabel zusammengefasst.

2 S. dazu ausführlich *Proelß*, Seevölkerrechtliche Rahmenbedingungen des Betriebs eines Weltraumbahnhofs in der ausschließlichen Wirtschaftszone, NordÖR 2021, 393-401.

3 S. §§ 57a, 133 BBergG, § 66 WindSeeG, § 2 SeeAnlG.

für Schifffahrt und Meeresumwelt ausgehen. Hingegen ist bisher kaum ein Augenmerk darauf gerichtet worden, dass sie selbst gegen von außen drohenden Gefahren geschützt werden müssen. Anschläge auf diese Einrichtungen sind insbesondere von Schiffen aus sowie mit Drohnen und autonomen oder ferngelenkten Unterwassersystemen möglich. Die inzwischen eingesetzten Diskussionen[4] fokussieren sich weitgehend darauf, wie die Einrichtungen durch technische Lösungen besser überwacht werden können. Der Einsatz geeigneter Sensoren und die Möglichkeit, jederzeit aktuelle und präzise Lagebilder zu erstellen, sind gewiss hilfreich, kann das doch eine abschreckende Wirkung entfalten. Das allein reicht jedoch nicht aus. Entscheidend ist vielmehr, dass, wenn erforderlich, konkrete Schutzmaßnahmen ergriffen und auch gegen Widerstand durchgesetzt werden können. Dabei ist vor allem an gezielte Zwangs- und Gewaltmaßnahmen gegenüber Personen sowie die Beschlagnahme, Beschädigung oder Unbrauchbarmachung von Gegenständen bis hin zu Schiffen zu denken.

Die damit verbundenen Fragen nach den rechtlichen Voraussetzungen für notwendige Schutzmaßnahmen sind bisher vernachlässigt worden. Gegenwärtig ändert sich das. Die 13. Nationale Maritime Konferenz hat sich im September 2023 erstmals mit dem Thema befasst. Ein dem Schutz kritischer Infrastruktur dienendes KRITIS-Dachgesetz ist in Vorbereitung.[5] Die NATO will ein Zentrum für die Sicherheit kritischer Unterwasserstrukturen einrichten[6] und hat mit der Erörterung der dabei zu berücksichtigenden Rechtsfragen begonnen. Diese Fragen sollen, soweit sie Deutschland betreffen, im Folgenden etwas näher beleuchtet werden. Die Überlegungen beschränken sich räumlich auf den Bereich seewärts der Außengrenze des Küstenmeeres, da in den Hoheitsgewässern, sieht man vom Recht der friedlichen Durchfahrt ab, letztlich von derselben Rechtslage wie an Land ausgegangen werden kann. Geklärt werden muss zum einen, welche völkerrechtlichen Eingriffsbefugnisse außerhalb des Hoheitsgebietes überhaupt bestehen, zum anderen wer nach nationalem Recht zu derartigen

4 So z. B. auf dem European Workshop of Maritime Systems of Resilience and Security (MARESEC 2023) des Deutschen Zentrums für Luft- und Raumfahrt, Bremerhaven, 27.6.2023; vgl. auch Presseerklärung des Europäischen Rates vom 24.10.2023 „Maritime security: Council approves revised EU strategy and action plan".

5 S. Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen, Referentenentwurf des Bundesministeriums des Innern und für Heimat, Bearbeitungsstand 25.7.2023.

6 S. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der AfD, BT-Drs. 20/8009, S. 2.

Maßnahmen befugt ist. Abschließende Antworten sind im Rahmen einer solchen Betrachtung nicht möglich; dazu bedarf es sehr viel detaillierterer Untersuchungen. Hier geht es erst einmal darum, auftretende rechtliche Probleme zu identifizieren und denkbare Lösungsansätze zur Diskussion zu stellen. Dabei wird im Folgenden davon ausgegangen, dass die Anschläge von Privatpersonen begangen werden und zumindest nicht hinreichend erkennbar ist, dass sie im Auftrag eines fremden Staates handeln.

B. Völkerrecht

Soweit es seewärts des Küstenmeeres um die bloße Lagebeobachtung geht, bedarf es keiner ausdrücklichen völkerrechtlichen Ermächtigung, da nicht in Rechte Dritter eingegriffen wird. Das gilt auch, wenn die bloße Anwesenheit von Behörden- oder Marinefahrzeugen in dem fraglichen Gebiet oder die Beobachtung und Begleitung eines verdächtigen Schiffes zu einem Verscheuchungseffekt führt. Anders ist es dann, wenn eine gezielte Kontrolle Verdächtiger vorgenommen wird. Dabei macht es einen Unterschied, ob die Kontrolle einem Schiff oder einer Einrichtung gilt, und ob die Maßnahmen in der AWZ oder auf der Hohen See vorgenommen werden. Außerdem wird zu differenzieren sein, ob i.S.d. des SRÜ[7] der Schutz einer Anlage oder einer Unterwasserrohrleitung oder eines Unterwasserkabels in Rede steht.

I. Befugnis zu Abwehrhandlungen in der AWZ

1. Maßnahmen gegenüber Schiffen

a) Umfang der Schifffahrtsfreiheit

Schiffskontrollen steht grundsätzlich die Freiheit der Schifffahrt entgegen, die nach Art. 87 Abs. 1 Buchst. a, Art. 58 Abs. 1 SRÜ auf der Hohen See und – mit Einschränkungen – auch für die AWZ gilt. Das bedeutet, dass ein Staat in diesen Bereichen, soweit nicht das Gegenteil von Rechts wegen zugelassen ist, nicht gegen Schiffe unter einer fremden Flagge vorgehen kann. Ausnahmen bei Verdacht der Seeräuberei, des Sklavenhandels und der

7 Seerechtsübereinkommen der Vereinten Nationen (BGBl. 1994 II 1798).

Verbreitung nicht genehmigter Rundfunksendungen (Art. 110 SRÜ) sind nicht einschlägig. Zusätzlich räumt Art. 220 Abs. 3 ff. SRÜ in der AWZ dem Küstenstaat Befugnisse gegenüber fremdflaggigen Schiffen im Fall eines Verstoßes gegen schifffahrtsbezogene internationale Umweltvorschriften ein. Zwar sind Fälle denkbar, bei denen der Anschlag auf eine Einrichtung zu einer Umweltverschmutzung führen kann, so vor allem wenn aus einer Gasrohrleitung größere Mengen Gas austreten. Allerdings liegt in diesem Fall kein Verstoß gegen einschlägige internationale Umweltvorschriften vor, da derartige Anschläge nicht von den Schifffahrtsregelungen erfasst werden. Auch die durch Art. 221 SRÜ bestätigte völkerrechtliche Befugnis, Maßnahmen zum Schutz vor einer infolge eines Seeunfalls eingetretenen oder drohenden Verschmutzung zu ergreifen, kann keine Anwendung finden, weil ein Anschlag keinen Seeunfall eines Schiffes darstellt.[8]

Bei widerrechtlichen Handlungen auf See, die gegen Schiffe gerichtet sind, können nach dem SUA-Übereinkommen[9] Maßnahmen gegenüber verdächtigen Schiffen zumindest dann ergriffen werden, wenn der Flaggenstaat dem zustimmt.[10] Das Übereinkommen wird im Hinblick auf feste Plattformen durch das darauf basierende SUA-Protokoll[11] ergänzt. Schwimmende Plattformen sowie Unterwasserrohrleitungen und -kabel werden davon allerdings nicht erfasst (Art. 1 Abs. 3). Nach dem SUA-Protokoll sind zahlreiche Bestimmungen des SUA-Übereinkommens sinngemäß auch auf feste Plattformen anzuwenden, jedoch werden Abwehrmaßnahmen gegenüber Schiffen nicht einbezogen (Art. 1 Abs. 1),[12] so dass sich aus dem SUA-Protokoll keine weiteren Befugnisse herleiten lassen.

8 Zum Begriff s. auch Art. II Abs. 1 Protokoll von 1973 über Maßnahmen auf Hoher See bei Fällen von Verschmutzung durch andere Stoffe als Öl (BGBl. 1985 II 593).

9 Übereinkommen zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Seeschifffahrt (BGBl. 1990 II 494, 496, BGBl. 2015 II 1446, 1448).

10 Art. 8^{bis} idF des Protokolls von 2005 zum Übereinkommen zur Bekämpfung widerrechtlicher Handlungen gen die Sicherheit der Seeschifffahrt (BGBl. 2015 II 1448).

11 Protokoll zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit fester Plattformen, die sich auf dem Festlandsockel befinden (BGBl. 1990 II 494, 508, BGBl. 2015 II 1446, 1474).

12 Vgl. Art. 2 Abs. 1 des Protokolls von 2005 zum Protokoll zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit fester Plattformen, die sich auf dem Festlandsockel befinden (BGBl. 2015 II 1448).

b) Einschränkung durch Befugnisse in Bezug auf Anlagen

Für Anlagen und Bauwerke in der AWZ gewährt Art. 60 Abs. 2 SRÜ dem Küstenstaat ausschließliche Hoheitsbefugnisse, einschließlich derjenigen in Bezug auf Zoll- und sonstige Finanzgesetze, Gesundheits-, Sicherheits- und Einreisegesetze und diesbezügliche sonstige Vorschriften.[13] Das könnte dafür sprechen, dass im Falle einer Bedrohung auch notwendige Abwehrmaßnahmen gegenüber Schiffen ergriffen werden können. Jedoch erscheint es im Hinblick auf die Freiheit der Schifffahrt äußerst problematisch, wollte man diese Befugnisse, die sich unmittelbar auf Anlagen und Bauwerke beziehen, generell auf Schiffe erstrecken, die sich in der Umgebung aufhalten. Dem steht entgegen, dass der Küstenstaat durch Art. 60 Abs. 4, 5 SRÜ ausdrücklich zur Einrichtung von Sicherheitszonen ermächtigt wird. In dieser Zone, die bis zu einer Entfernung von maximal 500 m von der Anlage eingerichtet werden kann, sind geeignete Maßnahmen des Küstenstaats zulässig, um die Sicherheit der Schifffahrt und der Anlage zu gewährleisten. Einer solchen Regelung würde es nicht bedürfen, wenn sich die Ausweisung von Sicherheitszonen bereits aus den generellen Hoheitsbefugnissen in Bezug auf Anlagen rechtfertigen lässt. Die Befugnisse in der Sicherheitszone erfassen nicht nur die erforderliche Rechtsetzung, sondern schließen Kontroll- und Zwangsmaßnahmen zur Abwehr eines Anschlags ein.[14]

Ein gewisses linguistisches Problem ergibt sich in diesem Zusammenhang aus dem Begriff „Sicherheit". Fraglich ist, ob der in der authentischen englischsprachigen Fassung in Art. 60 SRÜ verwendete Begriff „safety" auch die im Englischen als „security" bezeichneten Sicherheitsbelange umschließt. Während „safety" eher die von einer Sache ausgehenden Gefahren betrifft, bezieht sich „security" auf die einer Sache drohende Gefahr. So werden konsequenterweise die Maßnahmen zur Abwehr äußerer Gefahren

13 Nach Art. 80 SRÜ gilt diese Regelung auch für den Festlandsockelbereich, der für Deutschland mit der AWZ deckungsgleich ist.

14 *Proelss*, United Nations Convention on the Law of the Sea, 2017, Art. 60 Rn. 16 f., 24 f.; so auch das nach Anlage VII zum SRÜ eingerichtete Schiedsgericht im Fall „Arctic Sunrise", Arbitral Tribunal constituted under Annex VII to the 1982 United Nations Convention on the Law of the Sea, PCA Case No. 2014/02 v. 14.8.2015, Rn. 278; *Wolfrum and Kelly*, International Tribunal for the Law of the Sea, Case No. 22, Order of 22 November 2013, Joint Separate Opinion of Judges Wolfrum and Kelly, Nr. 12, *Golitsyn*, ibid., Dissenting Opinion of Judge Golitsyn, Nr. 25.

in Kapitel XI-2 der Anlage zu SOLAS[15] als „security measures" bezeichnet, wenngleich das Übereinkommen in seiner Zielsetzung auf „promoting safety" ausgerichtet ist. Würde man dieser – letztlich wohl nicht ganz eindeutigen – Differenzierung folgen, würde es sich bei Anschlägen von außen um nicht erfasste „security"-Fälle handeln. Aber es ist nicht zu erkennen, dass in den Verhandlungen zum SRÜ eine solche scharfe begriffliche Trennung angestrebt wurde, zumal das SRÜ den Begriff „security" für ganz andere Sachverhalte nutzt, nämlich die Sicherung von Frieden und staatlicher Ordnung oder finanzielle Sicherheiten.[16] Daher erscheint eine weite Anwendung entsprechend dem deutschen Sprachgebrauch gerechtfertigt. Das ließe sich ergänzend auch mit der Verwendung des Wortes „einschließlich" in Art. 60 Abs. 2 SRÜ begründen, die deutlich macht, dass die dortige Aufzählung der Gesetzesmaterien nicht abschließend ist, zumindest also weitere artverwandte Bereiche einbezogen werden können. Daraus ist zu folgern, dass das Seerecht Maßnahmen gegenüber fremdflaggigen Schiffen zwar in einer Sicherheitszone zulässt, dem ansonsten jedoch auch in der AWZ die Freiheit der Schifffahrt entgegensteht.[17]

c) Einbeziehung von ferngelenkten oder autonomen Drohnen

Bei Anschlägen auf Anlagen sind Fallgestaltungen denkbar, bei denen ferngelenkte oder autonome Unterwassergeräte, auch als Unterwasserdrohnen bezeichnet, eingesetzt werden. Dann stellt sich die Frage, ob ihr Betrieb von der Freiheit der Schifffahrt nach Art. 58, 80 SRÜ erfasst wird. Nicht zuletzt die authentische englische Fassung „freedom of navigation" spricht dafür, den Begriff der Schifffahrtsfreiheit weit auszulegen, so dass davon Schwimmkörper erfasst werden, die eine zielgerichtete Ortsveränderung ermöglichen, unabhängig davon, ob sie bemannt sind.[18] Folglich sind Abwehrmaßnahmen gegenüber diesen Geräten z. B. in der Form von Inspektionen, Aufbringen oder Zerstörung, außerhalb einer Sicherheitszone völkerrechtlich unzulässig. Bei fliegenden Drohnen tritt wegen der völkerrechtlichen Freiheit des Überflugs (Art. 87 Abs. 1 Buchst. b SRÜ) eine ent-

15 Internationales Übereinkommen zum Schutz des menschlichen Lebens auf See (BGBl. 1979 II 143).
16 S. u. a. Präambel, 7. Erwägungsgrund, Art. 19, 25 Abs. 3, 52 Abs. 2, 73 Abs. 2, 138, 218 Abs. 4, 220 Abs. 7, 226 Abs. 1 b.
17 So auch Arbitral Tribunal (Fn. 14), Rn. 211.

sprechende Problematik auf, wenn der Verdacht besteht, dass sie sich einer Anlage oder Installation in der Absicht nähern, diese zu beschädigen.

d) Geltung für Unterwasserrohrleitungen und -kabel

Fraglich ist, ob neben Plattformen auch Unterwasserrohrleitungen und -kabel begrifflich als Anlagen zu bewerten sind, so dass sie von den Regelungen des Art. 60 SRÜ erfasst werden. Sprachlich könnte der für Anlagen authentische englische Begriff „installations" eine Einbeziehung nahelegen. Dem steht jedoch entgegen, dass das SRÜ offenbar von einer begrifflichen Trennung ausgeht und für Anlagen einerseits und Rohrleitungen und -kabel andererseits unterschiedliche Regelungen trifft. Während die Errichtung von Anlagen und Bauwerken in der AWZ dem Küstenstaat vorbehalten ist (Art. 56 Abs. 1 Buchst. b i SRÜ), können Rohrleitungen und Kabel entsprechend dem Grundsatz der Meeresfreiheit grundsätzlich von allen Staaten betrieben werden, soweit dies mit den anderen Bestimmungen des SRÜ vereinbar ist (Art. 58 Abs. 1 SRÜ). Das wird weiter spezifiziert durch die Regelungen über den Festlandsockel, die zwischen Kabeln und Rohrleitungen sowie Anlagen differenzieren (Art. 79, 80 SRÜ). Für einen engen Anlagenbegriff, der Kabel und Rohrleitungen nicht einschließt, spricht schließlich auch deren kumulative Nennung in Art. 21 Abs. 1 Buchst. b und c und Art. 87 Abs. 1 Buchst. c und d SRÜ.[19] Mithin erstrecken sich die Befugnisse nach Art. 60 SRÜ nicht auf Rohrleitungen und Kabel, so dass für diese auch keine Sicherheitszonen eingerichtet werden können, um darauf Abwehrmaßnahmen zu stützen. Für die Trassenführung von

18 S. *Kraska, Pedrozo*, China's Capture of U.S. Underwater Drone Violates Law of the Sea, Lawfare, 16.12.2016, https://www.lawfaremedia.org/article/chinas-capture-us-underwater-drone-violates-law-sea (letzter Abruf am 27.08.24); *Fletcher* et al., Advancing Clarity: Analysis of UxS Legal Questions, S. 2, https://nps.edu/documents/114698888/139877137/CRUSER_Advancing+Legal+Clarity+Final+Report+%28Dec+2022%29.pdf/d8259e11-4a76-742d-355d-0901dc8da549?t=1675115748216 (letzter Abruf am 27.08.24); *Chang* et al., The international legal status of the unmanned maritime vehicles, Marine Policy 113 (2020) 103830, S. 4; vgl. *Klemmer*, Legal Ambiguities Concerning the Use of Unmanned Aerial Vehicles in Marine Scientific Research, The Arctic University of Norway, Academic Year 2021-2022, S. 22 f., https://munin.uit.no/bitstream/handle/10037/27811/thesis.pdf?sequence=2&isAllowed=y. (letzter Abruf am 27.08.24).

19 S. *Englender* in Proelss (Fn. 14), Art. 79 Rn. 17 f.; *Lagoni* in Vitzhum, Handbuch des Seerechts, 2006, Kapitel 3 Rn. 123.

Transitrohrleitungen – nicht jedoch für Transitkabel[20] – besteht zwar nach Art. 79 Abs. 3 SRÜ ein Zustimmungserfordernis des Küstenstaates, dadurch werden jedoch keine weiteren Befugnisse gegenüber Dritten begründet. Das gilt auch für die Rechte des Küstenstaates, bei Kabeln und Rohrleitungen, die in sein Hoheitsgebiet führen, Bedingungen festzulegen (Art. 79 Abs. 4 SRÜ). Die Streitfrage, ob sich die Bedingungen überhaupt auf die AWZ oder nur auf den im Hoheitsgebiet gelegenen Leitungsteil beziehen können,[21] bedarf hier keiner Klärung, da Bedingungen, von denen eine Genehmigung abhängig gemacht wird, ohnehin nur an die Errichter und Betreiber von Kabeln und Rohrleitungen adressiert werden können. Schließlich lassen sich auch aus den Vorschriften des SRÜ über Kabel und Rohrleitungen im Bereich der Hohen See, die gem. Art. 58 Abs. 2 SRÜ auch in der AWZ gelten, keine zusätzlichen Befugnisse herleiten, während nach dem auch in der AWZ geltenden Telegraphenkabel-Vertrag von 1884[22] zumindest ein Nationalitätsnachweis verlangt werden kann, wie unten näher dargelegt wird.

e) Geltung für Verdichterplattformen

Unklar ist die Rechtslage bei Verdichterplattformen für Gasrohrleitungen. Als wesentlicher Bestandteil einer Rohrleitung unterliegen sie dem Recht der Rohrleitung.[23] Ob sich die dennoch in der Praxis anzutreffende Einrichtung von Sicherheitszonen um eine solche Plattform mit einer entsprechenden Anwendung des Art. 60 SRÜ rechtfertigen lässt, weil daraus mangels Widerspruchs Völkergewohnheitsrecht entstanden ist,[24] erscheint zumindest zweifelhaft. Möglicherweise ließe sich argumentieren, dass das SRÜ zwischen auf einen festen Ort begrenzte Einrichtungen – Anlagen – und über eine längere Trasse führende Verbindungen – Kabel und Rohrleitungen – differenzieren will, zumal letztere auch durch Schifffahrtswege

20 *Englender* (Fn. 19), Rn. 23.
21 S. dazu *Englender* (Fn. 19), Rn. 24 f.; im Einzelnen *Proelß*, Völkerrechtliche Rahmenbedingungen der Verlegung grenzüberschreitender Seekabel im Bereich der ausschließlichen Wirtschaftszone und des Festlandsockels, in: Ehlers, Proelß, Ramming (Hrsg.), Kreuzpeilung - Festgabe für Marian Paschke, Veröffentlichungen des Instituts für Seerecht und Seehandelsrecht der Universität Hamburg, Bd. 25, 2021, S. 256ff.
22 Internationaler Vertrag zum Schutz unterseeischer Telegraphenkabel von 1884 (RGBl. 1888, 151).
23 S. *Lagoni* (Fn. 19), Rn. 123; *Englender* (Fn. 19), Rn. 17.
24 So *Lagoni* (Fn. 19), Rn. 168 f.

führen. Dort können ohnehin keine Sicherheitszonen eingerichtet werden, was sich in Art. 60 Abs. 7 SRÜ widerspiegelt.

2. Abwehrmaßnahmen mit unmittelbarem Bezug zu einer Anlage

Eindeutig ist die Völkerrechtslage, wenn es sich um Maßnahmen gegen Personen handelt, die sich widerrechtlich auf einer Anlage aufhalten oder versuchen, sich Zutritt zu verschaffen. Das schließt z. B. auch Taucher ein, die sich einer Anlage unter Wasser nähern. Gegenüber diesen Personen gilt, auch wenn sie fremder Nationalität sind, die auf die Anlage bezogene Eingriffsbefugnis nach Art. 60 Abs. 2 SRÜ.

3. Maßnahmen zur Ermittlung von Straftaten

Zu den Hoheitsbefugnissen sind nicht nur Maßnahmen zur Abwehr von Anschlägen zu zählen, sondern auch die Möglichkeit, entsprechende Aktivitäten als Straftaten oder Ordnungswidrigkeiten auszuweisen und zu verfolgen. Das SUA-Protokoll legt einschlägige Straftaten ausdrücklich fest, gilt allerdings nur für feste Plattformen,[25] so dass schwimmende Anlagen nicht erfasst werden. Das verschließt aber nicht die Möglichkeit, bei schwimmenden Anlagen entsprechende Regelungen unmittelbar auf Art. 60 Abs. 2 SRÜ zu stützen. Im Ergebnis sind also Ermittlungstätigkeiten gegenüber Personen auf oder in unmittelbarer Nähe von Anlagen und gegenüber Schiffen innerhalb einer Sicherheitszone völkerrechtlich zulässig, jedoch nicht bei fremdflaggigen Schiffen, die sich außerhalb dieses Bereichs befinden. Handelt es sich jedoch um Unterwasserrohrleitungen oder -kabel, besteht keine entsprechende Ermittlungsbefugnis, abgesehen von der bloßen Ermittlung der Nationalität nach dem Telegraphenkabel-Vertrag.

II. Befugnisse auf Hoher See

Die Rechtslage auf der Hohen See dürfte zumindest, soweit es Anlagen betrifft, für die Praxis gegenwärtig keine große Relevanz haben. Denn bisher sind keine Anlagen auf Hoher See errichtet worden. Auch der Schutz von Einrichtungen im Rahmen des Tiefseebergbaus ist zumindest aus deutscher

25 Art. 2 ff. iVm Art. 1 Abs. 3 SUA-Protokoll.

Sicht bisher kein Thema. Da aber zusätzlich zu Offshore-Windkraftanlagen, die fest mit dem Meeresgrund verbunden sind, die Errichtung schwimmender Windkraftanlagen geplant wird,[26] erscheint es nicht völlig ausgeschlossen, dass diese künftig auch auf der Hohen See zum Einsatz kommen werden. Allerdings dürfte angesichts der großen Wassertiefen auf der Hohen See eine ausreichende Verankerung auf dem Meeresgrund ganz erhebliche Probleme aufwerfen. Seit Langem schon verlaufen hingegen transkontinentale Unterwasserkabel durch Bereiche der Hohen See. Insoweit sind daher Anschläge vorstellbar, die von Schiffen aus begangen werden, wenngleich dafür wohl eher die küstennäheren Gebiete in Betracht kämen.

1. Regelungen des SRÜ

Aus der für die Hohe See geltenden Schifffahrtsfreiheit (Art. 88 Abs.1 Buchst. a SRÜ) folgt, dass Staaten dort grundsätzlich nur Maßnahmen gegenüber Schiffen unter ihrer Flagge ergreifen können, es sei denn, dass sich aus internationalen Regelungen etwas anderes ergibt (Art. 92 Abs. 1 SRÜ). An einer dem Art. 60 SRÜ entsprechenden Ermächtigung, Schutzmaßnahmen zu ergreifen und Sicherheitszonen einzurichten, fehlt es. Eine Einstufung der Anschläge auf Einrichtungen als Seeräuberei nach Art. 101 SRÜ kommt nicht in Betracht, denn das setzt grundsätzlich gegen ein Schiff gerichtete Handlungen voraus. Zwar werden auch Handlungen gegen Vermögenswerte an einem Ort, der keiner staatlichen Hoheitsgewalt untersteht, durch Art. 101 Buchst. a ii SRÜ einbezogen. Das lässt jedoch kein anderes Ergebnis zu, da damit offensichtlich nicht die Hohe See gemeint ist, die in Art. 101 Buchst. a i SRÜ gesondert geregelt ist und im Übrigen keinen rechtsfreien Raum darstellt.[27]

Auch aus den Einzelregelungen für Kabel und Rohrleitungen (Art. 112-115 SRÜ), die weitestgehend aus dem Genfer Seerechtsübereinkommen von 1958 übernommen worden sind,[28] lassen sich keine Eingriffsbefugnisse herleiten. Danach sind die Staaten zwar u.a. verpflichtet, die

26 Vgl. Floating wind platform now on site in Spain, Schiff&Hafen/Ship&Offshore, Energy at Sea, The European Offshore Wind Compendium, 2023, S. 18.

27 Vgl. *Guilfoyle* in Proelss (Fn. 14), Art. 101 Rn. 11; s. im Einzelnen *Halog, Margat, Stadermann*, Legal Considerations on the Protection of Submarine Cables in the International and National Legislative Framework, 3rd European Workshop on Maritime Systems, Resilience and Security 2023 (MARESEC 23), Bremerhaven, Germany, https://doi.org/10.5281/zenodo.8405962.

28 Art. 26-29 Übereinkommen vom 29.4.1958 über die Hohe See (BGBl. 1972 II 1089).

Unterbrechung oder Beschädigung eines Kabels oder einer Rohrleitung einschließlich darauf gerichteter Handlungen unter Strafe zu stellen. Das ist jedoch auf Verstöße durch Schiffe unter der eigenen Flagge oder Personen beschränkt, die der Gerichtsbarkeit des jeweiligen Staates unterliegen (Art. 113 SRÜ). Daraus lässt sich jedoch keine die Schifffahrtsfreiheit einschränkende Befugnis zu Ermittlungstätigkeiten auf Hoher See herleiten.

2. Telegraphenkabel-Vertrag

Etwas anders stellt sich die Rechtslage nach dem Telegraphenkabel-Vertrag dar, der nicht nur auf Telegrafenkabel, sondern auf alle unterseeisch verlegten Kabel Anwendung findet (Art. 1).[29] Der Vertrag weist das Zerreißen oder Beschädigen eines Kabels als Straftat aus und legt fest, dass die Staaten zur Strafverfolgung in Bezug auf Schiffe unter ihrer Flagge und ihre Staatsangehörigen zuständig sind, wie das im Wesentlichen in Art. 113 SRÜ seinen Niederschlag gefunden hat. Zusätzlich können jedoch im Verdachtsfall von einem Schiff nach Art. 10 Abs. 2 und 3 des Vertrages Nachweise über die Nationalität verlangt und Protokolle aufgenommen werden. Aus diesen Vorschriften lässt sich ableiten, dass ein Betreten des Schiffes gestattet ist. Zweifelhaft erscheint allerdings, ob sich daraus eine Befugnis zu weitergehenden Untersuchungen auf dem Schiff ergibt. Zumindest Beschlagnahme- und Festnahmerechte dürften sich nicht darauf stützen lassen. Letztlich erschöpft sich die Befugnis nach Feststellung der Nationalität in der Möglichkeit, den Flaggenstaat entsprechend zu unterrichten. Bemerkenswert ist allerdings, dass diese Befugnisse gegenüber fremdflaggigen Schiffen weder vom Genfer Seerechtsübereinkommen noch vom SRÜ übernommen worden sind,[30] obwohl dies nahegelegen hätte, da das SRÜ die Fälle für ein Betretungsrecht ausdrücklich festlegt.[31] Daher stellt sich die Frage, ob die neueren Übereinkommen als leges posteriores die frühere Regelung außer Kraft setzen. Dem steht jedoch entgegen, dass durch das SRÜ die Rechte und Pflichten aus anderen Übereinkünften grundsätzlich nicht beeinträchtigt werden.[32]

---

29 Unzutreffend beschränken *Halog, Margat, Stadermann* (Fn. 21), Abschnitt III A 1, den Vertrag auf Telegrafenkabel.

30 *Guilfoyle* in Proelss (Fn. 14), Art. 113 Rn. 2.

31 Art. 110 SRÜ.

32 Art. 311 Abs. 2 SRÜ, so auch *Guilfoyle* in Proelss (Fn. 14), Art, 110 Rn. 2.

III. Befugnisse nach allgemeinen völkerrechtlichen Grundsätzen

Nach allem ist festzustellen, dass Maßnahmen gegenüber Schiffen unter fremder Flagge außerhalb von eng begrenzten Sicherheitszonen in der AWZ zur Abwehr von Anschlägen auf kritische Infrastrukturen weitestgehend an der Schifffahrtsfreiheit scheitern. Im Ergebnis erscheint es jedoch äußerst unbefriedigend, wenn dem Schutz von Einrichtungen derartige Grenzen gesetzt werden. Zu erwägen ist daher, ob die Schifffahrtsfreiheit auch dann gilt, wenn sie für einen Anschlag missbraucht wird. Nach Art. 88 SRÜ ist die Hohe See friedlichen Zwecken vorbehalten; das gilt nach Art. 58 Abs. 2 auch für die Anwendbarkeit der Freiheitsrechte in der AWZ. Fraglich erscheint jedoch, ob ein solcher Missbrauch als „unfriedliche" Aktivität gewertet werden kann. Art. 301 SRÜ, in dem Pflichten im Hinblick auf die friedliche Nutzung statuiert werden, legt nahe, dass unter einer unfriedlichen Nutzung offenbar Gewaltaktionen von Staaten verstanden werden, also um verbotene kriegerische militärische Aktionen.[33] Etwas anderes lässt sich auch nicht aus den Vorschriften über das Recht der friedlichen Durchfahrt durch das Küstenmeer herleiten. Zwar ist nach Art. 19 Abs. 2 Buchst. k SRÜ eine Durchfahrt dann nicht friedlich, wenn Handlungen vorgenommen werden, die auf die Störung eines Nachrichtenübermittlungssystems oder anderer Anlagen und Einrichtungen gerichtet sind. Daraus kann jedoch noch nicht der Schluss gezogen werden, dass diese Handlungen unfriedlich iSd Art. 88 SRÜ sind. Denn wie sich aus den in der authentischen englischen Fassung des SRÜ verwendeten Begriffen „innocent" in Art. 19 SRÜ und „peaceful" in Art. 88 SRÜ ergibt, handelt es sich um zwei unterschiedliche Begriffe, auch wenn das in der deutschen Übersetzung nicht zum Ausdruck kommt. Das findet seine Bestätigung darin, dass Art. 19 Abs. 1 SRÜ die Begriffe Frieden, Ordnung und Sicherheit[34] alternativ nebeneinander verwendet. Anschläge auf Einrichtungen sind eher der Sicherheit und Ordnung zuzuordnen.

Ein anderer Diskussionsansatz könnte sich aus der Entscheidung des Internationalen Schiedsgerichts zum Fall „Arctic Sunrise" ergeben. Es hält es zumindest für denkbar, dass terroristische Angriffe auf Anlagen in der AWZ ein Verstoß gegen küstenstaatliche Rechte zu Errichtung und Betrieb

33 S. dazu im Einzelnen *Proelß*, Peaceful Purposes, in: Max-Planck Encyclopedia of Public International Law, updated May 2021; vgl. *Bothe* in Vitzhum, Proelß (Hrsg.), Völkerrecht, 8. Auflage, 2019, Kapitel VIII Rn. 43 f.

34 Im authentischen englischen Text "peace, good order or security".

von Anlagen sind und entsprechende Abwehrmaßnahmen rechtfertigen können,[35] trifft dazu aber mangels Entscheidungsrelevanz keine abschließende Feststellung. Derartige Überlegungen könnten vielleicht ergänzend darauf gestützt werden, dass die Schifffahrtsfreiheit nur unter gebührender Berücksichtigung der Rechte anderer Staaten ausgeübt werden darf, wie das in Art. 58 Abs. 3, Art. 87 Abs. 2 SRÜ zum Ausdruck kommt. Es bedarf daher einer Abwägung zwischen den Schutzinteressen des Küstenstaates und der Schifffahrtsfreiheit, die im Ergebnis eingeschränkt werden könnte. Das erscheint allerdings deshalb problematisch, weil Voraussetzung ist, dass dem betroffenen Staat entsprechende Rechte zustehen. Die Rechte des Küstenstaates werden jedoch ausdrücklich in Art. 60 SRÜ festgelegt und enthalten gerade keine weitere Einschränkung der Schifffahrtsfreiheit. Vieles spricht daher dafür, diese Regelung als abschließend zu bewerten. Entsprechende Überlegungen für den Bereich der Hohen See dürften zu einem ähnlichen Ergebnis führen.

Überlegenswert erschiene es, zusätzliche Befugnisse aus dem naturgegebenen Recht der Staaten zur Selbstverteidigung[36] herzuleiten. Das Recht zielt vornehmlich darauf ab, dass ein Staat sich gegen kriegerische und militärische Aktionen anderer Staaten zur Wehr setzen darf. Ob das auch Anschläge einschließt, die die Infrastruktur eines Staates betreffen, aber ohne herkömmliche militärische Gewaltanwendung erfolgen, ist rechtlich unklar. Zu klären wäre auch, ob das völkerrechtliche Gewaltverbot überhaupt ordnungs- und strafverfahrensrechtliche Zwangsmaßnahmen erfasst oder auf militärische Gewalt beschränkt ist. Gerade im Hinblick auf die Terrorismusbekämpfung ist die Völkerrechtsentwicklung zum Umfang des Selbstverteidigungsrechts im Fluss. Eine anerkannte Staatenpraxis hat sich noch nicht herausgebildet.[37] All diese Fragen bedürfen daher einer sehr viel gründlicheren Untersuchung, die mit diesem Diskussionsbeitrag nicht geleistet werden kann. Insgesamt bleibt nur festzustellen, dass Maßnahmen zum Schutz von Einrichtungen, die über die Befugnisse nach Art. 60 SRÜ und dem Telegraphenkabel-Vertrag hinausgehen, mit großen völkerrechtlichen Unwägbarkeiten behaftet sind.

35 Arbitral Tribunal (Fn. 14), Rn 314 f.
36 Art. 51. UN-Charta (BGBl. 1973 II 505).
37 S. zur Problematik *Bothe* (Fn. 33), Rn. 11 ff., 19, 128.

C. Innerstaatliches Recht

Soweit nach dem internationalen Seerecht staatliche Schutzmaßnahmen seewärts des Küstenmeeres zulässig sind, bedarf es der weiteren Klärung, ob und in welcher Weise von diesen Befugnissen innerstaatlich überhaupt Gebrauch gemacht werden kann. Angesichts des verfassungsrechtlich verankerten Vorbehalts des Gesetzes (Art. 20 GG) bedarf es dazu zum einen der materiellrechtlichen Ermächtigung, zum anderen der Bestimmung der zuständigen Behörde. Ausgangspunkt ist dabei, dass auch seewärts des Küstenmeeres grundsätzlich die Zuständigkeit der Länder gegeben ist, soweit nicht das Grundgesetz etwas anderes regelt oder zulässt (Art. 30, 70 Abs. 1, Art. 83 GG).[38] Zu differenzieren ist außerdem zwischen ordnungsrechtlichen und strafverfahrensrechtlichen Maßnahmen.

I. Ordnungsrechtliche Befugnis

Die Befugnis zur Gefahrenabwehr außerhalb des Küstenmeeres ergibt sich aus §§ 14 ff. iVm § 6 BPolG. Da der Bund verfassungsrechtlich nur sonderpolizeiliche Aufgaben wahrnehmen darf,[39] gilt die sehr umfassende Befugnis allerdings nur für solche Sachverhalte, für deren Regelung dem Bund die Gesetzgebungskompetenz zusteht. Für Abwehrmaßnahmen zum Schutz von Einrichtungen auf See lässt sich eine entsprechende ordnungsrechtliche Annexkompetenz aus Art. 74 Abs. 1 Nr. 11 GG (Recht der Wirtschaft) herleiten. Allerdings gelten die Befugnisse nach dem BPolG nur, soweit nicht spezialgesetzliche Regelungen diese verdrängen. Für die Schifffahrtspolizei und die sonstige schiffsbezogene Gefahrenabwehr erforderliche Befugnisse werden durch § 3 Abs. 1 iVm § 1 Nr. 3 Buchst. a und b SeeAufgG begründet.[40] Der Umfang der Befugnisse richtet sich im Einzelnen nach §§ 3 a f., 8 SeeAufgG.

Errichtung und Betrieb von Förderplattformen, Transit-Rohrleitungen mit dazu gehörenden Verdichterplattformen sowie Unterwasserkabel wer-

38 S. dazu *Ehlers*, Polizei auf See, in: Ehlers, Proelß, Ramming (Hrsg.), Kreuzpeilung - Festgabe für Marian Paschke, Veröffentlichungen des Instituts für Seerecht und Seehandelsrecht der Universität Hamburg, Bd. 25, 2021, S. 93 f.; *Proelß, Westmark*, Unterseeische Speicherung und Export von CO_2 in Deutschland: Rechtliche Hürden und Reformbedarfe – Teil I, KlimR 5/2023, S. 149 mwN.

39 S. BVerfGE 97, 198 ff.

40 S. *Ehlers* (Fn. 38), S. 96 ff.

den durch das BBergG geregelt; aufsichtsbehördliche Befugnisse ergeben sich aus §§ 70 ff. BBergG. Allerdings fällt auf, dass die bergrechtlichen Regelungen auf die Verhütung von Gefahren ausgerichtet sind, die von einer Einrichtung ausgehen. Hingegen bleiben die von außen einer Einrichtung drohenden Gefahren völlig unberücksichtigt. Das könnte die Argumentation rechtfertigen, dass derartige Gefahren gar nicht vom BBergG erfasst werden, so dass insoweit die allgemeine Gefahrenabwehr nach dem BPolG greift. Zu berücksichtigen ist auch, dass das BBergG nur in dem mit der AWZ deckungsgleichen Bereich des deutschen Festlandsockels gilt (§ 2 Abs. 3 BBergG) und daher Befugnisse auf der Hohen See nur aus dem BPolG hergeleitet werden können. Ob sich auch aus dem MBergG[41] Eingriffsbefugnisse ergeben, die für Vorhaben des Tiefseebergbaus Bedeutung erlangen könnten, bleibt hier außer Ansatz, da es gegenwärtig keine derartigen deutschen Aktivitäten gibt.

Im Grundsatz ähnlich sind die Regelungen nach dem WindSeeG und dem SeeAnlG, die auch für die Hohe See gelten (§§ 2 Abs. 2 WindSeeG, 1 Abs. 1 SeeAnlG). Davon erfasst werden Offshore-Windkraftanlagen mit dazu gehörenden Konverterstationen und Übertragungskabeln sowie Anlagen die anderen wirtschaftlichen Zwecken oder meereskundlichen Untersuchungen dienen. Überwachungsbefugnisse werden durch §§ 79 WindSeeG, 14 SeeAnlG festgelegt. Auch diese Vorschriften lassen jedoch erkennen, dass die Überwachung offenbar der Verhütung von Gefahren durch die Anlagen, nicht aber deren Schutz gegen Gefahren von außen dienen soll, so dass in diesen Fällen die allgemeine Gefahrenabwehr nach dem BPolG zum Tragen kommt. Als Ergebnis ist festzuhalten, dass eine materiellrechtliche Befugnis für Maßnahmen zum Schutz von Einrichtungen auf See durch entsprechende bundesgesetzliche Regelungen gegeben ist.

II. Zuständigkeit

Da auch der Vollzug von Bundesrecht nach Art. 83 GG grundsätzlich den Ländern obliegt, bedarf es der Klärung, ob das Grundgesetz für Anlagen auf See etwas anderes regelt oder zulässt. Zentrale Vorschrift ist § 6 BPolG,[42] der für die Aufgaben der Gefahrenabwehr die Zuständigkeit der Bundespolizei festlegt, soweit die Maßnahmen nach Bundesrecht nicht

41 Meeresbodenbergbaugesetz (BGBl. 1995 I 778): vgl. dazu *Ehlers* (Fn. 38), S. 100 f.
42 S. dazu *Ehlers* (Fn. 38), S. 94 ff.

einer anderen Behörde zugewiesen sind. Somit besteht nur eine subsidiäre Zuständigkeit der Bundespolizei.

1. Seeaufgabengesetz

Nicht nur für die Schifffahrtspolizei, sondern auch für die sonstige Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung ist nach § 3 Abs. 1 iVm § 1 Nr. 3 Buchst. a und b SeeAufgG im Einklang mit Art. 89 Abs. 2 S. 2 GG seewärts des Küstenmeeres die Zuständigkeit der WSV[43] gegeben. Angesichts der Zielsetzung des SeeAufgG ist Voraussetzung, dass ein unmittelbarer Bezug zur Seeschifffahrt besteht.[44] Das trifft zu, wenn Anschläge auf eine Einrichtung von einem Schiff aus erfolgen, so dass in diesen Fällen die Zuständigkeit der Bundespolizei verdrängt wird. Gleichwohl können diese Aufgaben durch Rechtsverordnung zur Ausübung an die Bundespolizei und die Zollverwaltung übertragen werden (§ 3 Abs. 2 SeeAufgG). Da nur die Ausübung der Aufgaben delegiert werden kann, bleibt die WSV weiterhin für die Aufgabenerledigung insgesamt verantwortlich und ist weisungsbefugt. Von dieser Möglichkeit ist für die polizeilichen Vollzugsaufgaben durch die SeeSchAÜV[45] Gebrauch gemacht worden. Danach können Bundespolizei und Zollverwaltung seewärts des Küstenmeeres unaufschiebbare Maßnahmen zur Erfüllung völkerrechtlicher Verpflichtungen oder zur Wahrnehmung völkerrechtlicher Befugnisse treffen. Entsprechende Befugnisse folgen aus den küstenstaatlichen Rechten in der AWZ (Art. 58, 60 SRÜ) und dem allen Staaten zustehenden Freiheitsrecht, Kabel und Rohrleitungen zu legen sowie Anlagen zu errichten und zu betreiben (Art. 87 Abs.1 Buchst. c und d SRÜ).

2. Bundesberggesetz

Geht man davon aus, dass die Verwaltungsaufgaben nach dem BBergG auch die Maßnahmen zur Abwehr von Gefahren umfassen, die einer Anlage von außen drohen, so findet § 6 BPolG keine Anwendung auf bergbauliche Anlagen, da hierfür nach § 136 BBergG die Zuständigkeit der Länder gegeben ist. Für Rohrleitungen und Unterwasserkabel hingegen begründet

43 Wasserstraßen- und Schifffahrtsverwaltung des Bundes.
44 S. *Ehlers*, Recht des Seeverkehrs, 2. Auflage, 2022, SeeAufgG § 1 Rn. 25.
45 Seeschifffahrtsaufgaben-Übertragungsverordnung (BGBl. 1982 I 733).

§ 133 BBergG eine zweigeteilte Verwaltungszuständigkeit; davon werden bei Gasrohrleitungen auch deren Verdichterplattformen erfasst, da sie Bestandteil des Leitungssystems sind. In bergbaulicher Hinsicht sind die Länder und, soweit es die Ordnung der Nutzung und Benutzung der Gewässer und des Luftraumes betrifft, das BSH[46] als Bundesbehörde zuständig. Die Abwehr eines Anschlages dürfte den bergbaulichen Verwaltungsaufgaben zuzuordnen sein, denn es geht dabei um die Gewährleistung der Funktionsfähigkeit der Einrichtung, nicht aber um die Ordnung der Nutzung des Gewässers oder des Luftraumes. Die Länderzuständigkeit wird allerdings dadurch eingeschränkt, dass nach § 134 BBergG Überwachungsaufgaben den Vollzugsbeamten des Bundes, also der Bundespolizei, der Zollverwaltung und der WSV[47] zugewiesen werden. Allerdings bezieht sich diese Aufgabe nur auf bestimmte unbefugte Handlungen, von denen Anschläge gegen Einrichtungen nicht erfasst werden. Die Rechtslage wird dadurch weiter verkompliziert, dass generell der Vollzug von Verwaltungsakten, die auf der Grundlage des BBergG erlassen worden sind, den Vollzugsbeamten des Bundes auch dann zugewiesen wird, wenn sie von einer Landesbehörde erlassen worden sind. Auch diese verworrene und bei Anschlägen auf See kaum anwendbare Zuständigkeitsregelung deutet jedoch darauf hin, dass das BBergG und die darauf fußende Offshore–BergVO[48] auf den Schutz vor Gefahren ausgerichtet sind, die von einer Anlage ausgehen, jedoch den Anlagenschutz gegen Bedrohungen durch Dritte überhaupt nicht in die Regelungen einbeziehen. Mithin besteht insoweit eine Gesetzeslücke, die durch § 6 BPolG geschlossen wird.

3. Windenergie-auf-See-Gesetz und Seeanlagengesetz

Nach §§ 79 WindSeeG, 14 SeeAnlG obliegt die Überwachung der Anlagen dem BSH. Unklar ist, ob die „Überwachung" begrifflich auch Maßnahmen auf See einschließt und damit die bundespolizeiliche Zuständigkeit verdrängt. Dafür spricht die umfassende Verwendung dieses Begriffs in § 2 SeeFischG.[49] Auch in § 1 Nr. 1 SeeSchAÜV werden entsprechende Tätigkeiten auf See als Überwachung qualifiziert. Zudem legen die ausdrückliche

46 Bundesamt für Seeschifffahrt und Hydrographie.
47 § 6 Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (BGBl. III Gliederungsnummer 201-5).
48 Offshore-Bergverordnung (BGBl. 2016 I 1866).
49 S. *Ehlers* (Fn. 38), S. 98 f.

Einschränkung des § 134 Abs. 1 BBergG sowie die Delegationsmöglichkeiten nach § 3 Abs. 2 SeeAufgG, § 2 Abs. 7 SeeFischG und § 58 Abs. 2 BNatSch den Schluss nahe, dass die Überwachungsaufgaben der zuständigen Fachbehörde im Grundsatz umfassend sind und auf See zu ergreifende Maßnahmen der Gefahrenabwehr einschließen, weil es anderenfalls gar keiner Delegationsregelung bedarf.[50] Ähnlich wie beim BBergG lässt sich jedoch argumentieren, dass die Überwachung nicht auf die Abwehr von Gefahren, die einer Anlage drohen, ausgerichtet ist und diese Regelungslücke durch § 6 BPolG ausgefüllt wird.

4. Verfassungsrechtliche Zulässigkeit

Geht man davon aus, dass BBergG, WindSeeG und SeeAnlG den Schutz von Einrichtungen gegen Bedrohungen durch Dritte nicht regeln, setzt die Anwendung des § 6 BPolG voraus, dass eine Aufgabenzuweisung an die Bundespolizei als Teil der Bundesverwaltung mit mehrstufigem Verwaltungsaufbau verfassungsrechtlich zulässig ist. Angesichts der grundsätzlichen Zuständigkeit der Länder für allgemeinpolizeiliche Aufgaben bedarf es der Prüfung, ob dennoch eine entsprechende Wahrnehmungskompetenz des Bundes gegeben ist. Sie könnte sich allenfalls aus der fakultativen Bundeskompetenz nach Art. 87 Abs. 3 Satz 2 GG herleiten lassen. Danach können für neue Aufgaben, für die dem Bund die Gesetzgebung zusteht, bei dringendem Bedarf bundeseigene Mittel- und Unterbehörden eingerichtet werden.[51] Die entsprechende gesetzliche Regelung, die sich als Annexkompetenz auf Art. 74 Abs. 1 Nr. 11 GG stützt, bedarf der Zustimmung des Bundesrates. Zwar fehlt es daran beim BPolG, jedoch ist die Gefahrenabwehr auf See dem seinerzeitigen Bundesgrenzschutz bereits durch § 6 des mit Zustimmung des Bundesrates beschlossenen Bundesgrenzschutzgesetzes[52] zugewiesen worden. Die damals begründete Verwaltungskompetenz des Bundes gilt auch nach Aufhebung der einschlägigen BGSG-Regelungen fort, da der Bundespolizei nach § 1 Abs. 2 BPolG auch die Aufgaben obliegen, die ihr durch ein anderes Bundesgesetz, zu denen auch das Bundesgrenzschutzgesetz zu zählen ist, bis zum 1.11.1994 zugewiesen worden sind.

Als Ergebnis lässt sich somit feststellen, dass sich für unaufschiebbare Abwehrmaßnahmen auf See, soweit sie gegen Schiffe gerichtet sind, eine

50 S. *Ehlers* (Fn. 38), S. 102.
51 S. im Einzelnen *Ehlers* (Fn. 38), S. 95.
52 BGBl. 1972 I 1834.

delegierte Zuständigkeit von Bundespolizei und Zollverwaltung, bei Maßnahmen mit unmittelbarem Bezug zu einer Einrichtung die originäre Zuständigkeit der Bundespolizei rechtfertigen lässt, wenn auch letztere nicht völlig eindeutig geregelt erscheint.

III. Strafverfahrensrechtliche Befugnisse und Zuständigkeiten

1. Straftaten

Zusätzlich stellt sich die Frage, ob Maßnahmen statt auf die polizeiliche Gefahrenabwehr auf Befugnisse zur Erforschung von Straftaten gestützt werden können. Anschläge auf Einrichtungen erfüllen zumindest den Tatbestand der Sachbeschädigung (§ 303 StGB); bereits der Versuch ist mittlerweile strafbar. § 318 StGB, der die Beschädigung von Wasserbauten unter Strafe stellt, kommt hingegen nicht zur Anwendung, da nur Bauwerke erfasst werden, die der Regulierung, Speicherung, Leitung oder Abdämmung von Wasser dienen.[53] Grundvoraussetzung ist allerdings, dass das deutsche Strafrecht bei Einrichtungen auf See außerhalb des Küstenmeeres überhaupt Anwendung findet, da es im Wesentlichen nur im Inland gilt. Unproblematisch ist dies, sofern die Tat auf einem Schiff unter der Bundesflagge erfolgt (§ 4 StGB). Die erweiterte Anwendbarkeit deutschen Strafrechts bei Auslandstaten mit besonderem Inlandsbezug nach § 5 StGB kommt nicht in Betracht, da in Katalog der Auslandstaten die Sachbeschädigung nicht aufgelistet wird, es sei denn, dass die Beschädigung strafrechtlich relevante Umweltauswirkungen hat (§ 5 Nr. 11 StGB). Soweit es sich um feste Plattformen handelt, liegt jedoch eine Tat vor, die auf Grund eines zwischenstaatlichen Abkommens zu verfolgen ist (§ 6 Nr. 9 StGB), denn das SUA-Protokoll legt in Art. 2 entsprechende Straftatbestände fest und verpflichtet die Vertragsstaaten in Art. 3 zu deren Verfolgung. Bei anderen Einrichtungen kommt deutsches Strafrecht nach § 7 StGB nur dann zur Anwendung, wenn sie einem Deutschen gehören oder der Täter Deutscher ist. Das bedeutet im Ergebnis, dass die Strafbarkeit nach deutschem Recht sehr eingeschränkt und nur für solche Anschläge gegeben ist, an denen ein Schiff unter der Bundesflagge oder ein deutscher Täter beteiligt ist, es sich um eine feste Plattform handelt oder die betroffene Einrichtung einem Deutschen gehört.

53 MüKoStGB/*Wieck-Noodt*, 4. Aufl. 2022, StGB § 318 Rn. 6.

Im Verdachtsfall sind die Behörden des Polizeidienstes nach § 163 StPO befugt, Straftaten zu erforschen und zu diesem Zweck um Auskünfte zu ersuchen, Durchsuchungen vorzunehmen, Verdächtige festzunehmen und Gegenstände zu beschlagnahmen. Gem. §§ 4 SeeAufgG, 12 Abs. 5 S. 2 BPolG gilt die StPO für Seegebiete außerhalb des Küstenmeere entsprechend.[54] Voraussetzung ist, dass es sich dabei um die Erfüllung völkerrechtlicher Verpflichtungen oder die Wahrnehmung völkerrechtlicher Befugnisse handelt. Entsprechende Befugnisse und Verpflichtungen ergeben sich aus Art. 60 SRÜ, Art. 3 SUA-Protokoll und äußerst eingeschränkt aus Art. 10 des Telegraphenkabel-Vertrages. Soweit es sich um Ermittlungstätigkeiten mit Bezug auf Schiffe handelt, gelten dieselben völkerrechtlichen Einschränkungen wie bei den Maßnahmen zur Gefahrenabwehr. Als zuständige Polizeidienststelle legt § 12 Abs. 1 Nr. 6 BPolG die Auffangzuständigkeit der Bundespolizei fest, wenn Strafverfolgungsmaßnahmen seewärts des deutschen Küstenmeeres im Rahmen des § 6 BPolG erforderlich sind. Die Bezugnahme auf § 6 BPolG ist so zu verstehen, dass die Verfolgungsbefugnis völkerrechtskonform sein muss und dass die Bundespolizei gem. § 6 Satz 2 BPolG dann nicht zuständig ist, wenn eine Zuständigkeit anderer Behörden für Maßnahmen auf See besteht. Die alternative Zuständigkeitsregelung des § 148 Abs. 2 BBergG, nach der neben den im UZwG genannten Vollzugsbeamten des Bundes, also Bundespolizei, Zollverwaltung und WSV, auch das BSH sowie die jeweiligen Landesbehörden zuständig sind, ist nicht einschlägig, da sie nur für Straftaten nach § 146 BBergG gilt. Eine eigenständige Zuständigkeitsregelung folgt aus § 1 Nr. 3 Buchst. d Doppelbuchst. bb SeeAufgG iVm § 1 Nrn. 1-2 ZustBV-See.[55] Danach sind bei Straftaten, die auf Schiffen unter der Bundesflagge begangen werden sowie auf Schiffen unter fremder Flagge im Falle einer in § 1 Nr. 2 ZustBV aufgelisteten Straftat die Bundespolizei und in eingeschränktem Maße die Zollverwaltung, daneben in bestimmten Fällen auch die Beamten der WSV mit strom- und schifffahrtspolizeilichen Befugnissen zuständig. Allerdings sind Sachbeschädigungen und das SUA-Protokoll in der Auflistung nicht enthalten, so dass sich aus der ZuStBV keine Zuständigkeit ergibt. Ein Rückgriff auf die allgemeine Verfolgungszuständigkeit der Bundespolizei nach § 12 Abs. 1 Nr. 6 BPolG erscheint äußerst problematisch, da es sich gerade nicht um eine Tätigkeit im Rahmen des § 6 BPolG handelt, sondern § 1 Nr. 3 Buchst. d Doppelbuchst. bb SeeAufgG Rechtsgrundlage ist. Im Ergebnis

54 S. *Ehlers* (Fn. 44), SeeAufgG § 4 Rn. 1.

55 Zuständigkeitsbezeichnungs-Verordnung See (BGBl. 1994 I 442).

bleibt festzustellen, dass Strafverfolgungsmaßnahmen auf See gegenüber Schiffen nur sehr eingeschränkt möglich sind.

2. Ordnungswidrigkeiten

Dem Schutz von Einrichtungen dienende Bußgeldtatbestände sind weder durch das BBergG noch das WindSeeG und das SeeAnlG ausgewiesen worden. Lediglich das Befahren der um eine Anlage errichteten Sicherheitszone stellt nach § 9 Abs. 1 Nr. 5 KVRV eine Ordnungswidrigkeit dar. Für Ermittlungstätigkeiten auf See sind in diesem Fall die Bundespolizei und die Zollverwaltung nach § 1 Abs. 1 SeeSchAÜV iVm §§ 1 Nr. 3 Buchst. d Doppelbuchst. aa, 4 Abs. 2 SeeAufgG zuständig.

D. Verpflichtung des Betreibers

Im Rahmen einer Gesamtbetrachtung müsste auch erörtert werden, inwieweit dem Betreiber einer Einrichtung aufgegeben werden kann, für die notwendige Überwachung der Einrichtung zu sorgen, um Anschläge zu verhindern, soweit er dazu nicht ohnehin aus Eigeninteresse bereit ist.[56] Diese Thematik bedarf einer zusätzlichen eigenständigen Untersuchung, die hier nicht erfolgen kann. Festzuhalten ist aber, dass weder das BBergG noch das WindSeeG und das SeeAnlG dazu ermächtigen, im Rahmen des Planfeststellungs- oder Genehmigungsverfahrens anzuordnen, dass Errichter und Betreiber einer Einrichtung selbst für die notwendige Überwachung zum Schutz der Einrichtung zu sorgen haben. Die einschlägigen Vorschriften sind lediglich auf die Vermeidung von Gefahren ausgerichtet, die von der Anlage ausgehen. Es wäre daher zu erwägen, die einschlägigen Gesetze durch entsprechende Befugnisse zu ergänzen. Ein etwas anderer Weg soll mit dem KRITIS-DachG beschritten werden, das sich hoffentlich nicht zu einem neuen Bürokratiemonster entwickelt. Danach sollen Betreiber einer durch Verordnung als kritisch bestimmten Anlage verpflichtet werden, geeignete Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen.[57] Es bleibt abzuwarten, in welcher Fassung das Gesetz schließlich verabschiedet

56 Vgl. zur Problematik auch *Brake*, Schutz maritimer Infrastruktur: Von den Grenzen staatlichen Handelns und Eigenverantwortung der Betreiber, Schiff&Hafen 2023, Heft 7/8, S. 46, 48.

57 § 1 iVm § 4 des Entwurfs (Fn. 5).

werden wird und ob und welche Einrichtungen auf See als kritisch bewertet werden.

E. Bewertung

Zusammenfassend muss festgestellt werden, dass der Schutz der Infrastruktur auf See zahlreiche, bisher ungeklärte Rechtsfragen aufwirft, die sowohl die völkerrechtlichen Grundlagen als auch die innerstaatlichen Befugnisse betreffen. Auf der 13. Nationalen Maritimen Konferenz wurde in diesem Zusammenhang von Küstennebel gesprochen. Noch zutreffender wäre wohl Seenebel. Dieser Nebel muss dringend aufgelöst werden. Für die im konkreten Fall zum Handeln aufgerufenen Behörden ist es unerlässlich, dass sie sich auf eine hinreichend eindeutige Rechtsgrundlage stützen können. Es ist daher in einem ersten Schritt dringendst geboten, die Thematik in einer umfassenden Studie genau zu untersuchen. Schon jetzt zeigt sich aber, wie unvollkommen auf nationaler Ebene das Ordnungsrecht auf See geregelt ist, das sich, bedingt durch die historische Entwicklung, aus zahlreichen, nicht aufeinander abgestimmten Einzelvorschriften zusammensetzt. Ohne den Ergebnissen einer gründlichen Studie vorzugreifen, lässt sich schon jetzt erkennen, wie wichtig es wäre, zumindest den Bereich der deutschen AWZ endlich durch ein in sich stimmiges Gesetz zu regeln.[58] Ganz entscheidend für den Schutz der Einrichtungen wird es jedoch sein, dass mit Hilfe technischer Mittel der Zustand der Einrichtungen und der sie umgebende Seeraum wirksam überwacht und, wenn erforderlich, jederzeit aktuelle Lagebilder erstellt werden und dass entsprechend befugte Einsatzkräfte schnell vor Ort sind. Das alles erscheint ohne Nutzung der speziellen Kapazitäten der Marine in der Praxis kaum erfolgversprechend. Nicht ohne Grund wird das Thema auch in der NATO behandelt. Ein Einsatz der Marine stößt, wenn es um mehr als nur die bloße Lagebeobachtung geht, jedoch sehr schnell an verfassungsrechtliche Grenzen. Wäre es daher nicht an der Zeit, die Zuständigkeitsregelung des Grundgesetzes für die innere und äußere Sicherheit[59] bei Vorfällen auf See außerhalb des Hoheitsgebiets zu überdenken und der Marine größere Befugnisse zuzuerkennen?

58 S. dazu bereits *Ehlers* (Fn. 38), S. 108; *Schiebert*, Marinebund fordert Seesicherheitsgesetz, Leinen los!, Heft 12, 2023, S. 12.

59 Art. 87 GG.

Der Schutz unterseeischer Datenkabel

Völkerrechtliche Hürden für die Verteidigung maritimer Infrastrukturen im hoheitsfreien Raum

Michael Stadermann[*]

Der vorliegende Beitrag widmet sich den völkerrechtlichen Fragestellungen im Zusammenhang mit dem Schutz unterseeischer Datenkabel auf der Hohen See. Diese Kabel, die eine zentrale Rolle für die globale Datenkommunikation spielen, sind sowohl physisch verletzlich als auch rechtlich unzureichend geschützt. Im Mittelpunkt der Untersuchung stehen die völkerrechtlichen Rahmenbedingungen des Seerechtsübereinkommens sowie der Charta der Vereinten Nationen, insbesondere im Hinblick auf das Gewaltverbot und das Flaggenstaatsprinzip. Der Beitrag analysiert die bestehenden rechtlichen Hindernisse für einen effektiven Schutz dieser Infrastrukturen in der Hohen See und identifiziert Lücken im geltenden internationalen Rechtsrahmen.

A. Einleitung

I. Seekabel als bedeutsame Infrastruktur

Der heutige Alltag ist von allgegenwärtiger Datenkommunikation durchdrungen. Unser Privat- und Berufsleben ist ohne Anbindung an das globale Datennetz kaum mehr vorstellbar: Ob die Überprüfung der Zugpünktlichkeit, das Hören eines Podcasts auf dem Weg zur Arbeit, der E-Mail-Austausch mit Kollegen, die Internetrecherche, der Einkauf im Onlinehandel, weltweite Finanztransaktionen oder das Streaming einer Serie am Feierabend – all dies sind nur wenige Beispiele für die tiefgreifende Abhängigkeit unserer Gesellschaft von einer reibungslos funktionierenden Dateninfrastruktur. Es ist ein verbreiteter Irrtum, dass der Großteil dieser

* Dr. Michael Stadermann, DLR - Institut für den Schutz maritimer Infrastrukturen, E-Mail: michael.stadermann@dlr.de, Forschungsschwerpunkte: Recht & Neue Technologien, Maritime Infrastrukturen, Autonome Schifffahrt.

Dienstleistungen durch lokale Datennetze oder durch Satellitenkommunikation ermöglicht wird. Regelmäßig sind internationale Server an unseren Online-Dienstleistungen beteiligt und sobald Datenverkehr internationale Wege nimmt, sind Seekabel der bevorzugte Übertragungsweg. Es wird geschätzt, dass bis zu 99 Prozent der internationalen versendeten Daten Seekabel als wesentlichen Übertragungsweg nutzen.[1] Entsprechend wird das weltweite Netz aus Unterseekabeln nicht selten auch als das Rückgrat des Internets bezeichnet.[2]

Ein Ausfall dieser Infrastruktur wäre mit erheblichen Störungen bis hin zum Ausfall zahlreicher Internet-Dienstleistungen verbunden. Die Konsequenzen für unsere digitalisierte Gesellschaft wären gleichermaßen für Privatpersonen als auch für den Wirtschaftssektor immens.[3] Aufgrund der Bedeutung des Seekabelnetzwerkes wurden im Jahr 2023 die Anlandestationen für Seekabel und damit deren Anbindung an die nationalen Telekommunikationsnetze in der BSI-Kritisverordnung[4] als Kritische Infrastruktur eingestuft.[5]

II. Vulnerabilität der Infrastruktur Seekabel

Ausgehend von der Bedeutung dieser Infrastruktur für unsere Gesellschaft stellt sich die Frage, wie resilient das Seekabelnetz gegenüber Schäden und Ausfällen ist. Bei der Untersuchung dieser Frage ist es sinnvoll, zwischen physischen und rechtlichen bzw. rechtspolitischen Faktoren der Resilienz zu differenzieren.

Heutige Seekabel sind zumeist Glasfaserkabel, die auf dem Grund der Weltmeere verlegt werden, um die Kommunikation von großen Datenmengen über große Distanzen, beispielsweise zwischen dem Festland und Inseln oder zwischen Kontinenten zu ermöglichen. Aufgrund der immensen

1 *Winseck*, The Geopolitical Economy of the Global Infrastructure, in: Journal of Information Policy, 7/2017, 228 (237); *Bueger et. al.*, Security threats to undersea communications cables and infrastructure – consequences for the EU, S.15.

2 *Podbregar*, Angriffsziel Unterseekabel, https://www.scinexx.de/dossier/angriffsziel-unterseekabel/, zuletzt abgerufen am 27.10.2024.

3 Vgl. *Bueger et. al.*, S. 15 f, s.o. Fn. 1.

4 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339).

5 Anhang 4 Teil 1 Nr. 2.3, Teil 3 Nr. 1.2.2 BSI-KritisV.

Bandbreiten von aktuell bis zu 224 Terabit/Sekunde und geringen Latenzen stellen Seekabel insbesondere im Vergleich zur Satellitenkommunikation das kostengünstigere und performantere Übertragungsnetz dar.[6] Der Aufbau eines typischen Seekabels umfasst zunächst die Glasfaserstränge im Kern des Kabels, ummantelt von Kupfer, Verbundstoffen und Aluminium, um die Glasfasern vor eindringendem Salzwasser zu schützen. Je nach Lage des Kabels wird der Kern durch mehrere Schichten aus Stahlseilen und Kunststoffen verstärkt, um ihn gegenüber physischen Einwirkungen robuster zu gestalten. Abhängig von der Tiefe des Meeresbodens und den typischen Aktivitäten im betroffenen Seegebiet variiert die Stärke eines Seekabels erheblich: Sie reicht von der Dicke eines Gartenschlauchs bis hin zu armdicken Querschnitten. Werden Seekabel in Küstennähe verlegt, so werden diese zudem für einen zusätzlichen Schutz im Meeresboden verbuddelt.[7] Mit mindestens 80 Prozent liegt der weit überwiegende Anteil des Seekabelnetzes in einer Meerestiefe von mehr als 1000 Metern, was aufgrund der damit verbundenen schweren Erreichbarkeit bereits einen eigenständigen Schutz dieser Kabel darstellt.[8] Gleichwohl ereignen sich Vorfälle, die zu einer Beschädigung oder gar zu einem Zerreißen eines Seekabels führen, nahezu alltäglich. Im Mittel kommt es jährlich und weltweit zu ca. 100 Schadensereignissen an Seekabeln.[9] Verursacht werden diese Ereignisse vorrangig durch Aktivitäten in den Bereichen Fischerei und Schifffahrt, insbesondere durch Schleppnetze und Schleppanker.[10] Für die mutwillige Zerstörung eines Seekabels bedarf es folglich keiner Spitzentechnologie oder gar militärischer Technologie. Schiffe mit Schleppanker oder alterna-

6 TeleGeography, Submarine Cable Frequently Asked Questions, 2024, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions, zuletzt abgerufen am 27.10.2014.

7 *Swinhoe*, What is a submarine cable? Subsea fiber explained, 2021, https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/, zuletzt abgerufen am 27.10.2024.

8 *Franken*, Seekabel als Maritime Kritische Infrastruktur, in: Schilling, Dreizack 21: Von historischen bis zukünftigen Herausforderungen im maritimen Raum, https://www.kielseapowerseries.com/files/ispk/content/workshops/Dreizack/Sammelband%20zum%20Dreizack21.pdf, zuletzt abgerufen am 27.10.2024.

9 *Mauldin, Swinhoe*, Cable Breakage: When and How Cables Go Down, 2017, https://blog.telegeography.com/what-happens-when-submarine-cables-break, zuletzt abgerufen am 27.10.2024; *Swinhoe*, s.o. Fn. 6.

10 *Patalong*, Die fragilen Lebensadern des Internets, 2015, https://www.spiegel.de/netzwelt/web/untersee-kabel-die-fragilen-lebensadern-des-internets-a-1015809.html, zuletzt abgerufen am 27.10.2024; *Franken*, s.o. Fn. 8.

tiv Taucher bzw. ferngesteuerte Tauchsysteme (ROV) aus der maritimen Wirtschaft mit einer hydraulischen Schere würden regelmäßig ausreichen.

Das Seekabelnetz umfasst im Jahr 2024 ein System von mehr als 600 Kabeln mit einer Gesamtlänge von ca. 1,4 Millionen Kilometern. Die Länge einzelner Seekabel variiert erheblich: Während kürzere Kabel von wenigen Kilometern häufig zur Anbindung von Inseln dienen, erreicht das Seekabel 2Africa beeindruckende 45.000 Kilometer. Es beginnt und endet in Europa und umspannt den gesamten afrikanischen Kontinent, wobei es zahlreiche afrikanische Staaten an das globale Datennetz anschließt.[11] Sowohl die Größe des Kabelnetzes als auch dessen Lage in teilweise mehreren tausend Metern Tiefe erschweren sowohl die Überwachung der gesamten Infrastruktur als auch deren unmittelbaren Schutz, beispielsweise durch patrouillierende Schiffe. Stark abhängig von der jeweiligen Weltregion ist die zugrunde liegende Dienstleistung der globalen Datenkommunikation durch Redundanzen, also durch mehrfache Kabelverbindungen zwischen den verbundenen Teilen der Welt, geschützt. So ist die EU durch eine Vielfalt von ca. 250 Kabeln an das globale Internet angebunden, ein Drittel davon terrestrisch verlegt, zwei Drittel als maritime Seekabel. Infolge dieser Kapazitäten können Ausfälle von Komponenten sowie einzelner Kabelverbindungen in der Regel durch alternative Kabelanbindungen kompensiert werden. Um signifikante Störungen der europäischen Anbindung an die globale Datenkommunikation zu bewirken, bedürfte es einer umfassenden und koordinierten Sabotageaktion an einer Vielzahl von Kabeln.[12] Zu derartigen Sabotageaktionen werden regelmäßig nur Staaten in der Lage sein. Die Inselstaaten und Überseegebiete der EU sowie zahlreiche Regionen der Welt verfügen dagegen über deutlich geringere bis keine Redundanzen. In manchen Regionen der Welt kann ein Sabotageakt an nur einem Seekabel zu einem umfassenden Ausfall der dortigen Datenkommunikation führen.[13] Eine Reparatur von beschädigten oder zerrissenen Seekabeln ist mit Hilfe spezialisierter Dienstleistungsunternehmen durchführbar. Abhängig von

11 TeleGeography, Submarine Cable Map, 2024. https://www.submarinecablemap.com/, zuletzt abgerufen am 27.10.2024.

12 Vgl. *Bueger et. al.*, S.16 u. S. 30, s.o. Fn. 1.

13 *Franken et. al.*, The digital divide in state vulnerability to submarine communications cable failure, 2022, https://www.sciencedirect.com/science/article/pii/S1874548222000130, zuletzt abgerufen am 27.10.2024; *Doherty, McClure*, Tonga could be cut off for weeks amid efforts to repair undersea communications cable, 2022, https://www.theguardian.com/world/2022/jan/18/tonga-could-be-cut-off-for-weeks-amid-efforts-to-repair-undersea-communications-cable, zuletzt abgerufen am 27.10.2024.

der Lage des Defekts kommen Taucher oder ferngesteuerte Tauchroboter zum Einsatz. Die Reparatur eines Kabels kann je nach Lage und Ausmaß des Schadens einige Tage bis wenige Monate dauern.[14]

Ein weniger offensichtlicher Faktor für die Vulnerabilität der Infrastruktur Seekabel ist in der internationalen Regulierung des Komplexes Seekabel zu finden. Ein Großteil des Seekabelnetzes liegt nicht nur außerhalb nationaler Küstenmeere, sondern ebenso außerhalb der Ausschließlichen Wirtschaftszonen im Bereich der Hohen See. Die Hohe See unterliegt keiner staatlichen Hoheitsgewalt, was rechtliche Herausforderungen für den Schutz der Seekabel in diesem Gebiet verursacht. Diesen völkerrechtlichen Rechtsfragen zum Schutz von Seekabeln im hoheitsfreien Raum widmet sich im Schwerpunkt der gegenständliche Beitrag.

III. Aktualität der Thematik

Die Notwendigkeit, unterseeische Infrastrukturen schützen zu müssen, wurde der Öffentlichkeit durch die Sprengstoff-Anschläge auf die Erdgas-Pipelines Nord Stream 1 und Nord Stream 2 erst kürzlich im Jahr 2022 verdeutlicht.[15] Die Lage der jeweiligen Tatorte in der Nähe der Insel Bornholm aber nicht im Hoheitsgebiet Dänemarks, sondern in der Ausschließlichen Wirtschaftszone (AWZ) Dänemarks bzw. Schwedens wurde nicht zufällig gewählt. Die Angreifer vermieden durch die Wahl der Anschlagsorte einen direkten Anschlag auf nationales Territorium. Der Anschlagsort offenbarte zudem Schwierigkeiten bei einer multinationalen Aufklärung von Vorfällen jenseits der Küstenmeere.[16] Damit verdeutlichen die Anschläge die Bedeutung aber auch die Schwächen des internationalen Rechts bei Konflikten in diesen Gewässern. Unterseeische Daten- und Kommunikationskabel queren im Gegensatz zu Pipelines, die überwiegend in Küstenmeeren und den sich anschließenden Wirtschaftszonen verlaufen, die Weltmeere, sodass sie folglich zu einem Großteil ihres Verlaufs im Bereich der Hohen See liegen.

14 *Kuhn*, Anschlagsziel Seekabel: So verwundbar ist der globale Datenverkehr, 2023, https://www.wiwo.de/technologie/digitale-welt/infrastruktur-unter-wasser-anschlagsziel-seekabel-so-verwundbar-ist-der-globale-datenverkehr/29027946.html, zuletzt abgerufen am 27.10.2024.

15 *Schwarte*, Drei Lecks an Nord-Stream-Pipelines, 2022, https://www.tagesschau.de/wirtschaft/nord-stream-eins-druckabfall-101.html, zuletzt abgerufen am 27.10.2024.

16 *Götschenberg*, Keine gemeinsamen Ermittlungen, 2022, https://www.tagesschau.de/inland/gesellschaft/nordstream-pipelines-ermittlungen-101.html, zuletzt abgerufen am 27.10.2024.

Entsprechend größer ist die Bedeutung des internationalen Rechts für die Infrastruktur Seekabel.

Vorfälle der vergangenen Jahre haben gezeigt, dass auch diese weltumspannende Infrastruktur durch Anschläge bedroht ist. So wurden im Oktober 2022 drei Unterseekabel vor Marseille gekappt, was weltweite Internet- und Verbindungsprobleme verursachte. Zur gleichen Zeit im Oktober 2022 wurden beide Seekabel der Shetland-Inseln, sowohl Richtung Färöer als auch Richtung Schottland, zerstört, sodass die Inselgruppe für wenige Tage vom Internet abgeschnitten war.[17] Die Verursacher dieser Vorfälle konnten nicht ermittelt werden, sodass Spekulationen verbleiben, es könnte sich um Sabotageakte gehandelt haben.[18] Als Konsequenz der Nord Stream-Anschläge gründete die NATO eine Koordinationszelle zum Schutz von Unterwasserinfrastruktur mit dem Ziel, diese Infrastrukturen, also Pipelines und Seekabel, zukünftig besser zu monitoren und ggf. Angreifer zu identifizieren.[19]

IV. Szenario und Rechtsgrundlagen

Der gegenständliche Beitrag soll an dieser Initiative anknüpfen und den hypothetischen Fall betrachten, dass das Monitoring durch die NATO erfolgreich ist, ein Angriff auf der Hohen See rechtzeitig bemerkt wird, sodass der Anschlag vereitelt und der Angreifer gestellt werden könnte. In einer solchen Situation stellt sich die Frage, ob und mit welchen Mitteln Unterseekabel geschützt werden dürfen.

Wenn bei koordinierten Anschlägen auf die Seekabel-Infrastruktur regelmäßig von staatlich veranlassten Sabotageakten auszugehen ist, stellt sich die Frage, ob betroffene Staaten berechtigt wären, militärische Gewalt zur Vereitelung dieser Anschläge anzuwenden. Die Voraussetzungen

17 *Holland*, Zwei Unterseekabel beschädigt: Shetlandinseln vom Internet abgeschnitten, 2022, https://www.heise.de/news/Zwei-Unterseekabel-beschaedigt-Shetlandinseln-vom-Internet-abgeschnitten-7315534.html, zuletzt abgerufen am 27.10.2024.

18 *Bollmann*, Zerstörte Unterseekabel in Europa – sind russische Fischtrawler schuld?, 2022, https://www.20min.ch/story/zerstoerte-unterseekabel-in-europa-sind-russische-fischtrawler-schuld-302741769825, zuletzt abgerufen am 27.10.2024.

19 NATO, NATO stands up undersea infrastructure coordination cell, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm, zuletzt abgerufen am 27.10.2024; *Tiedke*, Deutscher Ex-General leitet NATO-Zelle zum Schutz von Unterwasserinfrastruktur, 2023, https://www.bmvg.de/de/aktuelles/verbesserungen-schutz-kritischer-unterwasserinfrastruktur-5616738, zuletzt abgerufen am 27.10.2024.

hierzu finden sich in den Vorschriften zur Friedensicherung gemäß Kapitel VI der Charta der Vereinten Nationen (UN-Charta).[20] Ob betroffene Staaten zu nicht-militärischen hoheitlichen Eingriffen gegenüber potentiellen Angreifern berechtigt sind, bemisst sich am internationalen Rechtsrahmen für Unterseekabel. In diesem Zusammenhang sind insbesondere zwei internationale Konventionen von Bedeutung: Zum einen der Internationale Vertrag zum Schutze der unterseeischen Telegraphenkabel von 1884 (Kabelschutzkonvention)[21], der noch heute gilt. Zum anderen das Seerechtsübereinkommen der Vereinten Nationen (SRÜ) von 1982[22], das viele Regelungen der Kabelschutzkonvention übernommen hat. Dass zu der bestehenden internationalen Regulierung von Untersee-Infrastrukturen wie z. B. Pipelines und Seekabeln Forschungs- bzw. Klärungsbedarf besteht, zeigt die Einrichtung eines Ausschusses für Unterwasserkabel und Pipelines durch die International Law Association (ILA) im Jahr 2018.[23] Dieser Ausschuss soll rechtliche Probleme im Zusammenhang mit unterseeischen Infrastrukturen identifizieren, Lücken im geltenden Recht aufzeigen und konkrete Empfehlungen geben, wie der rechtliche Rahmen verbessert werden könnte.[24] Dieser Beitrag gibt einen Überblick zu den in diesem Kontext relevanten Rechtsvorschriften und deren Auswirkungen auf den Schutz unterseeischer Datenkabel.

B. Ius contra bellum

Die Frage, ob betroffene Staaten bevorstehende Anschläge auf Unterseekabel mit militärischer Gewalt vereiteln dürfen, bemisst sich insbesondere nach den Vorschriften der UN-Charta, die das „Ius contra bellum" bzw. das Recht der Friedenssicherung kodifiziert. Die danach zulässigen Möglich-

20 Charta der Vereinten Nationen, Vertragsschluss am 26.06.1945, in Kraft am 24.10.1945 (UN Charta).

21 Internationaler Vertrag zum Schutze der unterseeischen Telegraphenkabel, Vertragsschluss 14.03.1884, in Kraft am 01.05.1888 (Kabelschutzkonvention).

22 Seerechtsübereinkommen der Vereinten Nationen, Vertragsschluss am 10.12.1982, in Kraft am 16.11.1994, 1833 UNTS 397 (SRÜ).

23 Selbstverständlich existierte bereits zuvor vereinzelte Forschung zu diesen Fragestellungen, vgl. *Wolf*, Unterseeische Rohrleitungen und Meeresumweltschutz, 2011.

24 ILA, Proposal for establishment of a new ILA Committee on submarine cables and pipelines under international law, 2018, https://www.ila-hq.org/en_GB/committees/submarine-cables-and-pipelines-under-international-law, zuletzt abgerufen am 27.10.2024.

keiten, die Staaten zur Verfügung stehen, um sich gegen Gewalt bzw. Angriffe zu verteidigen, hängen von der Art bzw. der rechtlichen Einordnung dieser Angriffe ab. Bewaffnete Angriffe gegen einen Staat rechtfertigen eine militärische Selbstverteidigung gem. Art. 51 UN-Charta. Verstöße gegen das Gewaltverbot aus Art. 2 Nr. 4 UN-Charta, die nicht die Voraussetzungen eines bewaffneten Angriffs erfüllen, können gem. Art. 39 – 42 UN-Charta ggf. durch Maßnahmen des Sicherheitsrates sanktioniert werden. Die Einordnung eines Anschlages auf Unterseekabel in dieses System wird nachfolgend erörtert.

I. Recht auf Selbstverteidigung gem. Art. 51 UN-Charta

Das Völkerrecht verbietet grundsätzlich bewaffnete Gewalt zwischen Staaten, was als Verbot der Gewaltanwendung in Art. 2 Nr. 4 UN-Charta kodifiziert ist. Dieser Grundsatz des Verbots von Gewaltanwendung gilt für internationale Beziehungen, insbesondere – aber nicht abschließend – zwischen Staaten.[25] Als einzige Ausnahmen vom Verbot der Gewaltanwendung nennt die UN-Charta zum einen Maßnahmen, die durch den Sicherheitsrat nach Art. 39 ff. gestattet werden, und zum anderen die Ausübung des Rechts auf Selbstverteidigung gem. Art. 51. Unmittelbare militärische Reaktionen auf einen Anschlag sind für betroffene Staaten entsprechend nur als Selbstverteidigung in Folge eines bewaffneten Angriffs zulässig. Unter einem bewaffneten Angriff iSd Art. 51 UN-Charta wird der intensive Einsatz der Streitkräfte eines Staates gegen die Souveränität oder die Streitkräfte eines anderen Staates verstanden, in der Regel mit dem Ziel, in dessen Territorium einzudringen.[26]

Dieser Definition folgend erscheint es aus mehreren Gründen höchst fraglich, dass Anschläge auf Unterseekabel als bewaffnete Angriffe iSd Art. 51 UN-Charta einzuordnen wären. Ein erster Grund liegt in den typischen Mitteln, die für die Durchführung eines Sabotageaktes an Untersee-

25 Vgl. *Bruha*, Gewaltverbot und humanitäres Völkerrecht nach dem 11. September 2001, Archiv des Völkerrechts 12/2002, 383 (389 ff.); *Dau*, Die völkerrechtliche Zulässigkeit von Selbstverteidigung gegen nicht-staatliche Akteure, 2017, S. 58 ff.

26 Vgl. United Nations General Assembly, 1974. Resolution 3314 (XXIX) - Definition of Aggression, A/RES/3314(XXIX), Definition von Aggression in Art. 3; Internationaler Gerichtshof (IGH), 1986. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), No. 070-19860627-JUD-01-00-EN. https://www.icj-cij.org/node/103143, Rn. 195, zuletzt abgerufen am 27.10.2024.

kabeln erforderlich sind. Wie bereits aufgezeigt, reichen für die Zerstörung von Seekabeln regelmäßig herkömmliche Schiffe, beispielsweise Fischerboote, mit Schleppnetzen oder Schleppankern aus. Auch der Einsatz von ferngesteuerten Tauchrobotern mit entsprechenden Schneidevorrichtungen wäre als Verwendung von maritimem Industrie-Equipment und nicht als Einsatz von militärischem Equipment einzuordnen. Selbst die Verwendung militärischer Mittel, z. B. Sprengstoffe, wäre ggf. nicht als bewaffneter Angriff zu werten, wenn sie im Schweregrad dem Einsatz durch reguläre Streitkräfte nicht gleichkäme.[27] Zudem zielt der Begriff des bewaffneten Angriffs, der sich gewohnheitsrechtlich an der Aggressionsdefinition der UN-Generalversammlung orientiert, auf den Schutz der Souveränität, der territorialen Unversehrtheit und der politischen Unabhängigkeit des angegriffenen Staates.[28] Die Auswirkungen eines Sabotageaktes an einem Unterseekabel werden regelmäßig keine derart drastischen Folgen haben, dass diese Rechtsgüter der betroffenen Staaten tangiert werden. Vielmehr ist es wahrscheinlich, dass redundante Datenverbindungen den Ausfall kompensieren und dies maximal zu Verbindungsproblemen oder reduzierten Geschwindigkeiten der Datenverbindungen führt. Für Staaten oder Regionen, die nicht über ausreichende Redundanzen verfügen, mögen die Konsequenzen drastischer sein. Die verursachten Schäden werden aber auch dort vorrangig wirtschaftlicher Natur sein.[29]

Die Besonderheit eines Anschlags auf der Hohen See wirft außerdem die Frage auf, welcher Staat mit dem Anschlag eigentlich angegriffen wird. Seekabel verfügen über mindestens zwei Anlandungspunkte, können aber auch über dutzende verfügen. Die dahinterstehende Datenverbindung mit ihren Kapazitäten wird in der Regel von ganzen Regionen und einer Vielzahl von Staaten genutzt.[30] Als Betreiber der Kabel agieren regelmäßig multinationale Unternehmenskonsortien. Wäre es sachgerecht, einen Anschlag im hoheitsfreien Raum als einen Angriff auf eine Vielzahl von Staaten zu werten? Diese Frage bleibt im Beitrag unbeantwortet. Im Ergebnis ist fest-

27 IGH (Nicaragua v. United States of America), Rn. 195, s.o. Fn. 26.

28 *Dau*, Die völkerrechtliche Zulässigkeit von Selbstverteidigung gegen nicht-staatliche Akteure, 2017, S. 55 ff.

29 *Davenport*, Intentional Damage to Submarine Cable Systems by States, 2023, S. 11, https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf, zuletzt abgerufen am 27.10.2024.

30 TeleGeography, Submarine Cable Map, 2Africa, 2024, https://www.submarinecablemap.com/submarine-cable/2africa, zuletzt abgerufen am 27.10.2024.

zuhalten, dass ein Anschlag auf Seekabel regelmäßig nicht als bewaffneter Angriff zu qualifizieren ist.

Losgelöst von den vorstehenden Gegenargumenten muss zusätzlich darauf aufmerksam gemacht werden, dass dem Wunsch, Anschläge zu vereiteln, nur für solche Anschlagsszenarien mit einer Selbstverteidigung gem. Art. 51 UN-Charta abgeholfen werden könnte, bei denen ausreichend Nachweise für einen unmittelbar bevorstehenden Angriff vorliegen.[31] Eine hypothetische, vorbeugende bzw. präemptive Selbstverteidigung wird im völkerrechtlichen Schrifttum überwiegend als unzulässig abgelehnt.[32] Ein präventives Tätigwerden des Militärs ist somit auf das Zuvorkommen eines beginnenden bewaffneten Angriffs beschränkt. Die Grenzziehung zwischen der Verteidigung bevorstehender Angriffe und einer unzulässigen vorbeugenden Verteidigung erfolgt dabei graduell und ist mit einer gewissen Unschärfe konfrontiert.[33] Bezogen auf Sabotageakte an Seekabeln würden sich damit im Vorfeld des Anschlages regelmäßig Unsicherheiten ergeben, ob ausreichend Anhaltspunkte für einen unmittelbar bevorstehenden Angriff vorliegen. In Zeiten hybrider und verdeckter Kriegsführung und der Verwendung ziviler Technologien für militärische Zwecke dürfte die Gewissheit eines bevorstehenden Angriffes zunehmend fraglich sein.

II. Das Gewaltverbot gem. Art. 2 Nr. 4 UN-Charta

Die Anwendung von Gewalt zwischen Staaten ist gem. Art. 2 Nr. 4 UN-Charta grundsätzlich untersagt. Für den Gegenstand dieses Beitrages – Sabotageakte an Seekabeln – stellen sich die Fragen, ob diese gegen das Gewaltverbot verstoßen und ob etwaige Sanktionen zum Schutz der Infrastruktur beitragen. Als Tatbestandsvoraussetzungen des Art. 2 Nr. 4 UN-Charta müssen die nachfolgenden Kriterien erfüllt sein, um eine Verletzung des Gewaltverbots annehmen zu können. Der Angriff muss von einem

31 *Dörr*, Gewalt und Gewaltverbot im modernen Völkerrecht, Aus Politik und Zeitgeschichte 43/2004, 2004, 14 (16 f.), https://www.bpb.de/system/files/pdf/78TS50.pdf, zuletzt abgerufen am 27.10.2024.

32 Vgl. *Murswiek*, Die amerikanische Präventivkriegsstrategie und das Völkerrecht, NJW 2003, 1014 (1016 ff.); darstellend Wissenschaftliche Dienste des Deutschen Bundestages, Zum Konzept der präemptiven Selbstverteidigung, WD 2 – 3000-049/07, 2007, https://www.bundestag.de/resource/blob/414640/44a2b7337d3b8fd94962639cb365c9c8/WD-2-049-07-pdf-data.pdf, zuletzt abgerufen am 27.10.2024.

33 *Dörr*, S. 17, s.o. Fn. 31.

Staat ausgehen und durch seine Auswirkungen die internationalen Beziehungen beeinträchtigen. Er muss auf die territoriale Integrität oder die politische Unabhängigkeit eines anderen Staates abzielen oder in sonstiger Weise mit den Zielen der Vereinten Nationen unvereinbar sein. Da es umstritten ist, ob private Angreifer im Allgemeinen unter Art. 2 Nr. 4 UN-Charta fallen,[34] geht der vorliegende Beitrag von einem staatlich durchgeführten oder mindestens staatlich initiierten Anschlag aus. Ein Anschlag auf der Hohen See verletzt regelmäßig nicht die territoriale Integrität eines anderen Staates, auch wenn ein Seekabel ggf. auf dessen Festland anlandet. Territoriale Integrität umfasst üblicherweise die Unversehrtheit der Landesgrenzen und betrifft insbesondere solche Fälle, in denen Gewalt mit dem Eindringen z. B. von Truppen in das Staatsgebiet verbunden ist.[35] Ob die politische Unabhängigkeit eines Staates betroffen ist, hängt maßgeblich von den Auswirkungen des Anschlages ab, die, wie bereits erörtert, von den stark variierenden Redundanzen einzelner Staaten und Regionen abhängt. Ein Angriff auf extraterritorial gelegene Infrastrukturen verstößt jedoch fraglos gegen die Ziele der Vereinten Nationen, Weltfrieden und internationale Sicherheit zu verwirklichen.[36]

Um einen Verstoß gegen das Gewaltverbot zu begründen, müsste der Anschlag auf ein Seekabel zudem als eine Androhung von Gewalt oder als Anwendung von Gewalt verstanden werden. Der Begriff Gewalt wird in der UN-Charta nicht definiert, aber im völkerrechtlichen Schrifttum nach herrschender Auffassung so ausgelegt, dass er sich auf bewaffnete Gewalt oder militärische Gewalt beschränkt. Diese restriktive Auslegung des Begriffs orientiert sich am Wortlaut der Präambel der UN-Charta sowie an Art. 44 UN-Charta, die jeweils den Begriff der Gewalt in einen militärischen Kontext stellen.[37] Dieser Auslegung folgend setzt ein Verstoß gegen Art. 2 Nr. 4 UN-Charta bewaffnete oder militärische Gewalt und damit den Einsatz militärischer Waffen voraus. Wie bereits ausgeführt, bieten sich jedoch diverse nicht-militärische Methoden für Anschläge auf Seekabel an, sodass ein Verstoß gegen das Gewaltverbot durch potentielle Angreifer

34 Vgl. erörternd *Bruha*, Gewaltverbot und humanitäres Völkerrecht nach dem 11. September 2001, Archiv des Völkerrechts 12/2002, 383 (396 ff.).

35 *Gornig*, Territoriale Souveränität und Gebietshoheit als Begriffe des Völkerrechts, in: Gornig, Horn, Territoriale Souveränität und Gebietshoheit, 2016, S. 62 f.; *Randelzhofer, Dörr*, Art. 2 (4) in: The Charter of the United Nations: A Commentary, 2012.

36 Vgl. Präambel der UN-Charta, s.o. Fn. 20.

37 *Randelzhofer. Dörr*, Art. 2 (4) in: The Charter of the United Nations: A Commentary, 2012.

vermeidbar wäre. Infolgedessen wäre ein nicht-militärischer Anschlag auf Seekabel nicht als Verstoß gegen Art. 2 Nr. 4 UN-Charta einzustufen. Es verbliebe ggf. die Einordnung eines solchen Anschlages als Verstoß gegen das aus Art. 2 Nr. 1 UN-Charta folgende und völkergewohnheitsrechtlich anerkannte Interventionsverbot. Dieses verbietet Staaten, andere Staaten unterhalb der Schwelle der Waffengewalt einem Zwang zu unterwerfen.[38] Ein Verstoß gegen das Interventionsverbot würde jedoch als Gegenmaßnahme keine Gewaltanwendungen legitimieren.

Für den Fall, dass ein Anschlag aufgrund seiner militärischen Ausführung als Verstoß gegen das Gewaltverbot aus Art. 2 Nr. 4 UN-Charta einzuordnen ist, dürfte der Sicherheitsrat gem. Art. 39 ff UN-Charta Maßnahmen zur Wahrung und Wiederherstellung des Weltfriedens beschließen. Unmittelbare Verteidigungshandlungen betroffener Staaten wären durch einen Verstoß gegen Art. 2 Nr. 4 UN-Charta dagegen nicht per se gerechtfertigt. Im Ergebnis bietet die UN-Charta somit keine rechtlich zulässige Handhabe an, bevorstehende Anschläge auf Seekabel gewaltsam zu vereiteln. Infolgedessen kann das zugrunde liegende Szenario nicht durch eine militärische Intervention angegangen werden. Diese Einschränkung entspricht dem Telos der UN-Charta. Im Kontext des Rechts der Friedenssicherung ist die Anwendung von Gewalt bewusst begrenzt und sollte nur als letztes Mittel eingesetzt werden. Dieser Maßstab spiegelt sich auch in der Definition des Begriffs Aggression seitens der UN-Generalversammlung wider: Gemäß Art. 5 Abs. 1 der Resolution 3314 (XXIX) darf keine Aggression, einschließlich der Anwendung von Waffengewalt, aus keinem Grund, sei er politisch, wirtschaftlich, militärisch oder anderweitig, gerechtfertigt werden. Insofern dürfen Verteidigungsmaßnahmen gegen feindliche Handlungen, die nicht die Schwelle des Gewaltverbots erreichen, ebenso diese Schwelle nicht überschreiten.

Abseits der Vorschriften der UN-Charta zur Friedenssicherung gilt es im Weiteren, nach nicht-militärischen Möglichkeiten zu suchen, die es betroffenen Staaten ermöglichen, in rechtskonformer Weise Anschläge auf der Hohen See zu vereiteln. Es werden nachfolgend die einschlägigen Völkerrechtsverträge erörtert, die hoheitliche Maßnahmen zum Infrastrukturschutz im Bereich der Hohen See vorsehen, nämlich der Internationale Vertrag zum Schutze der unterseeischen Telegraphenkabel von 1884 sowie das Seerechtsübereinkommen der Vereinten Nationen von 1982.

38 *Randelzhofer, Dörr*, s.o. Fn. 37.

C. Internationales Seerecht

I. Internationaler Vertrag zum Schutze der unterseeischen Telegraphenkabel

Die Nutzung erster Seekabel geht auf die 50er Jahre des 19. Jahrhunderts zurück. Am 28. August 1850 wurde zwischen Dover und Calais das erste Seekabel zur Überbrückung des Ärmelkanals verlegt, mit dem Ziel eine telegraphische Verbindung zwischen London und Paris aufzubauen. Jedoch wurde dieses „Pionier-Kabel" bereits am Folgetag wieder zerstört. Es brach an Land und wurde anscheinend unabhängig davon durch ein Fischerboot zerstört.[39] Im Jahr 1858 wurde bereits das erste transatlantische Kabel in Betrieb genommen. Aber auch dessen Nutzung beschränkte sich auf nur wenige Wochen.[40] Nichtsdestotrotz hatte mit der Verlegung von Seekabeln das Zeitalter der globalen Telekommunikation begonnen. Aufgrund der kostspieligen und gleichzeitig „zerbrechlichen" Infrastruktur ließ eine internationale Regulierung zum Schutz der Seekabel nicht lange auf sich warten. So wurde bereits am 14. März 1884 der Internationale Vertrag zum Schutze der unterseeischen Telegraphenkabel in Paris durch 27 Vertragsstaaten unterzeichnet. Der Vertrag ist zum gegenwärtigen Zeitpunkt im Jahr 2024 nach wie vor in Kraft. Die mit dem Vertrag bezweckte Schutzwirkung für Seekabel ist vor dem Hintergrund der gegenständlichen Anschlagsszenarien und aufgrund diverser Einschränkungen des Vertrages jedoch fraglich. Die derzeitige Beschränkung des Vertrags auf 37 Vertragsparteien gewährleistet keinen hinreichenden Schutz des mittlerweile globalen Seekabelnetzes. Insbesondere fehlt es an Vertragsparteien aus dem asiatischen und pazifischen Raum und damit an einer Repräsentanz der tatsächlichen Stakeholder.[41]

Aber auch inhaltlich erscheinen die Rechte und Pflichten des Vertrages nicht ausreichend, um einen effektiven Schutz des heutigen Seekabelnetzes zu gewährleisten. Das beginnt mit der fraglichen Anwendbarkeit des Ver-

39 *Neukirch*, Erstes Transatlantik-Seekabel verlegt, 2010, https://www.br.de/radio/bayern2/sendungen/kalenderblatt/0508-Transatlantik-Seekabel-Aermelkanal100.html, zuletzt abgerufen am 27.10.2024.

40 *De Cogan*, Dr E.O.W. Whitehouse and the 1858 trans-Atlantic Cable, in: History of Technology, Vol. 10, 1985, https://atlantic-cable.com/Books/Whitehouse/DDC/index.htm, zuletzt abgerufen am 27.10.2024.

41 *Takei*, Law and Policy for International Submarine Cables: An Asia-Pacific Perspective, Asian Journal of International Law 2/2012, 205 (229).

trages auf heutige Glasfaser-Datenkabel. Neben der Ausrichtung und Bezeichnung des Vertrages auf Telegraphenkabel, nehmen die Strafbarkeitsvoraussetzungen des Artikel 2 ausdrücklich Bezug auf eine Unterbrechung der telegraphischen Verbindung. Ob der heutige Austausch von Daten als Telegraphie auszulegen ist und heutige Seekabel weiterhin als Telegraphenkabel verstanden werden können, ist im Schrifttum umstritten.[42] Zudem beschränkt sich der Vertrag darauf, einen Schutz der Telegraphenkabel über Strafbarkeitsvorschriften und deren Vollstreckbarkeit sicherzustellen. Zentrale Vorschriften des Vertrages sind Art. 2 sowie Art. 12, die das vorsätzliche oder fahrlässige Zerreißen oder Beschädigen eines Telegraphenkabels unter Strafe stellen und die Vertragsstaaten verpflichten, diese Strafbarkeit im nationalen Recht zu verankern. Der Vertrag enthält in diesem Zusammenhang gem. Art. 10 zwar Rechte zur Sicherstellung von Beweismitteln, inklusive der Inspektion verdächtiger Schiffe durch Kriegsschiffe sämtlicher Vertragsstaaten. Präventive Befugnisse zur Vereitelung bevorstehender Anschläge umfasst der Vertrag dagegen nicht. Eine etwaige präventive Wirkung der Strafbarkeitsvorschriften unterwandert der Vertrag zudem durch Art. 8, der die Gerichtsbarkeit für Verstöße auf die Flaggenstaaten der handelnden Schiffe beschränkt bzw. alternativ an die Staatsangehörigkeit der handelnden Personen anknüpft. Dieser Schutzmechanismus lässt außer Acht, dass Anschläge auf Seekabel gegenwärtig zunehmend als potentielles Mittel einer hybriden Kriegsführung eingeordnet werden, sodass feindselige Staaten hinter den Anschlägen stehen.[43] Im Ergebnis wären diese Staaten verantwortlich für die Aufklärung und Verfolgung der selbst initiierten Anschläge. Der Internationale Vertrag zum Schutze der unterseeischen Telegraphenkabel bietet aus den vorstehenden Überlegungen keinen ausreichenden Schutz, um Anschläge auf der Hohen See zu vereiteln.[44]

---

42 *Mudrić*, Rights of States Regarding Underwater Cables and Pipelines, Australian Resources and Energy Law Journal, 29(2), 2010, 235 (249). https://search.informit.org/doi/10.3316/agispt.20103904, zuletzt abgerufen am 27.10.2024; auch *Takei*, S. 228, s.o. Fn. 37; widersprechend *Ehlers*, Rechtlicher Schutz von Einrichtungen auf See, NordÖR 2024, 49 (53).

43 *Gehringer*, Unterseekabel als Kritische Infrastruktur und geopolitisches Machtinstrument, 2022, S. 3 f.

44 Im Ergebnis ebenso: *Davenport*, Submarine Cables: Problem in Law and Practice, 2010, S. 3 ff., https://cil.nus.edu.sg/wp-content/uploads/2010/10/TaraDavenport-Rhodes-ICPC-Article-on-Submarine-Cables.pdf, zuletzt abgerufen am 27.10.2024; *Takei*, S. 228 f. , s.o. Fn. 41.

Auf dem Weg zum Seerechtsübereinkommen von 1982 wurden zwischenzeitliche Versuche unternommen, umfassendere Bereiche der See, inklusive dem Themenkomplex Seekabel, zu regulieren. Insbesondere wurden im Jahr 1958 die Genfer Seerechtskonventionen verabschiedet, die unter anderem Übereinkommen über die Hohe See und über den Festlandsockel umfassten. Die Vorschriften zu Seekabeln innerhalb der Genfer Seerechtskonventionen orientieren sich wesentlich an den Inhalten der Kabelschutzkonvention von 1884.[45] Diese Regelwerke dienten als Inspiration für die heute im Seerechtsübereinkommen enthaltenen Bestimmungen. Nichtsdestotrotz fanden nur Elemente der Kabelschutzkonvention Einzug in das Seerechtsübereinkommen, sodass für die Vertragsstaaten der Kabelschutzkonvention der Vertrag bis zum heutigen Zeitpunkt weiterhin in Kraft ist.[46] Der nachfolgende Teil befasst sich mit den rechtlichen Regeln des Seerechtsübereinkommens zur Hohen See und erörtert die Möglichkeiten dieses Regimes, Seekabel vor Anschlägen zu schützen.

II. Seerechtsübereinkommen

Das Seerechtsübereinkommen der Vereinten Nationen, das 1982 verabschiedet wurde und 1994 in Kraft trat, normiert einen umfassenden Regulierungsrahmen für die Nutzung aller Meere und legt Rechte und Pflichten hinsichtlich der Schonung von Meeresressourcen fest.[47] Die bedeutendste Regulierung durch das Übereinkommen ist die Aufteilung der Meere in Zonen. Die Zonierung bezweckt einen Ausgleich zwischen den Interessen der Küstenstaaten an der Nutzung ihrer Küstenmeere und dem Wunsch sämtlicher Staaten, die Ressourcen der Meere frei zu nutzen.[48] Als Konsequenz dieser Zonierung nehmen nationalstaatliche Befugnisse ab, je weiter eine Zone von der Küste entfernt liegt. Der gegenständliche Beitrag befasst sich mit der Hohen See, der von den Küsten am weitesten entfernten Meereszone. Fehlende nationalstaatliche Befugnisse erschweren in dieser

45 *Raha, Raju*, Submarine Cables Protection and Regulations: A Comparative Analysis and Model Framework, 1st Edition, 2021, Singapore: Springer Nature. Available at: https://doi.org/10.1007/978-981-16-3436-9, zuletzt abgerufen am 27.10.2024.

46 *Englender*, Art. 79, Rn. 5, in: Proelss, UNCLOS – A Commentary, 2017; *Takei*, S. 206, s.o. Fn. 41.

47 WBGU, Welt im Wandel – Menschheitserbe Meer, 2013, S. 76.

48 *Blümel et. al.*, World ocean review: Lebensgarant Ozean – nachhaltig nutzen, wirksam schützen, 2021, S. 257.

Zone einen effektiven Schutz von gefährdeten Infrastrukturen, wie z. B. Seekabeln.

1. Freiheit der Hohen See

Die Hohe See ist ein hoheitsfreier Raum. Losgelöst von einem Status als Küsten- oder Binnenstaat, steht die Nutzung der Hohen See gem. Art. 87 Abs. 1 SRÜ allen Staaten offen. Die Nutzungen bzw. Freiheiten der Hohen See werden in Art. 87 SRÜ beispielhaft aufgezählt und in den nachfolgenden Artikeln näher ausgeführt. Gem. Art. 87 Abs. 1 lit. c) iVm Art. 112 – 115 SRÜ umfasst die Freiheit der Hohen See auch das Recht unterseeische Kabel zu verlegen. Neben diesem Recht enthalten die Vorschriften über Seekabel in Art. 113 SRÜ auch Pflichten zu deren Schutz, indem die Mitgliedsstaaten zum Erlass nationaler Gesetze verpflichtet werden, die die vorsätzliche oder fahrlässige Beschädigung unterseeischer Kabel im Bereich der Hohen See unter Strafe stellen. Die Strafbarkeit beschränkt sich dabei auf Schiffe, die unter eigener Flagge fahren sowie Personen, die der eigenen Gerichtsbarkeit unterstehen, in der Regel die eigenen Staatsbürger.[49] Das Schutzkonzept des Seerechtübereinkommens gleicht insofern dem bereits erörterten Konzept der Kabelschutzkonvention von 1884. Auch hier erscheint die Androhung von Repressionen aufgrund nationalstaatlicher Strafbarkeitsvorschriften unzureichend, wenn das Ziel die Vereitelung drohender Anschläge ist. Verschärfend kommt hinzu, dass die meisten Mitgliedsstaaten ihrer Verpflichtung gem. Art. 113 SRÜ bislang nicht nachgekommen sind, sodass weltweit diesbezüglich noch erhebliche Strafbarkeitslücken bestehen.[50]

2. Flaggenstaatsprinzip

Die Bedeutsamkeit der Flagge findet sich nicht nur in Art. 113 SRÜ wieder. Als Grundprinzip der hoheitlichen Ordnung im Bereich der Hohen See gilt dort das sogenannte Flaggenstaatsprinzip, das sich im Ergebnis ebenfalls

49 *Davenport*, Intentional Damage to Submarine Cable Systems by States, 2023, S. 3, https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf, zuletzt abgerufen am 27.10.2024.

50 *Beckman*, Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea, S. 14, https://cil.nus.edu.sg/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf, zuletzt abgerufen am 27.10.2024.

nachteilig auf die Effektivität des Infrastrukturschutzes auswirkt. Das Flaggenstaatsprinzip basiert auf Art. 91 Abs. 1 S. 2, 92 Abs. 1 und 94 SRÜ und ordnet Schiffen eine Staatsangehörigkeit durch das Führen einer Flagge zu.[51] Diese Schiffe unterliegen sodann der ausschließlichen Jurisdiktion und Kontrolle ihrer Flaggenstaaten im Bereich der AWZ und der Hohen See.

Art. 91 Abs. 1 S. 2 SRÜ legt fest, dass jedes Schiff die Staatsangehörigkeit des Staates besitzt, dessen Flagge es führt. Art. 92 Abs. 1 SRÜ konkretisiert diesen Grundsatz, indem er bestimmt, dass Schiffe auf der Hohen See ausschließlich der Jurisdiktion des Flaggenstaates unterliegen. Ein konkretes Beispiel dieser Exklusivität enthält Art. 97 Abs. 1 SRÜ, wonach ein Schiff der ausschließlichen Straf- und Disziplinargewalt seines Flaggenstaates bei Kollisionen und anderen navigationsbedingten Zwischenfällen auf See unterfällt. Die exklusive Jurisdiktion bedeutet, dass nur der Flaggenstaat berechtigt ist, rechtliche und administrative Maßnahmen gegenüber dem Schiff und dessen Besatzung zu ergreifen. Andere Staaten sind grundsätzlich nicht befugt, in die Hoheitsrechte des Flaggenstaates einzugreifen.[52] Die Exklusivität der Jurisdiktion des Flaggenstaates erstreckt sich zudem auf die Durchführung von Zwangsmaßnahmen.[53] Nur der Flaggenstaat hat das Recht, Maßnahmen wie Durchsuchungen, Festnahmen oder Beschlagnahmen durchzuführen. Auch hier finden sich ausdrückliche Konkretisierungen in den Vorschriften des Seerechtübereinkommens. So ist gem. Art. 94 Abs. 6 SRÜ ausschließlich der Flaggenstaat dafür zuständig, die Kontrolle und Hoheitsgewalt über seine Schiffe wiederherzustellen, sofern es an dieser mangelt. Auch bestimmt Art. 97 Abs. 3 SRÜ, dass nur die Behörden des Flaggenstaates ein Fest- bzw. Zurückhalten eines Schiffes im Fall einer Kollision anordnen dürfen. Die Exklusivität der Jurisdiktion als Element des Flaggenstaatsprinzips stellt ein Hindernis für den effektiven Schutz von Seekabeln im Bereich der Hohen See dar.[54] Staaten, die nicht der Flaggenstaat sind, dürfen hiernach keine unmittelbaren Maßnahmen gegen verdächtige Aktivitäten ergreifen, selbst wenn diese Aktivitäten eine Bedro-

51 *Guifoyle*, Art. 91, Rn. 3, in: Proelss, UNCLOS – A Commentary, 2017.

52 *Guifoyle*, Art. 92, Rn. 1, in: Proelss, UNCLOS – A Commentary, 2017.

53 *Guifoyle*, Art. 92, Rn. 1, s.o. Fn. 52; Wissenschaftliche Dienste des Deutschen Bundestages, Welches Recht gilt auf ausländischen Kreuzfahrtschiffen in deutschen Hoheitsgewässern? WD 2 – 3000-013/14, 2014, https://www.bundestag.de/resource/blob/636154/3e3f64ef6ab8588d2d4ff1a671b08381/WD-2-013-14-pdf-data.pdf, zuletzt abgerufen am 27.10.2024.

54 Vgl. *Takei*, S. 230, s.o. Fn. 41; *Davenport*, 2010, S. 39, s.o. Fn. 44; vgl. auch *Guifoyle, Miles*, Art. 113, Rn. 4, in: Proelss, UNCLOS – A Commentary, 2017.

hung für Seekabel darstellen. Auch lässt sich aus dem Recht gem. Art. 112 Abs. 1 SRÜ, Seekabel auf dem Boden der Hohen See zu verlegen, nicht die Annexkompetenz herleiten, zum Schutz dieser Seekabel Schiffe von Drittstaaten anhalten und durchsuchen zu dürfen. Dagegen sprechen insbesondere zwei Argumente. Zum einen verlangt der Wortlaut des Art. 92 Abs. 1 SRÜ eine ausdrückliche Regelung für Ausnahmen zum Flaggenstaatsprinzip. Die Exklusivität solcher Ausnahmen wird durch Art. 110 Abs. 1 SRÜ untermauert, der das Recht zum Betreten eines fremden Schiffes nur für die aufgezählten Vergehen oder für den Fall anderer völkervertragsrechtlicher Befugnisse annimmt. Zudem regelt das SRÜ systematisch im Kontext der Rechte, Infrastrukturen im Meer zu errichten, auch die dazugehörigen Rechte für Schutzmaßnahmen. Das zeigen die Artikel 60, 73, 79 und 113 ff. SRÜ. Durch diese ausdrückliche Regelung von Schutzmaßnahmen werden staatliche Interessen an der Ausbeutung von Meeresressourcen und die Gewährleistung der Freiheit der Hohen See in Ausgleich gebracht. Eine Ausweitung dieser Schutzrechte – über das ausdrücklich gewährte Maß hinaus – würde dieses Gleichgewicht gefährden.

Obwohl das Flaggenstaatsprinzip eine allgemeine Regel darstellt, enthält Art. 92 Abs. 1 S. 1 SRÜ, wie bereits angeführt, eine Öffnung des Grundsatzes für Ausnahmen, die andere Staaten zur Durchführung von Zwangsmaßnahmen berechtigen. Diese Ausnahmen müssen ausdrücklich in internationalen Verträgen oder im Seerechtsübereinkommen selbst geregelt sein. Das Übereinkommen selbst enthält entsprechend in den Art. 99 ff. Ausnahmen für bestimmte internationale Verbrechen wie beispielsweise Sklavenhandel und Seeräuberei.

3. Universelle Eingriffsrechte auf der Hohen See

Universelle Eingriffsrechte auf der Hohen See stellen eine bedeutsame Ausnahme vom Flaggenstaatsprinzip gem. Art. 92 Abs. 1 SRÜ dar und ermöglichen es Staaten unter bestimmten Voraussetzungen, Zwangsmaßnahmen gegenüber fremden Schiffen durchzuführen. Diese Rechte sind, obwohl die Auswahl der Verbrechen kontrovers ist, von zentraler Bedeutung für die Bekämpfung ausgewählter internationaler Verbrechen und damit auch für die Aufrechterhaltung der Sicherheit und Ordnung auf den Weltmeeren.[55] Sie sind zumeist im Seerechtsübereinkommen oder aber in internationalen Übereinkommen ausdrücklich vorgesehen und ermöglichen es den ver-

55 *Guifoyle*, Art. 110, Rn. 2, in: Proelss, UNCLOS – A Commentary, 2017.

pflichteten Staaten, in spezifischen Fällen Zwangsmaßnahmen gegen fremde Schiffe zu ergreifen, unabhängig von deren Flaggenstaat. Nachfolgend werden die wichtigsten dieser Eingriffsrechte angeführt, um sodann zu prüfen, ob Anschläge auf Seekabel von einem Tatbestand dieser Eingriffsrechte erfasst werden.

Die relevantesten Ausnahmen vom Flaggenstaatsprinzip wurden bereits mit dem Seerechtsübereinkommen kodifiziert. Mit den Artikeln 99 – 110 SRÜ werden Sklavenhandel (Art. 99 SRÜ), Seeräuberei (Art. 100–107 SRÜ) und nicht genehmigte Rundfunksendungen (Art. 109 SRÜ) in unterschiedlichem Ausmaß einer universellen Jurisdiktion unterworfen, die im Mindestmaß gem. Art. 110 SRÜ das Recht zum Anhalten und Betreten verdächtiger Schiffe umfasst. Das Regime der Seeräuberei ist mit Vorschriften zu Definition, Ausnahmen, Rechtfolgen und Haftung insbesondere im Kontrast zu den weiteren Eingriffsrechten auffallend detailliert geregelt.[56] Auch wenn der Begriff der Seeräuberei zunächst keinen offensichtlichen Zusammenhang mit Anschlägen auf Seekabel erkennen lässt, lohnt sich eine genauere Betrachtung des Tatbestandes im Kontext des vorliegenden Themas. Bereits bei den Verhandlungen der Vertragsstaaten zur Kabelschutzkonvention von 1884 vertraten die Vereinigten Staaten die Auffassung, dass Verbrechen gegen Seekabel mit Piraterie gleichzusetzen seien. Sie schlugen infolgedessen eine universelle Zuständigkeit für die Verfolgung von Straftaten gegen Seekabel vor, konnten sich mit dieser Auffassung allerdings nicht durchsetzen.[57] Zum geltenden Recht findet sich im Schrifttum die Diskussion, dass zumindest der Diebstahl von Seekabeln dem Tatbestand der Seeräuberei unterfallen könnte und damit eine universelle Jurisdiktion begründet.[58] Betrachtet man die Rechtsfolgen der Seeräuberei gemäß Art. 105 SRÜ, so zeigt sich, dass jeder Staat ein Seeräuberschiff aufbringen, die Personen an Bord festnehmen und dort befindliche Vermögenswerte beschlagnahmen darf. Die Gerichte dieses Staates entscheiden über die zu verhängenden Strafen und Maßnahmen hinsichtlich des Schiffes. Solch umfassende Eingriffsrechte würden das Vorgehen gegen Anschläge auf Seekabel erheblich vereinfachen.

56 Die Regulierung der Seeräuberei umfasst die Artikel 100–107 sowie Art. 110 SRÜ und regelt darin den Umgang mit Piraterie mit einem Detailgrad, der in einem deutlichen Kontrast zu den rudimentären Vorschriften zum Transport von Sklaven auf See gem. Art. 99 SRÜ und zum nicht genehmigten Ausstrahlen von Rundfunksendungen gem. Art. 109 SRÜ steht.

57 *Davenport*, 2023, S.18, Endnote 30, s.o. Fn. 29.

58 *Beckman*, S. 15 f., s.o. Fn. 50; auch *Davenport*, 2010, S. 39 f., s.o. Fn. 44.

Inwieweit Anschläge gegen Seekabel der Definition der Seeräuberei unterfallen, verrät ein Blick in Art. 101 SRÜ:

> ***Piracy consists of any of the following acts:***
> *(a)* ***any illegal acts of violence*** *or detention, or any act of depredation,* ***committed for private ends by the crew*** *or the passengers* ***of a private ship*** *or a private aircraft, and directed:*
> *(i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;*
> *(ii)* ***against*** *a ship, aircraft, persons or* ***property in a place outside the jurisdiction of any State;***

Nach dieser Definition der Seeräuberei könnten Anschläge auf Seekabel möglicherweise als „act of violence committed for private ends by the crew of a private ship against property in a place outside the jurisdiction of any state" subsumiert werden. Fraglich erscheint eine Subsumtion hinsichtlich der Tatbestandsmerkmale „property outside the juridiction of any state" und „for private ends". Teile des Schrifttums erachten die Verortung der Seekabel im Bereich der Hohen See als ausreichend, um das Merkmal „an einem Ort, der keiner staatlichen Hoheitsgewalt untersteht" anzunehmen.[59] Doch muss dieser Auffassung die historische Auslegung dieser Formulierung entgegengehalten werden.[60] Die Definition der Seeräuberei im Seerechtsübereinkommen basiert auf den „Articles concerning the Law of the Sea" der International Law Commission (ILC), die 1956 zur Vorbereitung der ersten Seerechtskonferenz veröffentlicht wurden.[61] Der Wortlaut des damaligen Art. 39 entspricht nahezu identisch dem der heutigen Definition gem. Art. 101 SRÜ. Den ebenfalls durch die ILC veröffentlichten Kommentaren zu diesen Artikeln ist zu entnehmen, dass die Formulierung auf sogenanntes Terra Nullius abzielte, also auf Landmassen, die bislang nicht

59 *Beckman*, S. 15 f., s.o. Fn. 50; darstellend *Beckman*, *Davenport*, Workshop Report – Workshop on submarine cables and law of the sea, 2009, S. 27 ff., https://cil.nus.edu.sg/wp-content/uploads/2009/10/Workshop-Report-29-Jan-2010.pdf, zuletzt abgerufen am 27.10.2024.

60 *Takei*, S. 220, s.o. Fn. 41; *Halog*, *Margat*, *Stadermann*, Submarine Infrastructures and the International Legal Framework, Transactions on Maritime Science Vol. 13 No. 1, 2024, S. 9, https://www.toms.com.hr/index.php/toms/article/view/739/557, zuletzt abgerufen am 27.10.2024.

61 International Law Commission, Report of the International Law Commission: Articles Concerning the Law of the Sea, Yearbook of the International Law Commission, Vol. II., 1956, S. 260 f., https://legal.un.org/ilc/texts/instruments/english/draft_articles/8_1_8_2_1956.pdf, zuletzt abgerufen am 27.10.2024.

staatlich beansprucht wurden.[62] Eine Subsumtion der Hohen See unter diese Formulierung erscheint unter Berücksichtigung dieses ursprünglichen Verständnisses zumindest zweifelhaft. Als weitere Voraussetzung der Definition gem. Art. 101 SRÜ müsste die Handlung der Seeräuberei „for private ends" sein, also privaten Zwecken dienen. Handlungen, die aus politischen Motiven begangen werden oder gar staatlich gefördert sind, sind gegenteilig hierzu nicht privat.[63] Damit verbleiben allenfalls und unter den beschriebenen Vorbehalten gelegentlich vorkommende Kabeldiebstähle als mögliche Anwendungsfälle der Seeräuberei.[64] Legt man wie vorliegend staatlich veranlasste Sabotageakte als Regelfall für Seekabelanschläge zugrunde, mangelt es an den Voraussetzungen der Seeräuberei, sodass die Vorschriften der Art. 100 – 107 SRÜ keine Anwendung zum Schutz von Seekabeln finden.

Jenseits des Seerechtsübereinkommens sind Eingriffsrechte gegenüber fremden Schiffen äußerst selten. Selbst internationale Verträge, die vergleichbare Angelegenheiten der maritimen Sicherheit regulieren, wie das Übereinkommen zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Seeschifffahrt (SUA-Abkommen) oder das Übereinkommen der Vereinten Nationen gegen den unerlaubten Verkehr mit Suchtstoffen und psychotropen Stoffen (Wiener Übereinkommen von 1988), beachten das Flaggenstaatsprinzip, indem Vollstreckungsmaßnahmen gegenüber fremden Schiffen auf eigene Staatsangehörige beschränkt werden oder von einer Ermächtigung des Flaggenstaates abhängig gemacht werden. Nur vereinzelt sind Ausnahmen vom Flaggenstaatsprinzip zu finden, so etwa in Art. 21 des Fish Stocks Agreements, der die Inspektion von fremden Fischereibooten im Bereich der Hohen See vorsieht. Da das Seerecht zurzeit keine Ausnahmen bereithält, die ein universelles Vorgehen zur Abwehr von Angriffen und Gefahren für Seekabel vorsehen, liegen die Zuständigkeiten und Kompetenzen, den allgemeinen Vorgaben des Seerechtsübereinkommens folgend, insbesondere bei den Flaggenstaaten der involvierten Schiffe.

Losgelöst von aktuellen völkerrechtlichen Verträgen bietet Art. 92 Abs. 1 SRÜ eine Möglichkeit, durch internationale Verträge Ausnahmen vom Flaggenstaatsprinzip zu etablieren, die eine universelle Vollstreckung erlau-

62 International Law Commission, Report of the International Law Commission: Articles Concerning the Law of the Sea with commentaries, Yearbook of the International Law Commission, Vol. II., 1956, S. 282, https://legal.un.org/ilc/texts/instruments/english/commentaries/8_1_8_2_1956.pdf, zuletzt abgerufen am 27.10.2024.

63 *Guifoyle*, Art. 101, Rn. 10, in: Proelss, UNCLOS – A Commentary, 2017.

64 *Wilkens*, Diebe stehlen Seekabel vor Vietnam, 2007, https://www.heise.de/news/Diebe-stehlen-Seekabel-vor-Vietnam-133631.html, zuletzt abgerufen am 27.10.2024.

ben. Hierin könnte ein denkbarer Ansatz für einen effektiveren Schutz von unterseeischen Datenkabeln auf der Hohen See liegen. Eine solche Erweiterung der universellen Eingriffsrechte auf den Schutz maritimer Infrastrukturen, wie Seekabel, würde es den Staaten ermöglichen, präventive und reaktive Maßnahmen gegen Bedrohungen der Seekabel zu ergreifen, unabhängig von der Flagge eines verdächtigen Schiffes. Dies würde eine effektivere Überwachung und den Schutz dieser essenziellen Kommunikationsinfrastruktur gewährleisten.

III. Notstand im Völkergewohnheitsrecht

Angesichts der zunehmenden Gefahr hybrider Anschläge auf maritime Infrastruktur erscheint die aufgezeigte Abhängigkeit der internationalen Gemeinschaft von der Verantwortung und Rechtschaffenheit der Flaggenstaaten unbefriedigend. In Zeiten zunehmender internationaler Spannungen und technologischer Fortschritte, die Sabotageakte erleichtern, besteht ein Bedürfnis der Staaten, effektive Maßnahmen zum Schutz ihrer Infrastrukturen, auch im Bereich der Hohen See, ergreifen zu können. Es stellt sich somit die Frage, wie Anschläge auf Seekabel vereitelt werden können, wenn Vollstreckungsmaßnahmen exklusiv den Flaggenstaaten vorbehalten bleiben und somit das Aufbringen und das Festhalten verdächtiger fremder Schiffe regelmäßig völkerrechtswidrig wäre.

Das Völkergewohnheitsrecht enthält den Grundsatz, dass vermeintliche Verstöße gegen das Völkerrecht aufgrund einer Notstandssituation gerechtfertigt sein können.[65] Als historisches Beispiel für die Anwendung dieser Notstandsregel – insbesondere im maritimen Kontext – kann die Torrey Canyon-Katastrophe von 1967 angeführt werden.[66] Als der Supertanker "Torrey Canyon" vor der Küste Cornwalls auf Grund lief und eine massive

65 *Reinisch*, Sachverständigengutachten zur Frage des Bestehens und der Wirkung des völkerrechtlichen Rechtfertigunggrundes „Staatsnotstand", ZaöRV 68 (2008), S. 4 ff; Internationaler Gerichtshof, Entscheidung vom 25. September 1997, Gabcíkovo-Nagymaros Project <Hungary/Slovakia>, I.C.J. Reports 1997, S. 7 ff.

66 Vgl. *Utton*, Protective Measures and the "Torrey Canyon", Vol. 9 Boston College Law Review, 1968, 613 (623), https://core.ac.uk/download/pdf/71456406.pdf, zuletzt abgerufen am 27.10.2024; International Law Commission, Report of the International Law Commission on the work of its fifty-third session, UN-Doc A/56/10, Yearbook of the International Law Commission: 2001 vol. II (2), Art. 25 Rn. 9, https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf, zuletzt abgerufen am 27.10.2024.

Ölkatastrophe drohte, entschied sich die britische Regierung, das Wrack zu bombardieren, um das Öl zu verbrennen und so eine noch größere Umweltkatastrophe zu verhindern.[67] Das Beispiel veranschaulicht, dass in extremen Notlagen Maßnahmen ergriffen werden können, die unter normalen Umständen als völkerrechtswidrig angesehen würden.

Es stellt sich die Frage, ob auch Angriffe auf Seekabel als ein Notstand eingestuft werden könnten, der den Bruch von völkerrechtlichen Vorschriften, beispielsweise die zum Flaggenstaatsprinzip des Seerechtsübereinkommens, rechtfertigen würde. Die Voraussetzungen zur Annahme eines Staatsnotstands wurden durch die International Law Commission (ILC) in Art. 25 ihres Entwurfs von Artikeln zur Staatenverantwortlichkeit (ILC-Entwurf) kodifiziert.[68] Zwar handelt es sich beim völkerrechtlichen Notstandrecht um ein ungeschriebenes Gewohnheitsrecht, doch wird dieses nach übereinstimmender Auffassung von Schrifttum und internationaler Rechtsprechung in Art. 25 ILC-Entwurf korrekt abgebildet. Entsprechend kann zur Subsumtion eines Staatsnotstandes der nachfolgende Wortlaut des Artikels in seiner deutschen Übersetzung zugrunde gelegt werden:

> *1. Ein Staat kann sich nur dann auf einen Notstand als Grund für den Ausschluss der Rechtswidrigkeit einer Handlung, die mit einer völkerrechtlichen Verpflichtung dieses Staates nicht im Einklang steht, berufen, wenn die Handlung:*
> *a) die einzige Möglichkeit für den Staat ist, ein wesentliches Interesse vor einer schweren und unmittelbar drohenden Gefahr zu schützen, und*
> *b) kein wesentliches Interesse des Staates oder der Staaten, gegenüber denen die Verpflichtung besteht, oder der gesamten internationalen Gemeinschaft ernsthaft beeinträchtigt.*
> *2. In keinem Fall kann ein Staat sich auf einen Notstand als Grund für den Ausschluss der Rechtswidrigkeit berufen,*
> *a) wenn die betreffende völkerrechtliche Verpflichtung die Möglichkeit der Berufung auf einen Notstand ausschließt oder*
> *b) wenn der Staat zu der Notstandssituation beigetragen hat.*

Die strengen Voraussetzungen des Art. 25 ILC-Entwurf verdeutlichen, dass es sich beim Staatsnotstand um eine Ultima Ratio-Notlage handelt, die nur in seltenen Ausnahmezuständen vorliegt.[69] Ob bei Anschlägen auf Seekabel

67 *Utton*, S. 624 f., s.o. Fn. 66.
68 International Law Commission, Art. 25, s.o. Fn. 66.
69 International Law Commission, Art. 25 Rn. 14, s.o. Fn. 66.

die Anwendungsschwelle des Art. 25 erreicht wird, kann nur anhand der konkreten Umstände und des Ausmaßes dieser Anschläge beurteilt werden. Da das Funktionieren einer internationalen Datenkommunikation von systemischer Bedeutung für heutige Gesellschaften ist,[70] kann die Unversehrtheit einer Anbindung an das globale Datennetz durchaus als wesentliches Staatsinteresse gesehen werden. Ob durch einen Anschlag dieses Interesse allerdings einer schweren und unmittelbaren Gefahr ausgesetzt ist, liegt an den konkreten Umständen des Anschlages. Wie in der Einleitung bereits dargestellt, ist die Resilienz des internationalen Datennetzes regional sehr heterogen ausgestaltet. Regionen wie beispielsweise Europa und Nordamerika verfügen über zahlreiche mehrfach redundante Anbindungen an das globale Datennetz, sowohl seeseitig als auch landseitig mit ausreichenden Kapazitäten. Da weltweit nahezu täglich versehentlich Beschädigungen an Seekabeln verursacht werden, sind diese und andere Regionen darauf vorbereitet den Ausfall einzelner bzw. weniger Datenanbindungen zu kompensieren.[71] Dem gegenüber stehen Inseln und Nationen, wie z. B. die Shetland Inseln oder Tonga, deren Anbindung an das globale Datennetz zum Teil von einem einzigen Seekabel abhängt.[72] Der Maßstab für eine schwere und unmittelbare Gefahr muss diese Unterschiedlichkeit der Regionen in der Resilienz ihrer Netzinfrastruktur berücksichtigen. In einer resilienten Weltregion würde der Anschlag auf ein einzelnes Seekabel möglicherweise durch die Bevölkerung nicht bemerkt werden, wohingegen einige Inselstaaten mit dem Zusammenbruch der globalen Kommunikationsmittel konfrontiert wären. In beiden Fällen unterschiedslos einen Staatsnotstand anzunehmen erscheint nicht sachgerecht. Da ein Staatsnotstand ein Abweichen von völkerrechtlichen Pflichten rechtfertigt und deshalb ein Missbrauch dieser Vorschrift droht, empfiehlt sich zudem eine zurückhaltende Anwendung dieser Ausnahme.[73] Entsprechend kommt die pauschale Annahme eines Staatsnotstands im Fall eines Anschlages auf Seekabel nicht in Betracht. Der Staatsnotstand und das Abweichen vom geltenden Völkerrecht können somit nicht als Blaupause zur Vereitelung sämtlicher Seekabel-Anschlägen dienen. Nichtsdestotrotz bietet der Staatsnotstand gegebenenfalls eine Möglichkeit, auf Anschläge, die absehbar schwere Konsequenzen für die Datenkommunikation der betroffenen Region haben wer-

70 S.o. A. Einleitung, I. Seekabel als bedeutsame Infrastruktur.
71 S.o. A. Einleitung, II. Vulnerabilität der Infrastruktur Seekabel.
72 S.o. A. Einleitung, II. Vulnerabilität der Infrastruktur Seekabel.
73 International Law Commission, Art. 25 Rn. 2, s.o. Fn. 66.

den, mit hoheitlichen Maßnahmen zu reagieren, die ansonsten aufgrund des Flaggenstaatsprinzips völkerrechtswidrig wären. Für eine vertiefte Auseinandersetzung mit dem hier skizzierten Ansatz wäre weitere, über den vorliegenden Beitrag hinausgehende Forschung erforderlich.

D. Zusammenfassung & Ausblick

Das weltweite Netzwerk unterseeischer Datenkabel ist das Rückgrat der globalen Datenkommunikation. Für die zunehmend digitalisierte Weltgesellschaft ist diese Infrastruktur entsprechend bedeutsam. Aufgrund der aktuellen sicherheitspolitischen Lage seit Beginn des Ukrainekrieges und der in diesem Kontext stattgefundenen Anschläge auf die Nord Stream-Pipelines sind Seekabel als eine vulnerable Infrastruktur Bestandteil des öffentlichen Diskurses. Dieser Beitrag hat gezeigt, dass zum einen die Lage der Infrastruktur im Bereich der Hohen See zum anderen die Zerstörbarkeit der Kabel durch konventionelle Mittel Achillesfersen für den Schutz der Kabelinfrastruktur darstellen. Zwischen dem Friedensicherungsrecht der UN-Charta und dem Flaggenstaatsprinzip des Seerechtsübereinkommen verbleibt eine Schutzlücke im geltenden Völkerrecht, die es feindseligen Flaggenstaaten ermöglicht das Seekabelnetz anzugreifen, ohne Gegenmaßnahmen anderer Staaten befürchten zu müssen. Hybride Angriffe auf Seekabel können im Bereich der Hohen See so gestaltet werden, dass sie nicht als bewaffneter Angriff iSd Art. 51 UN-Charta zu werten sind. Für Gegenmaßnahmen gegen das angreifende Schiff wäre, dem Flaggenstaatsprinzip folgend, nur der jeweilige Flaggenstaat zuständig. Diese Schutzlücke wird zurzeit weder durch eine Ausnahme zum Flaggenstaatsprinzip, z. B. durch eine universelle Verantwortlichkeit vergleichbar zur Seeräuberei, noch durch den völkerrechtlichen Grundsatz des Staatsnotstands zufriedenstellend geschlossen.

Im internationalen Schrifttum wird insbesondere der Ansatz verfolgt, die bestehenden Völkerrechtsverträge gegen internationalen Terrorismus (z. B. das SUA-Abkommen) um den Tatbestand der Kabelzerstörung zu erweitern.[74] Da auch diese Verträge für Angelegenheiten auf See regelmäßig die Zuständigkeit der Flaggenstaaten voraussetzen, wäre insbesondere im Hinblick auf Maßnahmen zur Abwehr von Kabelanschlägen nur wenig

74 *Beckman*, S. 14 f., s.o. Fn. 50; *Davenport, Tara*, 2010, S. 40 f., s.o. Fn. 44.

gewonnen. Auch wenn es im Schrifttum teilweise als unwahrscheinlich eingestuft wird[75], bedarf es universeller Rechte zum Betreten und Festhalten von Schiffen, um effektiv der Bedrohung von Infrastruktur auf der Hohen See durch hybride Anschläge zu begegnen. Art. 92 Abs. 1 SRÜ erlaubt eine Erweiterung dieser universellen Rechte auch außerhalb des Seerechtsübereinkommens, sodass sowohl eine Adaption bestehender Verträge (z. B. die Kabelschutzkonvention von 1884 oder das SUA-Abkommen) als auch der Abschluss eines neuen multilateralen Vertrages denkbare Lösungsansätze zur Verbesserung der Schutzmöglichkeiten für die Infrastruktur der Seekabel darstellen.

75 *Davenport*, 2010, S. 41, s.o. Fn. 44.

Die Rolle des Investitionskontrollrechts beim Schutz maritimer Infrastrukturen

Christian Tietje und Philipp Reinhold[*]

A. Einleitung

Spätestens seit dem Einstieg des chinesischen Schiffskonzerns *China Ocean Shipping Company* (COSCO) im Hamburger Hafen wird die Rolle der Investitionskontrolle auch im Bereich maritimer Infrastrukturen öffentlich intensiv diskutiert. Als maritime Infrastrukturen werden gemeinhin Infrastruktureinrichtungen verstanden, die seewärts der oder direkt oder jedenfalls mit Anschluss an der Küstenlinie bzw. Basislinie verortet sind. Hierzu sind punktförmige Infrastrukturanlagen, wie bspw. Offshore-Windparks, sowie linienförmige Anlagen, wie etwa Seekabel und seeverlegte Rohrleitungen, aber auch Seehäfen zu zählen.[1] Der Schutz solch maritimer Infrastrukturen aufgrund von Belangen nationaler Sicherheit ist ein altes Thema im internationalen System. Dabei haben schon immer gleichermaßen Fragen militärischer Sicherheit und wirtschaftliche Interesse eine große Bedeutung gespielt. Das schon legendäre Beispiel des US-amerikanischen Jones Act aus dem Jahre 1920, der den küstennahen Seeverkehr der USA zahlreichen Beschränkungen unter anderem zugunsten einer ausschließlichen Nutzung in diesem Bereich von Schiffen, die in den USA gebaut wurden, unterwirft, ist hierfür ein historisch herausragendes Beispiel.[2] Insgesamt sind weltweit in vielen Staaten sogenannte Kabotage-Regelungen[3] in Kraft.

---

* Der Autor *Tietje* ist Inhaber des Lehrstuhls für Öffentliches Recht, Europarecht und Internationales Recht sowie des Jean Monnet Chair for EU Value Oriented Neighbourhood and Trade Policy an der Martin-Luther-Universität Halle-Wittenberg. Der Autor *Reinhold* ist Akademischer Rat a.Z. am Lehrstuhl für Öffentliches Recht, Völkerrecht, Europarecht und Internationales Wirtschaftsrecht an der Universität des Saarlandes, Saarbrücken.

1 Zur Definition vgl. *Schubert*, Maritimes Infrastrukturrecht, 2015, S. 7 f.

2 Ausführlich zum Jones Act *Stoll, Tietje*, Beschränkungen des küstennahen Seeverkehrs in den USA: Der Jones Act, RIW 1996, 654.

3 Siehe *Giemulla*, Stichwort: Cabotage, in: MPEPIL, abrufbar unter: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1505?rskey=sHEpzc&result=1&prd=MPIL (letzter Abruf am 15.01.25).

Diese sehen regelmäßig Beschränkungen aus Gründen militärischer Sicherheit, aber auch mit wirtschaftspolitischer Zielsetzung, für maritime Infrastruktur im küstennahen Bereich zulasten ausländischer Investoren und Wettbewerber vor. Auch die überarbeitete und aktualisierte EU-Strategie zur maritimen Sicherheit, die vom Ministerrat der EU am 24. Oktober 2023 angenommen wurde,[4] verweist auf „Risiken und Bedrohungen, die sich aus ausländischen Direktinvestitionen" im Bereich der maritimen Sicherheit ergeben. Allerdings wird dieser Aspekt in der einschlägigen EU-Strategie nicht weiter ausgeführt. Vielmehr wird ohne weitere Konkretisierung nur auf das allgemeine Investitionskontrollrecht der EU verwiesen.[5]

In diesem Beitrag soll die Rolle des Investitionskontrollrechts beim Schutz ausgewählter maritimer Infrastruktur näher beleuchtet werden. In einem ersten Teil geht es um die völkerrechtlichen und rechtstatsächlichen Rahmenbedingungen für Investitionen im Bereich maritimer Infrastrukturen und darauf bezogene Herausforderungen für die maritime Sicherheit (B.). Anschließend wird dargestellt, inwieweit maritime Infrastrukturen Schutzobjekt für Investitionskontrolle in Europa sind bzw. sein können (C.). Schließlich soll kurz noch ein Blick de lege ferenda auf notwendige Anpassungen der Investitionskontrolle zum effektiveren Schutz maritimer Infrastrukturen geworfen werden (D.).

B. Völkerrechtlicher und rechtstatsächlicher Rahmen für Investitionen im Bereich maritimer Infrastrukturen

Das allgemeine Völkerrecht kennt keine Pflicht der Staaten (bzw. entsprechend der EU), ausländische Investitionen innerhalb der jeweils eigenen Jurisdiktion zuzulassen. Ebenso wie Staaten völkerrechtlich betrachtet weitgehend frei sind, über den Zuzug natürlicher Personen zu entscheiden, gilt dies für ausländische Investitionen.[6] Einschränkungen dieser staatlichen Regelungsfreiheit können sich nur aus völkerrechtlichen Verträgen ergeben. Neben dem EU-Recht, das im Rahmen der Grundfreiheiten durch die Nie-

4 Rat der Europäischen Union, Schlussfolgerungen des Rates zu der überarbeiteten Strategie der EU für maritime Sicherheit (EUMSS) und dem dazugehörigen Aktionsplan, Rats-Dok. 14280/23.

5 Ebda., S. 30.

6 *Reinisch*, Internationales Investitionsschutzrecht, in: Tietje, Nowrot, Internationales Wirtschaftsrecht, 3. Aufl. 2022, § 9 Rn. 34 ff.

derlassungsfreiheit (Art. 49 AEUV) und die Kapitalverkehrsfreiheit (Art. 63 Abs. 1 AEUV) Investitionsfreiheit im Binnenmarkt für unionsangehörige Unternehmen sowie, allerdings im beschränkten Umfang, auch für Investitionen aus Drittstaaten gewährt, enthalten Freihandelsabkommen und insbesondere das Recht der Welthandelsorganisation (WTO) bestimmte Pflichten zur Zulassung ausländischer Investitionen.[7] Im WTO-Recht ist dies insbesondere im Allgemeinen Dienstleistungsabkommen (GATS) und dem Übereinkommen über handelsbezogene Investitionsmaßnahmen (TRIMS) geregelt, wobei Letzteres bislang deutlich hinter den Erwartungen an eine stärkere Liberalisierung des grenzüberschreitenden Kapitalverkehrs zurückgeblieben ist.[8] Während etwa die Energieübertragung klar vom GATS (und auch vom Warenhandelsrecht des GATT) erfasst wird, stellte sich schon bei den Verhandlungen über die heutige WTO-Rechtsordnung heraus, dass der gesamte Bereich des maritimen Transports, der rechtlich im Wesentlichen ebenfalls als Dienstleistung einzustufen ist, politisch ausgesprochen sensibel ist. Vor diesem Hintergrund konnten wesentliche Bereiche der Liberalisierung des maritimen Dienstleistungsbereiches, die zu einem Recht auf Investitionszugang geführt hätten, nicht verhandelt werden.[9] Ursprünglich waren weitere Verhandlungen im Rahmen der WTO für Seeverkehrsdienstleistungen vorgesehen, diese sind allerdings bereits 1996 suspendiert worden. Auch in der seit 2001 laufenden Doha-Verhandlungsrunde der WTO gibt es bislang diesbezüglich keine nennenswerten Fortschritte.

Die Schwierigkeiten bei der Liberalisierung des Marktzugangsrechts für Seeverkehrsdienstleistungen, zu denen auch Einrichtungen der maritimen Infrastruktur und deren Betrieb zählen, sind historisch betrachtet in erster Linie auf militärische Sicherheitsbedenken zurückzuführen. Auf den US-amerikanischen Jones Act aus dem Jahr 1920, der dies besonders deutlich macht, wurde bereits hingewiesen. Überhaupt war das Investitionskontrollrecht lange Zeit auf Gesichtspunkte militärischer Sicherheit beschränkt. Auch in Deutschland bestand jahrelang nur auf Militärtechnologie bezogen die rechtliche Möglichkeit der Beschränkung von Investitionen aus

7 *Reinisch* (Fn. 6), Rn. 39 f.

8 Zum Ganzen etwa *Velten*, Screening Foreign Direct Investment in the EU, 2022, S. 230 ff.

9 Dazu insgesamt *Senti, Hilpold*, WTO, 2. Aufl. 2017 Rn. 1226 ff.; sowie ausführlich *Taylor*, Evaluating the Continuing GATS Negotiations Concerning International Maritime Transport Services, TUL. MAR. L.J. 27 (2002), 129 ff.

Drittstaaten.[10] Zur Verschärfung des Investitionskontrollrechts kam es nach ersten Ansätzen im Jahre 1993 in den USA durch das sogenannte Byrd-Amendment, erst in der Nachfolge der Terroranschläge vom 11. September 2001.[11] Auslöser für die entsprechenden Rechtsverschärfungen war dabei in den USA ein Sachverhalt im Bereich maritimer Infrastruktur. Es ging hierbei im Wesentlichen darum, dass ein Staatsunternehmen aus den Vereinigten Arabischen Emiraten, *Dubai Ports World's* (DP World), im Begriff war, über eine britische Unternehmensbeteiligung einen Kontrollerwerb an zahlreichen US-amerikanischen Seehäfen zu erlangen. Das führte im Jahr 2006 zur intensiven politischen Diskussion in den USA und schließlich zur Verabschiedung des Foreign Investment and National Security Act of 2007 (FINSA).[12] Mit diesem Gesetz wurden unter anderem die Voraussetzungen für die Untersagung ausländischer Investitionen in den USA weit über den traditionellen Bereich militärischer Sicherheit hinaus auf eine große Anzahl allgemeiner öffentlicher Belange ausgedehnt. Der *Dubai Port*-Sachverhalt kann als Beginn einer Regulierungsentwicklung weltweit gesehen werden, die zu einer Intensivierung des Investitionskontrollrechts führte.[13] Das gilt auch für die Entwicklung des Investitionskontrollrechts in der Europäischen Union und in Deutschland, auf dessen Inhalte sogleich noch näher einzugehen ist. Maritime Infrastruktur war und ist insofern jedenfalls in der rechtspolitischen Diskussion ein wesentliches Element des Investitionskontrollrechts.

Die politische Sensibilität, die mit einem durch Investitionskontrolle vermittelten Schutz maritimer Infrastruktur vor unerwünschter, vermeintlich missbräuchlicher oder möglicherweise staatliche Interessen gefährdender Einflussnahme verbunden wird, lässt sich nur bedingt empirisch erklären. Beispiele für eine missbräuchliche, die nationale Sicherheit oder öffentliche Ordnung gefährdende Nutzung maritimer Infrastruktur, die über geheim-

10 Siehe z.B. *Roth*, Der Erwerb von Rüstungs- und Kryptounternehmen durch Gebietsfremde, AW-Prax 2004, 431.

11 Siehe z.B. *Tietje, Kluttig*, Beschränkungen ausländischer Unternehmensbeteiligungen und -übernahmen – Zur Rechtslage in den USA, Großbritannien, Frankreich und Italien, Beiträge zum Transnationalen Wirtschaftsrecht 5/2008, S. 7 ff.

12 *Casselman*, China's Latest 'Threat' to the United States: The Failed CNOOC- UNOCAL Merger and its Implications for Exon-Florio and CFIUS, Ind. Int'l & Comp. L. Rev. 17 (2007), 155 (161); *Haley*, A Shot Across the Bow: Changing the Paradigm of Foreign Direct Investment Review in the United States, Brooklyn J. Int'l L. 32 (2007), 1157 (1164).

13 Zu den einschlägigen Regelungen und deren Entwicklung in ausgewählten Staaten siehe umfassend *Tietje, Kluttig* (Fn. 11).

dienstliche Aktivitäten und militärische Sicherheitsbelange hinausgehen, lassen sich nur schwer finden. Im Wesentlichen geht es um potentielle Gefahren, die von der Verfügungsgewalt über maritime Infrastruktur ausgehen könnten. Spionagetätigkeiten wie zum Beispiel das Abhören von Unterseekabeln, die der internationalen Kommunikation dienen, oder der Datensammlung durch bestimmte Technologien, die u.a. in Containerkränen in Überseehäfen eingesetzt werden, beides sind sicherheitsgefährdende Aktivitäten im Hinblick auf maritime Infrastruktur,[14] setzen allerdings keine Investitionen im Sinne des Investitionskontrollrechts voraus. Wie bereits das Beispiel von *Dubai Port* zeigt, geht es im Investitionskontrollrecht mit Blick auf maritime Infrastruktur in erster Linie um Häfen und Investitionen in diese durch Drittstaatsunternehmen, zumal wenn es sich um Staatsfonds oder Staatsunternehmen aus Drittstaaten handelt. Das europäische Parlament hat hierzu eine Ende 2023 veröffentlichte Studie in Auftrag gegeben, die sich mit Investitionen aus China in europäische maritime Infrastruktur befasst. Die Studie behandelt im Wesentlichen drei Fallstudien chinesischer Investitionen in europäischen Häfen, konkret die Häfen von Piräus (Griechenland), Hamburg (Deutschland) und Kumport (Türkei).[15] Diese Fokussierung auf Häfen im Hinblick auf potentielle Gefahren durch eine Drittstaatskontrolle ist verständlich wenn man berücksichtigt, dass mehr als 80% des globalen Handels durch Seeverkehr erfolgt; Hafeninfrastruktur ist insofern zentral für die Sicherheit und Stabilität der weltweiten Lieferketten.

Die Konzentration der maritimen Investitionskontrolle auf Häfen steht in einem gewissen Spannungsverhältnis zur Einordnung und Regulierung von Häfen nach einschlägigem Völkerrecht. Insbesondere das Übereinkommen und Statut über die internationale Rechtsordnung der Seehäfen vom 9. Dezember 1923[16] sowie zahlreiche Freundschafts-, Schifffahrts- und Han-

14 Hierzu und zu weiteren Bedrohungen der Sicherheit maritimer Infrastruktur ausführlich die Beiträge in: Voelsen (Hrsg.), Maritime kritische Infrastrukturen, SWP-Studie 3, Februar 2024.

15 Chinese Investments in European Maritime Infrastructure, PE 747.278, September 2023, abrufbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/747278/IPOL_STU(2023)747278_EN.pdf (letzter Abruf am 15.01.25).

16 Abgedruckt in: AVR 26 (1988), 480.

delsabkommen[17] und Seeverkehrsabkommen[18] statuieren bestimmte staatliche Pflichten zur Gewährleistung eines freien Hafenzugangs.[19] Diese Völkerrechtspflichten haben Staaten auch gegenüber Eigentümern von Häfen durchzusetzen, die aus Drittstaaten kommen. Der Hafenstaat hat diesbezüglich immer die volle territoriale Regelungshoheit. Soweit es bei der Anwendung vorgelagerten Investitionskontrollrechts gegenüber Drittstaatsinvestitionen um Fragen der Verhältnismäßigkeit geht, ist dies mit zu berücksichtigen.

C. Maritime Infrastrukturen als Schutzobjekt der Investitionskontrolle in Europa

Die Marktzugangskontrolle für ausländische Investitionen befasst sich mit denjenigen Sicherheitsrisiken, die aus der Schaffung oder Erweiterung von Einsichts-, Zugriffs- und Kontrollrechten für ausländische Investoren in Bezug auf kritische Infrastrukturen und sonstige wirtschafts- wie gesellschaftspolitisch bedeutsame Sektoren erwachsen können.[20] Wie bereits einleitend bemerkt, identifiziert die überarbeitete EU-Strategie zur maritimen Sicherheit „Risiken und Bedrohungen, die sich aus ausländischen Direktinvestitionen ergeben".[21] Zu deren Bewältigung verweist sie ohne nähere

17 Siehe z.B. *Paulus*, Stichwort: Treaties of Friendship, Commerce, and Navigation, in: MPEPIL, abrufbar unter: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1482?rskey=I50tUq&result=1&prd=MPIL (letzter Abruf am 15.01.25).

18 Siehe z.B. das Seeverkehrsabkommen zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Regierung der Volksrepublik China andererseits, ABl. EU Nr. L 046 v. 21.02.2008, S. 25 ff.

19 Ausführlich *Lagoni*, Stichwort: Ports, in: MPEPIL, abrufbar unter: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1207?rskey=pqqnxg&result=1&prd=MPIL (letzter Abruf am 15.01.25).

20 *Bungenberg, Reinhold*, Investitionskontrollrecht, 2023, Rn. 12.

21 Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat über die Aktualisierung der EU-Strategie für maritime Sicherheit und des Aktionsplans „Eine erweiterte EU-Strategie für maritime Sicherheit angesichts sich wandelnder maritimer Bedrohungen", Rats.-Dok. 7311/23, S. 5.

Konkretisierung auf die Befugnisse der EU auf Basis der Verordnung (EU) 2019/452 (EU-Screening-Verordnung; EU-Screening-VO)[22].[23]

Die unionale Investitionskontrolle bewegt sich im Schnittfeld der europäischen Sicherheits- und Handelspolitik. Ihr Grundansatz einer industrie- und/oder sicherheitspolitisch motivierten „Übernahmeabwehr" ist nicht neu.[24] Der zunehmend starke Einfluss geopolitischer Erwägungen in der wirtschaftspolitischen Debatte hat ihre Bedeutung zuletzt indes noch einmal enorm gesteigert und hat zugleich die Stimmen, die auf eine „Gefahr des Protektionismus" hindeuten, leiser werden lassen.[25] Auf die Investitionskontrolle wird inzwischen vielfach Bezug genommen, wenn es um die sicherheitspolitische Ausrichtung der EU im Hinblick auf ihre internationalen Wirtschaftsbeziehungen geht, so bspw. im Rahmen des Konzepts der „strategischen Autonomie"[26] und der „Europäischen Strategie für wirtschaftliche Sicherheit"[27]. Das europäische Investitionskontrollrecht ist allerdings trotz gewisser Zentralisierungstendenzen bislang ein unvollendet zweistufiges System, bestehend aus einem unionsrechtlichen Rahmen und den verschiedenen nationalen Kontrollregimen (I.). Vor diesem Hintergrund ist auch der Schutz maritimer Infrastrukturen innerhalb der EU-Screening-VO (II.) bzw. im deutschen Investitionskontrollrecht (III.) und den anderen mitgliedstaatlichen Prüfungsregimen (IV.) zu sehen.

22 Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union, ABl. L 79I vom 21.3.2019, S. 1.

23 Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat über die Aktualisierung der EU-Strategie für maritime Sicherheit und des Aktionsplans „Eine erweiterte EU-Strategie für maritime Sicherheit angesichts sich wandelnder maritimer Bedrohungen", Rats.-Dok. 7311/23, S. 5, 14 f.

24 Siehe dazu *Heinemann*, Ökonomischer Patriotismus, 2011, S. 11 ff.

25 Siehe etwa die Kritik bei *Heinemann* (Fn. 24), S. 105 ff., der zugleich die problematische Rolle von Staatsfonds hervorhebt, hier jedoch auf eine Verbesserung der Transparenz setzt.

26 *Hoffmeister*, Strategic Autonomy in the European Union's External Relations Law, CMLR 2023, 667 (677 ff.).

27 Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat und den Rat über eine „Europäische Strategie für wirtschaftliche Sicherheit", JOIN (2023) 20 final, S. 3, 9.

I. Das europäische Investitionskontrollsystem

Erste Überlegungen zur Schaffung einer europäischen Investitionskontrolle[28] wurden bereits 2007 angestellt, mangels Realisierbarkeit jedoch nicht weiterverfolgt.[29] Auch die Europäische Kommission stand derartigen Plänen zunächst kritisch gegenüber.[30] Dies änderte sich durch die explizite Einbeziehung von „ausländischen Direktinvestitionen" in die gemeinsame Handelspolitik in Folge des Vertrags von Lissabon: Zunächst schlugen die EU-Kommissare *Tajani* und *Barnier* Anfang 2011 einen umfassenden Screening-Mechanismus für ausländische Direktinvestitionen auf Unionsebene vor.[31] Auch das Europäische Parlament forderte daraufhin in einer Resolution, ausländische Investitionstätigkeiten stärker in den Blick zu nehmen.[32] Konkret wurden Überlegungen indes erst im Jahr 2017 als Deutschland, Frankreich und Italien in einem gemeinsamen Schreiben an Handelskommissarin *Malmström* regulatorische Schritte gegen einen Ausverkauf von europäischem Know-how, aber auch im Hinblick auf den Mangel an Reziprozität für EU-Unternehmen forderten.[33] Hintergrund war die zunehmend kritische Einstellung gegenüber chinesischen Investitionen in Europa.[34] Während eine große Zahl von Mitgliedern des Europäischen

28 Zur Historie siehe m.w.N. *Bungenberg, Reinhold* (Fn. 20), Rn. 51 ff.

29 *Kollman*, Prüfung ausländischer Investitionen in Deutschland, AW-Prax 2009, 205.

30 Dazu *Kretzschmar*, Die Überprüfung drittstaatlicher Unternehmensakquisitionen zum Schutz der öffentlichen Ordnung und Sicherheit in der Europäischen Union, 2022, S. 50 f.

31 Europäische Kommission, Kabinettsbrief des Vizepräsidenten der Europäischen Kommission Tajani, Nr. 33 vom 11. Februar 2011, http://ec.europa.eu/archives/commission_2010-2014/tajani/about/newsletter/files/2011-02/cabnews-33-20110211_en.pdf (letzter Abruf am 15.01.25).

32 Europäisches Parlament, Entschließung vom 23. Mai 2012 zum Thema „Die Europäische Union und China: ein Handelsungleichgewicht?" (2010/2301(INI)), P7 TA (2012) 0218.

33 *Zypries, Sapin, Calenda*, Brief an die Europäische Kommission, Februar 2017, abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/S-T/schreiben-de-fr-it-an-malmstroem.pdf?__blob=publicationFile&v=5 (letzter Abruf am 15.01.25); Zum Gesetzgebungsverfahren *Voland, Slobodenjuk*, in: Krenzler, Herrmann, Niestedt (Hrsg.), EU-Außenwirtschafts- und Zollrecht, 22. EL Dezember 2023, Erwgr. VO (EU) 452/2019 Rn. 7 ff.; *Warchol*, The Birth of EU Screening Regulation, in: Hindelang, Moberg, YSEC 2020, 53, 56 ff.; *Kretzschmar* (Fn. 30), S. 52 f.

34 *Gerhard*, Mehr Schutz vor ausländischen Direktinvestitionen?, Wirtschaftsdienst 2018, 814 (815).

Parlaments die Initiative unterstützte,[35] zeigten sich einige der Mitgliedstaaten von der Notwendigkeit einer solchen Kontrolle nicht überzeugt bzw. lehnten deren Verortung auf EU-Ebene ab.[36] Dennoch konnte bereits 2019 eine Einigung für die Schaffung der EU-Screening-VO als einem ersten europäischen Rechtsakt im Bereich der Investitionskontrolle erzielt werden.[37]

Die EU-Screening-VO wurde auf Art. 207 Abs. 2 AEUV gestützt, bezeichnet sich selbst jedoch als einen „Rahmen für die Überprüfung ausländischer Direktinvestitionen". Unter einer „Überprüfung" wird dabei ein Verfahren verstanden, „mit dessen Hilfe ausländische Direktinvestitionen geprüft, untersucht, genehmigt, an Bedingungen geknüpft, untersagt oder rückabgewickelt werden können" (Art. 2 Nr. 3 EU-Screening-VO). Die Verordnung enthält keine zentrale EU-Investitionskontrolle, sondern lediglich Regelungen für einen EU-weiten Kooperationsmechanismus (Art. 6 bis 8 EU-Screening-VO) sowie gewisse inhaltliche Vorgaben für mitgliedstaatliche Prüfungsmechanismen (Art. 2 Nr. 4 EU-Screening-VO). Zugleich werden die Mitgliedstaaten allerdings zur Einführung einer entsprechenden Kontrolle nicht verpflichtet (Erwgr. 8 und Art. 3 Abs. 1 EU-Screening-VO). Auch wird explizit betont, dass das Recht der Mitgliedstaaten zur Abweichung vom freien Kapitalverkehr gem. Art. 65 Abs. 1 lit. b AEUV, ebenso wie ihre alleinige Verantwortung für den Schutz der nationalen Sicherheit (Art. 4 Abs. 2 EUV) und die Wahrung ihrer wesentlichen Sicherheitsinteressen (Art. 346 AEUV) unberührt bleiben (Art. 1 Abs. 2 EU-Screening-VO).[38]

In Summe hat dies zu Diskussionen darüber geführt, inwieweit der Rückgriff auf die ausschließliche Kompetenz der EU für den Bereich der

35 Europäisches Parlament, Vorschlag für einen Rechtsakt der Union zur Überprüfung (Screening) ausländischer Investitionen in strategischen Bereichen, 20. März 2017, B [8-0000/2017].

36 Siehe dazu Europäischer Rat, Tagung des Europäischen Rates (22. und 23. Juni 2017) - Schlussfolgerungen, EUCO 8/17 (CO EUR 8 CONCL 3), Rn. 17.

37 Siehe zu diesem Prozess im Einzelnen z. B. *Warchol* (Fn. 33), S. 53, 66 ff. Angesichts der grundlegenden Unterschiede zwischen den Mitgliedstaaten sowie innerhalb der Kommission und des Europäischen Parlaments hat die Geschwindigkeit, mit der die Verordnung schließlich zustande kam, dabei viele überrascht. Siehe etwa *Malmström*, Foreword: A Common European Law on Investment Screening, in: Hindelang, Moberg, YSEC 2020, S. ii, iv: "The regulation proposal passed very quickly for an EU law (less than 18 months!) and in March 2019 a final trilogue between MS, EP and the Commission was able to agree on a compromise and adopt the regulation."

38 Erwägungsgrund 7 der Verordnung.

Handelspolitik überhaupt als gerechtfertigt erscheint.[39] Teilweise wurde angenommen, der EU-Screening-VO fehlten sowohl die von Art. 207 Abs. 1 AEUV geforderten „einheitlichen Grundsätze" als auch der verpflichtende Charakter, der mit Regelungen auf Grundlage von Art. 207 Abs. 2 AEUV notwendig einhergehen müsse.[40] *GA Ćapeta* hat die EU-Screening-VO vor diesem Hintergrund als ein „Schnabeltier" und „seltsames Geschöpf im Vergleich zu den ‚normalen' nach Art. 288 AEUV erlassenen Verordnungen" bezeichnet, geht jedoch mit Teilen der Literatur letztlich davon aus, dass die EU-Screening-VO eine Rückdelegation an die Mitgliedstaaten bewirkt.[41]

Politisch erklärt sich die Zurückhaltung bzgl. einer verpflichtenden Einführung einer Investitionskontrolle aus den unterschiedlichen Positionen, die noch im Einigungszeitpunkt auf EU-Ebene einander gegenüberstanden.[42] Anders als etwa im Bereich der Fusionskontrolle fehlte es an einem gemeinsamen Grundverständnis hinsichtlich der Notwendigkeit und des erforderlichen Prüfprogramms.[43] Seit Erlass der Verordnung hat sich jedoch bereits ein Stimmungswechsel gezeigt, der durch den rasanten Anstieg nationaler Kontrollregime von 11 auf nunmehr 24 eindrucksvoll belegt

39 Zu dieser Diskussion u.a. *Günther*, Der Vorschlag der Europäischen Kommission für eine Verordnung zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Europäischen Union – Investitionskontrolle in der Union vor dem Hintergrund kompetenzrechtlicher Fragen, Beiträge zum Transnationalen Wirtschaftsrecht 157/2018, S. 17 ff.; *Herrmann*, Europarechtliche Fragen der deutschen Investitionskontrolle, ZEuS 2019, 429 (436 f. u. 466); *Hindelang, Moberg*, The Art of Casting Political Dissent in Law: The EU's Framework for Screening of Foreign Direct Investments, CMLR 2020, 1435 (1446 ff.); *Korte*, Exploring the Possibilities and Limits of the EU and Member States to Set Up an Investment Screening Mechanism in the Light of Union Law, in: Hindelang, Moberg (eds.), YSEC 2020, S. 435, 451 ff.; *Daniel*, Comment on Exploring the Possibilities and Limits of the EU and Member States to Set Up an Investment Screening Mechanism in the Light of Union Law, in: Hindelang, Moberg, YSEC 2020, 467, 473 f.; *Kretzschmar* (Fn. 30), S. 362 ff.; *Bungenberg, Reinhold* (Fn. 20), Rn. 58 ff.

40 So insbesondere *Korte* (Fn. 39), S. 435, 451 f.

41 *GA Ćapeta*, Schlussanträge, Rs. C-106/22, ECLI:EU:C:2023:267, Rn. 32 u. 35 – Xella Magyarország. In diese Richtung auch *Günther*, BTWR 157/2018, S. 34; *Herrmann* (Fn. 39), 429, 436 f., 466; *Bungenberg, Reinhold* (Fn. 20), Rn. 61; A. A. *Korte* (Fn. 39), S. 435, 443 ff.

42 *Bungenberg, Reinhold*, The Evolution of the EU Investment Control Legal Regime: Decentralization as a Unifying Factor, in: de Jong, Looijestijn-Clearie, Tans, Veenbrink, The Rise of Public Security Interests in Corporate Mergers and Acquisitions, 2022, S. 31, 39 f.

43 *Bungenberg, Reinhold* (Fn. 42), S. 31, 40.

wird.[44] Neben den ersten rechtlichen Regelungen zur Investitionskontrolle auf EU-Ebene, hat die EU-Screening-VO überdies eine europäische Investitionskontrollpolitik begründet.[45] Die Investitionskontrolle findet im politischen Dialog statt; die Kommission berichtet außerdem in regelmäßigen Abständen über die europäischen Entwicklungen in diesem Bereich, darunter insbesondere über die Zahl der Prüfregime und Prüffälle.[46] Auch hat die Kommission anlässlich der Corona-Krise und des Ukraine-Kriegs Leitlinien erlassen, in denen sie die Mitgliedstaaten zu einer aufmerksamen Prüfung aufforderte.[47]

Im Januar 2024 hat die Kommission einen Vorschlag zur Reform der EU-Screening-VO vorgelegt.[48] Darin ist wiederum keine zentrale EU-Investitionskontrolle vorgesehen, sondern lediglich eine Verpflichtung der Mitgliedstaaten zur Einführung eines nationalen Überprüfungsmechanismus (Art. 3 Abs. 1 des Reformvorschlags). Zugleich werden weitergehende Mindestanforderungen festgelegt (Art. 4). Abgesehen von einer weiteren Ausdifferenzierung des Kooperationsmechanismus (Art. 5 bis 12) liegt eine

44 Siehe dazu „List of screening mechanisms notified by Member States (Last update: 8 January 2024)", abrufbar unter https://policy.trade.ec.europa.eu/enforcement-and-protection/investment-screening_en (letzter Abruf am 15.01.25). Hinzu treten die Regime von Bulgarien sowie jüngst auch Irland.

45 So bereits *Bungenberg, Reinhold* (Fn. 42), S. 31, 37.

46 Zuletzt Europäische Kommission, Vierter Jahresbericht über die Überprüfung ausländischer Direktinvestitionen in der Union, COM(2024) 464 final.

47 Europäische Kommission, Mitteilung der Kommission, Leitlinien für die Mitgliedstaaten betreffend ausländische Direktinvestitionen, freien Kapitalverkehr aus Drittländern und Schutz der strategischen Vermögenswerte Europas im Vorfeld der Anwendung der Verordnung (EU) 2019/452 über die Überprüfung ausländischer Direktinvestitionen, ABl. C 99I/1. Vgl. dazu *Sahin*, Die Leitlinien der Europäischen Kommission zur Kontrolle ausländischer Direktinvestitionen in der COVID-19-Krise, in: COVID-19 und Recht, COVuR 2020, 192; Europäische Kommission, Mitteilung der Kommission Leitlinien für die Mitgliedstaaten betreffend ausländische Direktinvestitionen aus Russland und Belarus angesichts der militärischen Aggression gegen die Ukraine und der in den jüngsten Verordnungen des Rates über Sanktionen festgelegten restriktiven Maßnahmen (Verordnung (EU) Nr. 833/2014 des Rates über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren (ABl. L 229 vom 31.7.2014, S. 1) und ihre Änderungen sowie Verordnung (EG) Nr. 765/2006 des Rates vom 18. Mai 2006 über restriktive Maßnahmen angesichts der Lage in Belarus (ABl. L 134 vom 20.5.2006, S. 1) und ihre Änderungen.) 2022/C 151 I/01.

48 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Überprüfung ausländischer Investitionen in der Union und zur Aufhebung der Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates, COM (2024) 23 final.

wesentliche Neuerung in einer expliziten Einbeziehung sog. „Investitionen innerhalb der Union unter ausländischer Kontrolle" (Art. 2 Nr. 1 u. 3). Sie werden definiert als „eine Investition jeder Art, die von einem ausländischen Investor über dessen Tochterunternehmen in der Union getätigt wird und darauf abzielt, dauerhafte und direkte Beziehungen zwischen dem ausländischen Investor und einem bestehenden oder zu gründenden Ziel in der Union zu schaffen oder aufrechtzuerhalten, und für die der ausländische Investor Kapital bereitstellt, um eine wirtschaftliche Tätigkeit in einem Mitgliedstaat auszuüben". Diese Anpassung war als notwendig erachtet worden, nachdem der EuGH in der Rs. *Xella* – einer sehr formalistischen Auslegung des Art. 1 Abs. 1 EU-Screening-VO folgend – derartige Investitionstätigkeiten als nicht vom Anwendungsbereich der EU-Screening-VO umfasst angesehen hatte.[49] Auch erweitert der Reformvorschlag die bereits bestehende Liste sog. Unionsprogramme und fügt zugleich Technologien hinzu, die einem unionalen Sicherheitsinteresse entsprechen (Annex I und II). Insgesamt bleibt es indes bei der unvollständig zweistufigen Architektur der europäischen Investitionskontrolle.

II. Der Schutz maritimer Infrastrukturen durch die EU-Screening-Verordnung

Maritime Infrastrukturen werden innerhalb der EU-Screening-VO nicht explizit erwähnt, jedoch auf zweifache Weise in Bezug genommen: Zunächst „können" die Mitgliedstaaten und die Kommission gemäß Art. 4 Abs. 1 EU-Screening-VO bei der Prüfung, ob eine ausländische Direktinvestition die Sicherheit oder die öffentliche Ordnung voraussichtlich beeinträchtigt, potentielle Auswirkungen auf verschiedene in lit. a bis e aufgeführte Bereiche „berücksichtigen". In diesem Zusammenhang erwähnt lit. a „kritische Infrastrukturen physischer oder virtueller Art, einschließlich Energie, Verkehr, Wasser, Gesundheit, Kommunikation, Medien, Datenverarbeitung oder -speicherung, Luft- und Raumfahrt, Verteidigung, Wahl- oder Finanzinfrastrukturen und sensible Einrichtungen sowie Investitionen in Grundstücke und Immobilien, die für die Nutzung dieser Infrastrukturen von entscheidender Bedeutung sind". Diese beispielhafte Auflistung umfasst ein breites Spektrum von Einrichtungen und Vermögenswerten, die als kritisch für

49 EuGH, Urt. v. 13.7.2023, C-106/2022– Xella Magyarország, Rn. 29 ff.

das Funktionieren eines Mitgliedstaats oder der EU als Ganzes gelten.[50] Darüber hinaus bezieht etwa lit. c die „Versorgung mit kritischen Ressourcen, einschließlich Energie oder Rohstoffen, sowie Nahrungsmittelsicherheit" in eine mögliche Prüfung ein.

Die einzelnen Begriffe sind hochgradig konkretisierungsbedürftig, auch enthält Art. 4 Abs. 1 EU-Screening-VO keine Angaben zu Schwellenwerten.[51] Man wird hierunter jedoch – gerade wegen der offenen Formulierung – unproblematisch den Gesamtbereich maritimer Infrastrukturen fassen können. Primärrechtlich betrachtet erstreckt sich der Begriff „Verkehr" auch auf die Seeschifffahrt (Art. 100 Abs. 2 AEUV). Zudem lassen sich mit dem Schlagwort der „transeuropäischen Netze" (Art. 170 bis 172 AEUV) „transnationale" Verkehrs-, Telekommunikations- und Energieinfrastrukturen wie Häfen oder Leitungen verbinden.[52] Art. 194 AEUV steht daneben für ein weites Verständnis im Hinblick auf den Gesamtbereich „Energie".[53] Abgesehen davon kommt es für eine Effektuierung der in Art. 4 Abs. 1 EU-Screening-VO angelegten Prüfung entscheidend auf die Ausgestaltung des jeweiligen nationalen Investitionskontrollrechts der Mitgliedstaaten an, denen in Bezug auf eine Benennung kritischer Sektoren ein Ermessensspielraum eingeräumt wird.[54]

Ein weiterer Anknüpfungspunkt für eine Berücksichtigung maritimer Infrastrukturen in der Investitionskontrolle bietet die im Anhang zur EU-Screening-VO enthaltene Auflistung der in Art. 8 Abs. 3 genannten „Projekte oder Programme von Unionsinteresse". Hier wird explizit auf das Transeuropäische Verkehrsnetz (TEN-T), Energienetz (TEN-E) und die Transeuropäischen Netze im Bereich der Telekommunikation Bezug genommen (Nr. 4, 5 und 6). Art. 8 Abs. 1 EU-Screening-VO sieht dabei eine Stellungnahmemöglichkeit der Kommission gegenüber dem Mitgliedstaat vor, in dem eine betreffende ausländische Direktinvestition geplant ist oder abgeschlossen wurde. Der Mitgliedstaat trägt der Stellungnahme der Kommission „umfassend Rechnung und gibt der Kommission gegenüber eine Erklärung ab, falls er deren Stellungnahme nicht nachkommt" (Art. 8 Abs. 2 lit. c EU-Screening-VO).

---

50 *Lübbig, Salaschek*, in: Röhling/Stein, Recht der Investitionskontrolle, 2023, Screening-VO Rn. 121.

51 *Voland, Slobodenjuk* (Fn. 33), Art. 4 VO (EU) 452/2019 Rn. 7.

52 So im Hinblick auf die Einbeziehung maritimer Infrastrukturen in den Anwendungsbereich auch *Schubert* (Fn. 1), S. 69 ff.

53 *Schubert* (Fn. 1), S. 79 ff.

54 *Lübbig, Salaschek* (Fn. 50), Rn. 122.

Unabhängig von dem Vorliegen eines solchen Projekts oder Programms, können die Kommission und die Mitgliedstaaten gemäß dem in Art. 7 EU-Screening-VO vorgesehenen Verfahren Mitgliedstaaten, in denen eine Überprüfung einer ausländischen Direktinvestition nicht durchgeführt wurde, zu einer Erklärung hierüber auffordern bzw. Kommentare und Stellungnahmen an diesen richten, die dieser „angemessen" berücksichtigen muss. Diese Möglichkeit steht neben der Mitteilungspflicht des Art. 6 Abs. 1 EU-Screening-VO, die sich auf Fälle bezieht, die einer Überprüfung unterliegen. Eine durchsetzbare Verpflichtung zur Berücksichtigung von Prüfungsbegehren oder Anmerkungen anderer Mitgliedstaaten sowie der Kommission besteht allerdings nicht. Der Kooperationsmechanismus dient eher der Identifizierung möglicher EU-weit relevanter Fälle, die bereits geprüft oder noch ungeprüft sind. Hierzu sollen die Mitgliedstaaten untereinander sowie zusammen mit der Kommission in einen Austausch treten können.

Insgesamt bleibt der Beitrag der EU-Screening-VO zum Schutz maritimer Infrastrukturen damit überschaubar. Mangels eigener Prüfkompetenz, ist die EU hier auf ein Tätigwerden der Mitgliedstaaten angewiesen und kann diese lediglich informieren bzw. zu einem Vorgehen auffordern. Grundvoraussetzung eines nationalen Vorgehens ist jedoch wiederum eine entsprechende Rechtsgrundlage. Diesbezüglich enthält die EU-Screening-VO bislang keine Vorgaben dazu, in welcher Weise maritime Infrastrukturen und andere Sektoren im Rahmen der Prüfung Berücksichtigung finden sollen.

In Folge der Reform der EU-Screening-VO sollen die Mitgliedstaaten nun dazu verpflichtet werden, eine Notifizierungspflicht jedenfalls für die in Annex I und II genannten Programme und Projekte bzw. Technologien vorzusehen (Art. 4 Abs. 4 des Reformvorschlags). Dies umfasst u.a. die bislang durch Art. 8 Abs. 3 EU-Screening-VO in Bezug genommenen Transeuropäischen Netze (Annex I, Nr. 7 bis 9). Die Mitgliedstaaten sollen zudem jede Anmeldung in diesem Bereich innerhalb des Kooperationsnetzwerkes den anderen Mitgliedstaaten sowie der Kommission gegenüber mitteilen (Art. 5 Abs. 1). Es bleibt allerdings dabei, dass Mitgliedstaaten die im Wege des Kooperationsmechanismus erhaltenen Kommentare und Stellungnahmen lediglich „weitestgehend" berücksichtigen müssen (Art. 7 Abs. 5). Inwieweit hierin eine echte Steigerung gegenüber einer „angemessenen" Berücksichtigung liegt, wird sich zeigen müssen. Zusätzlich müssen sie sich nunmehr ggf. in einem eigenen Meeting erklären, wenn sie diesen nicht hinreichend Rechnung tragen (Abs. 9).

Eine weitere Änderung betrifft die bislang in Art. 4 Abs. 1 EU-Screening-VO vorgesehene Berücksichtigung von Auswirkungen einer ausländischen Direktinvestition auf spezifische Sektoren. Art. 13 Abs. 3 formuliert nun explizit eine Pflicht zur Berücksichtigung derartiger Auswirkungen bei der materiellen Prüfung. Art. 13 Abs. 3 lit. a spricht dabei nur noch von der „Sicherheit, Integrität und Funktionsweise kritischer physischer oder virtueller Infrastrukturen", bezieht dabei zugleich allerdings auch die Resilienz sog. „kritischer Einrichtungen" i.S.d. Richtlinie (EU) 2022/2557[55] und der Richtlinie (EU) 2022/2555[56] mit ein. Hinter diesem Begriff steht eine öffentliche oder private Einrichtung, die von den Mitgliedstaaten bis zum 17. Juli 2026 als kritisch eingestuft wurde (Art. 6 RL (EU) 2022/2557). Diese Form der Konkretisierung anhand des einschlägigen Sekundärrechts war so von der Literatur bereits nahegelegt worden.[57] Hierdurch bleibt der eingeräumte Spielraum der Mitgliedstaaten zugleich erhalten. Abgesehen vom Bereich der kritischen Infrastrukturen und Einrichtungen sollen weiterhin Auswirkungen etwa auf die Versorgung mit kritischen Ressourcen (lit. c) berücksichtigt werden.

Der Reformvorschlag nimmt damit einzelne wichtige Anpassungen vor, insbesondere durch die Pflicht zur Einführung einer Investitionskontrolle und der verpflichtenden Berücksichtigung kritischer Infrastrukturen im Rahmen der inhaltlichen Prüfung. Zugleich vermag er es jedoch mangels zentraler Prüfungskompetenz auf EU-Ebene nicht, eine Stärkung eines gesamteuropäischen Schutzes maritimer Infrastrukturen durch die EU-Screening-VO zu bewirken.

55 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333 vom 27.12.2022, S. 164.

56 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), ABl. L 333 vom 27.12.2022, S. 80.

57 *Lübbig, Salaschek* (Fn. 50), Rn. 124.

III. Maritime Infrastrukturen als Schutzobjekt der Investitionskontrolle in Deutschland

Der Schutz maritimer Infrastrukturen durch das deutsche Investitionskontrollrecht wurde bzw. wird spätestens seit dem Einstieg des chinesischen Unternehmens *COSCO* im Hamburger Hafen in der Öffentlichkeit kontrovers diskutiert.[58] Es darf indes nicht übersehen werden, dass bereits zuvor chinesische Investitionen im Bereich maritimer Infrastrukturen durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ohne vergleichbares Aufsehen genehmigt wurden, so etwa der Erwerb einer 80 % Beteiligung des chinesischen Unternehmens *China Three Gorges* am deutschem Offshore-Windpark „Meerwind".[59] *COSCO* plante ursprünglich eine Beteiligung von 35 % am Terminal Tollerort zu erwerben, die sich in Folge einer politischen Auseinandersetzung zwischen Bundeskanzler *Olaf Scholz* mit Wirtschaftsminister *Robert Habeck*, aber auch dem Auswärtigen Amt und anderen Stellen, schließlich auf 24,9 % reduzierte. Dem Fall lässt sich weniger eine mangelnde Reichweite der deutschen Investitionskontrolle bei der Prüfung von Investitionen im Bereich maritimer Infrastrukturen entnehmen als vielmehr die nicht unproblematische politische Einflussnahme auf den Entscheidungsprozess im Rahmen eines investitionskontrollrechtlichen Verfahrens.[60]

Allgemein ist in Deutschland die Kontrolle ausländischer Investitionen innerhalb der §§ 4, 5, 6, 14a und 15 des Außenwirtschaftsgesetzes (AWG) sowie der §§ 55 bis 62a der Außenwirtschaftsverordnung (AWV) gebündelt worden.[61] Einzelne Spezialkontrollen, wie etwa im Bereich des Satellitendatensicherheitsgesetzes, sind darin aufgegangen.[62] Bestand haben daneben

58 Zu diesem Fall *Herrmann*, Hamburger Hafenrundfahrt im Regierungsviertel: Investitionskontrollrechtliche Überlegungen zur Übernahme eines Hamburger Terminals durch die chinesische Reederei COSCO, VerfBlog, 2022/10/25, https://verfassungsblog.de/hamburger-hafenrundfahrt-im-regierungsviertel/ (letzter Abruf am 15.01.25); *von Rummel/Gertz*, Einführung in die deutsche Investitionskontrolle anlässlich des COSCO Investments am Hamburger Container Terminal Tollerort, Recht der Transportwirtschaft, RdTW 2022, 465; *Bungenberg, Reinhold* (Fn. 20), Rn. 39 ff.; Chinese Investments in European Maritime Infrastructure, PE 747.278, September 2023, S. 28.

59 *Bungenberg, Reinhold* (Fn. 20), Rn. 13.

60 Vgl. *Herrmann* (Fn. 58); *von Rummel, Gertz*, (Fn. 58), 470; *Bungenberg, Reinhold* (Fn. 20), Rn. 85.

61 Zum Entstehungsprozess *Bungenberg, Reinhold* (Fn. 20), Rn. 44 ff.; auch *Röhling/Stein*, in: dies., Recht der Investitionskontrolle, 2023, Einl. Rn. 1 ff.

62 *Bungenberg, Reinhold* (Fn. 20), Rn. 50.

weiterhin ganz spezifische Marktzugangskontrollen, teils auch mit großer Relevanz für den maritimen Sektor, wie etwa die Möglichkeit eines Ausschlusses von unionsfremden Bietern von Ausschreibungsverfahren im Bereich der Windenergie, sofern „die Bezuschlagung oder der Betrieb der gebotsgegenständlichen Anlage die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt" (§ 15 Abs. 2 des Windenergie-auf-See-Gesetzes; WindSeeG). Hinsichtlich der allgemeinen Investitionskontrolle bestehen derzeit Pläne für eine Herauslösung aus AWG/AWV und Überführung in ein eigenständiges Gesetz.[63] Dabei ist nach derzeitigem Stand jedoch nicht von einer substantiellen Anpassung des Prüfverfahrens auszugehen. Zu der bestehenden investitionskontrollrechtlichen Vorabprüfung eines Erwerbsvorgangs (1.) treten weiterhin zusätzliche einzelfallbezogene Eingriffsbefugnisse hinzu, die i.S.e. nachträglichen Investitionskontrolle wirken können (2.).

1. Die Überprüfung von Investitionen im Bereich maritimer Infrastrukturen

Das geltende Investitionskontrollrecht unterscheidet zwischen einer sektorübergreifenden (§§ 55 ff. AWV) und einer sektorspezifischen Kontrolle (§§ 60 ff. AWV), wobei in dem einen Fall eine „voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit" Deutschlands, eines anderen EU-Mitgliedstaats oder in Bezug auf ein Projekt bzw. Programm i.S.v. Art. 8 Abs. 3 EU-Screening-VO als Maßstab einer Intervention fungiert, während es im Bereich der sektorspezifischen Kontrolle auf eine „voraussichtliche Beeinträchtigung wesentlicher Sicherheitsinteressen der Bundesrepublik Deutschland" ankommt. In beiden Fällen kommt es dadurch zu einer vorausschauenden Gefahrenanalyse, die sich allerdings zugleich auf gewisse Anhaltspunkte stützen muss.[64] Der Prüfungsmaßstab einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit ist als unionsrechtlicher Begriff nach der Rechtsprechung des EuGH mit einer hinreichend „schweren Gefährdung" von „Grundinteressen der Gesellschaft"[65] zu übersetzen und schließt dadurch eine Einbeziehung rein

63 Dazu *Bungenberg, Reinhold*, Reform des Investitionskontrollrechts – Stärkung von Effektivität, Effizienz und Rechtsstaatlichkeit, ZASA 2023, 314.

64 *Herrmann* (Fn. 39), 429 (448 ff.); *Bungenberg, Reinhold* (Fn. 20), Rn. 353 ff.

65 Ständige Rspr. EuGH, Urt. v. 18.10.1975, C-36/1975 – Rutili/Ministre de l'intérieur, Rn. 28; Urt. v. 20.10.1977, C-30/1977 – Regina, Bouchereau, Rn. 35; Urt. v. 14.3.2000,

wirtschaftlicher Gesichtspunkte aus.[66] Ein Beurteilungsspielraum wird von der h.M., wenn überhaupt, nur für spezifische Konstellationen (etwa der sicherheits- und verteidigungspolitischen Einschätzung) anerkannt.[67] Etwas anderes gilt für den engen Bereich der wesentlichen Sicherheitsinteressen im Bereich der sektorspezifischen Investitionskontrolle.[68]

Das Prüfverfahren ist in beiden Fällen zweistufig ausgestaltet und wird entweder durch die (verpflichtende) Meldung eines Erwerbs[69] oder durch Eigeninitiative des BMWK oder einen Antrag auf Unbedenklichkeitsbescheinigung gem. § 58 AWV ausgelöst.[70] Das BMWK entscheidet hierbei in einer ersten Prüfphase von zwei Monaten zunächst, ob es von seiner Prüfkompetenz überhaupt Gebrauch machen will (§ 14a Abs. 1 Nr. 1 AWG). Für die zweite Prüfphase gilt anschließend eine Frist von vier Monaten, die jedoch in besonderen Fällen verlängert werden oder auch gehemmt sein kann (§ 14a Abs. 1 Nr. 2, Abs. 4 und 6 AWG).[71] Abschließende Maßnahmen können die Freigabe des Erwerbs (§§ 58a Abs. 1, 61 Satz 1 AWV), die Untersagung (§§ 59, 62 AWV) oder auch eine Freigabe unter Auflagen sein (§§ 58a Abs. 3, 61 Satz 3 AWV). Bei einer Untersagung bedarf es gem. § 13 Abs. 3 AWG der Zustimmung durch die Bundesregierung, durch die eine – im *COSCO*-Fall augenscheinlich gewordene – politische Einflussnahme eröffnet wird.

C-54/1999 – Association Église de scientologie de Paris, Rn. 17; Urt. v. 7.6.2012, C-39/11 – VBV - Vorsorgekasse, Rn. 29; Urt. v. 16.9.2020, C-339/2019 – Romenergo und Aris Capital, Rn. 40.

66 *Bungenberg, Reinhold* (Fn. 20), Rn. 347; *Röhling, Salaschek*, in: ders./Stein, Recht der Investitionskontrolle, 2023, § 55 AWV Rn. 30.

67 So etwa *Voland*, Voland: Rechtsschutz gegen Maßnahmen der Investitionskontrolle im Außenwirtschaftsrecht - Fiat iustitia?! EuZW 2010, 132 (135 f.); *Bungenberg, Reinhold* (Fn. 20), Rn. 350; *Ludwig*, Die Kontrolle ausländischer Direktinvestitionen, 2023, S. 393 ff.; *Backenstraß, Kirst*, Die gerichtliche Überprüfbarkeit behördlicher Entscheidungen im Rahmen der sektorübergreifenden Investitionskontrolle, ZEuS 2023, 279 (292 ff.); *Röhling, Salaschek* (Fn. 66), § 55 AWV Rn. 39 ff. A.A. *Sattler*, in: Sachs/Pelz, Außenwirtschaftsrecht, 3. Aufl. 2024, § 55 AWV Rn. 87, der pauschal auf einen Beurteilungsspielraum verweist.

68 *Bungenberg, Reinhold* (Fn. 20), Rn. 376; *Stein, Kassem*, in: Röhling/ders., Recht der Investitionskontrolle, 2023, § 60 AWV Rn. 42 f.

69 Näher zum Erwerbsbegriff *Bungenberg, Reinhold* (Fn. 20), Rn. 103 ff. u. 152 ff.; *Röhling, Salaschek* (Fn. 666), § 56 AWV Rn. 6 ff.

70 Zum Verfahren *Bungenberg, Reinhold* (Fn. 20), Rn. 44 ff.; auch *Friton, Ackermann*, in: Röhling/Stein, Recht der Investitionskontrolle, 2023, § 14a AWG Rn. 4 ff.

71 Zu den Verlängerungs- bzw. Hemmungsgründen *Bungenberg, Reinhold* (Fn. 20), Rn. 94 ff.; auch *Friton, Ackermann* (Fn. 70), § 14a AWG Rn. 17 ff.

Von entscheidender Bedeutung sowohl für die Frage nach dem Bestehen einer Meldepflicht als auch im Rahmen der inhaltlichen Prüfung durch das BMWK („kann insbesondere berücksichtigt werden") sind die in § 55a Abs. 1 bzw. § 60 Abs. 1 Satz 1 AWV genannten Fallgruppen. Während für Erwerbsziele i.S.v. § 55a Abs. 1 Nr. 1 bis 7 oder § 60 Abs. 1 Satz 1 Nr. 1 bis 4 AWV eine Erwerbsschwelle von 10 % der Stimmrechte gilt, liegt sie für Ziele i.S.v. § 55a Abs. 1 Nr. 8 bis 27 AWV bei 20 % und in Bezug auf alle sonstigen Unternehmen bei 25 %.

Maritime Infrastrukturen werden weder in § 55a Abs. 1 noch in § 60 Abs. 1 Satz 1 AWV explizit genannt. § 55a Abs. 1 Nr. 1 AWV bezieht sich allerdings auf Betreiber einer „kritischen Infrastruktur" nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz).[72] Gemäß § 2 Abs. 10 BSI-Gesetz werden kritische Infrastrukturen darin definiert als „Einrichtungen, Anlagen oder Teile davon, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden". Eine genaue Zuordnung im Einzelfall ist nur in Verbindung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) möglich, worin

72 Zu dieser Fallgruppe *Bungenberg, Reinhold* (Fn. 20), Rn. 110 ff.; *Röhling, Salaschek* (Fn. 66), § 55a AWV Rn. 3 ff. Der Gesetzgeber plant daneben den Erlass eines Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz), s. dazu den Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, BT-Drucks. 20/13961. Darin wird der Begriff „maritime Infrastrukturen" räumlich definiert als „Anlagen auf oder unter See im Küstenmeer und der ausschließlichen Wirtschaftszone der Bundesrepublik Deutschland" (§ 2 Nr. 12). Als „Anlage" wird „eine Betriebsstätte, eine sonstige ortsfeste Installation, eine Maschine, ein Gerät und eine sonstige ortsveränderliche technische Installation" verstanden, die dann als „kritisch" einzuordnen ist, wenn sie „für die Erbringung einer kritischen Dienstleistung erheblich ist" (§ 2 Nr. 2 und 3). Eine „kritische Dienstleistung" ist nach dem Entwurf „eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde" (Nr. 4). Da die AWV bislang allerdings allein das BSI-Gesetz für die Zwecke einer näheren Konkretisierung kritischer Infrastrukturen in Bezug nimmt, ist im Folgenden allein auf dieses abzustellen.

die Kritikalität des Erwerbsziels je nach Sektor und anhand verschiedenster Schwellenwerte genauer aufgeschlüsselt wird.

Maritime Infrastrukturen lassen sich in diesem Zusammenhang innerhalb der Sektoren Energie (§ 2 BSI-KritisV, Anhang 1), Kommunikation (§ 5 BSI-KritisV, Anhang 4) sowie Verkehr (§ 8 BSI-KritisV, Anhang 7) verorten. Punktförmige Anlagen wie Offshore-Windräder können der in § 2 BSI-KritisV umfassend angesprochenen Energieversorgung zugeordnet werden. Anhang 1, Teil 1, Ziff. 2.1 BSI-KritisV bezieht sich dabei auf Erzeugungsanlagen i.S.v. § 3 Nr. 11 Energiewirtschaftsgesetz, deren Kritikalität sich nach der auf Basis von Teil 2 berechneten installierten Nettonennleistung i.S.d. in Teil 3 enthaltenen Tabelle bemisst. Darüber hinaus sind grundsätzlich auch Anlagen zur Energieübertragung von § 2 i.V.m. Anlage 1 BSI-KritisV umfasst. Infrastruktureinrichtungen wie bspw. Seekabelanlandestationen werden gar explizit in § 5 i.V.m. Anlage 4 Teil 1 Ziff. 2.3 bzw. Teil 3 Ziff. 1.2.2 BSI-KritisV genannt. Die erforderliche hohe Bedeutung für das Funktionieren der Gesellschaft wird hierbei ab einem angebundenen Seekabel angenommen. Schließlich werden Einrichtungen der See- und Binnenschifffahrt in § 8 Abs. 2 i.V.m. Anlage 7 Teil 1 Ziff. 1.14 bis 1.19 u. 1.25 bzw. Teil 3 Ziff. 1.3 u. 1.6 BSI-KritisV aufgeführt, wobei sich die notwendig hohe Bedeutung anhand der Güter- bzw. Frachtmenge bestimmt. Vor diesem Hintergrund war etwa die Beteiligung von *COSCO* als Erwerb einer kritischen Infrastruktur i.S.v. § 2 Abs. 10 BSIG i.V.m. § 8 Abs. 3 und Anlage 7, Ziel 1 Ziff. 1.25 u. Teil 3 Ziff. 1.3.5 BSI-KritisV zu betrachten.

Inwieweit die innerhalb der BSI-KritisV angegebenen Schwellenwerte mögliche Sicherheitsrisiken angemessen widerspiegeln, lässt sich juristisch nicht beurteilen. Allerdings lassen sich sowohl die erfassten Anlagen als auch deren zugehöriger Schwellenwert durch Anpassung der BSI-KritisV gem. § 10 Abs. 1 BSI-Gesetz ohne gleichzeitige Änderung von AWG und AWV modifizieren. So kann zugleich der investitionskontrollrechtliche Anwendungsbereich des § 55a Abs. 1 Nr. 1 AWV gesteuert werden. Aus diesem ergibt sich für maritime Infrastrukturen derzeit eine Meldepflicht ab einem Erwerb von 10 % der Stimmrechte (§§ 55a Abs. 4 S. 1, 56 Abs. 1 AWV). § 56 Abs. 2 stellt klar, dass diese sich auch auf einen Zuerwerb bezieht, der zu einem Anteil von 20, 25, 40, 50 oder 75 % der Stimmrechte führt. Außerdem werden durch Möglichkeiten des mittelbaren bzw. atypischen Kontrollerwerbs (§ 56 Abs. 3 bis 5 AWV) Umgehungslücken geschlossen.[73]

73 Umfassend dazu *Röhling, Salaschek* (Fn. 66), § 56 AWV Rn. 25 ff.

Es sei zudem darauf hingewiesen, dass § 55 Abs. 2 Satz 1 AWV bereits jetzt missbräuchliche Gestaltungen durch Unionsansässige erfasst.

2. Zusätzliche Eingriffsrechte nach Außenwirtschaftsgesetz und Energiesicherheitsgesetz

Außerhalb eines konkreten Investitionskontrollverfahrens verbleiben dem BMWK in Einzelfällen zusätzliche Interventionsmöglichkeiten nach dem AWG und teils auch anderen Spezialgesetzen, wie insbesondere dem Energiesicherungsgesetz (EnSiG).[74] Diese Eingriffsbefugnisse sind im Rahmen des russischen Überfalls auf die Ukraine relevant geworden, in Folge dessen sich Deutschland der Gefahr ausgesetzt sah, dass Russland seinen Einfluss auf russische Energieunternehmen dazu einsetzen könnte, die deutsche Energieversorgung zu beeinträchtigen. So wurde zunächst das russische Unternehmen *Gazprom Germania GmbH* auf Basis von § 6 Abs. 1 AWG unter die Treuhandschaft der Bundesnetzagentur gestellt.[75] § 6 Abs. 1 AWG berechtigt zu Beschränkungen von Rechtsgeschäftigen oder sonstigen Handlungen sowie zur Anordnung von Handlungspflichten, insofern eine konkrete und gegenwärtige Gefahr für die nach § 4 Abs. 1 AWG geschützten Güter besteht, zu denen auch die öffentliche Ordnung oder Sicherheit bzw. die wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland gehören.

Eine spätere Anordnung einer Treuhandverwaltung gegenüber der *Rosneft Deutschland GmbH* und der *RN Refining & Marketing GmbH* wurde von Seiten des BMWK auf § 17 EnSiG gestützt, durch den Eingriffsbefugnisse gegenüber Unternehmen eingeräumt werden, die im Bereich kritischer Energieinfrastrukturen i.S.v. § 2 Abs. 10 des BSI-Gesetzes tätig sind, insofern eine Beeinträchtigung der Versorgungssicherheit droht.[76] Das BVerwG hat diese Treuhandanordnung gem. § 17 EnSiG inzwischen bestä-

74 Dazu *Bungenberg, Reinhold* (Fn. 20), Rn. 168 ff.

75 *BMWK*, Anordnung gemäß § 6 des Außenwirtschaftsgesetzes bezüglich der Anteile an der Gazprom Germania GmbH v. 4. April 2022, BAnz AT 04.04.2022 B13. Dazu *Ludwig,* Energiesicherheit durch Außenwirtschaftsrecht: Die Bestellung der Bundesnetzagentur durch das BMWi zum Treuhänder für die Betreiberfirmen von Erdgasspeichern in Deutschland, VerfBlog, 2022/4/06, abrufbar unter: https://verfassungsblog.de/energiesicherheit-durch-ausenwirtschaftsrecht/ (letzter Abruf am 15.01.25).

76 Näher dazu *Bungenberg, Reinhold* (Fn. 20), Rn. 171 ff.; *Holterhus*, Verfassungs-, unions- und völkerrechtliche Aspekte der Treuhandverwaltung nach dem Energiesicherungsgesetz (EnSiG), NVwZ 2024, 554.

tigt und dabei deutlich gemacht, dass derartige Eingriffe durch die Verfolgung des überragend wichtigen gemeinschaftlichen Ziels der Gewährleistung der Energieversorgung grds. gerechtfertigt werden können.[77] Neben einer Treuhandverwaltung erlauben die §§ 17a, 17b, 18 und 19 EnSiG daneben weitere Interventionen in den unternehmerischen Geschäftsbetrieb bis hin zu einer Enteignung (§§ 18, 19 EnSiG).

Damit wird jedenfalls ein Teil der maritimen Infrastruktur durch spezifische Kontrollinstrumente abgedeckt, während etwa im Bereich von Häfen – neben allgemeinen polizeirechtlichen Befugnissen – ein Einzeleingriff gem. § 6 AWG in Betracht kommt. Bei all diesen Maßnahmen ist jedoch zu beachten, dass sich hierbei durchaus eine Verletzung grundrechtlicher und auch völkerrechtlicher investitionsschutzrechtlicher Standards ergeben kann.[78]

3. Schutz maritimer Infrastrukturen durch das deutsche Investitionskontrollrecht

Insgesamt ergibt sich damit in Bezug auf maritime Infrastrukturen ein recht weiter Anwendungsbereich der deutschen Investitionskontrolle, die sowohl eine Vorabprüfung als auch Möglichkeiten einer nachträglichen Intervention im Einzelfall umfasst. Eine andere Frage ist, wie das BMWK die ihm eingeräumte Prüfungsbefugnis ausübt. Bislang werden gemeldete Erwerbsvorgänge weit überwiegend freigegeben oder ein Phase II-Verfahren gar nicht erst eröffnet, was indes nicht darauf hindeuten muss, dass hier eine Schutzlücke besteht.[79] Der Fall *COSCO* zeigt, dass die Überprüfung in der Praxis grundsätzlich funktioniert, zugleich jedoch bei Untersagungen eine starke politische Einflussnahme erfolgen kann. Dies ändert indes nichts an der grundsätzlich bestehenden Möglichkeit zur Identifizierung investitionsbezogener Sicherheitsrisiken für maritime Infrastrukturen innerhalb der deutschen Investitionskontrolle. Daneben haben die Fälle um *Gazprom* und *Rosneft* deutlich gemacht, dass der deutsche Staat in Notsituationen

77 BVerwG, Urt. v. 14.3.2022 – 8 A 2.22, NVwZ 2023, 1326 Rn. 35; Dazu *Holterhus* (Fn. 76).

78 Dazu im Hinblick auf den *Rosneft*-Fall *Holterhus* (Fn. 76), 554 (559 ff.).

79 Bericht des Bundesministeriums für Wirtschaft und Klimaschutz, Evaluierung des Ersten Gesetzes zur Änderung des Außenwirtschaftsgesetzes und der 15.–17. Verordnung zur Änderung der Außenwirtschaftsverordnung, Stand: September 2023, S. 17 f.; Investitionsprüfung in Deutschland: Zahlen und Fakten, Sämtliche Zahlen mit Stand vom 31.01.2025, S. 12.

durchaus handlungsfähig ist, auch wenn Investitionen in kritischen Bereichen bereits getätigt wurden. Über den rein nationalen Bereich hinaus ist Deutschland allerdings zugleich von einer effektiven Kontrolle durch die anderen Mitgliedstaaten abhängig.

IV. Das Schutzniveau der Investitionskontrolle im europäischen Vergleich

Inzwischen verfügt der Großteil der EU-Mitgliedstaaten über eine Form der Investitionskontrolle und ist zugleich in das durch die EU-Screening-VO geschaffene Kooperationsnetzwerk eingebunden.[80] Neben Deutschland gehören dabei Belgien, Bulgarien, Dänemark, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Malta, die Niederlande, Polen, Portugal, Rumänien, Schweden, Slowenien, Spanien und Zypern zu den Küstenstaaten der EU. Von diesen verfügen lediglich Griechenland, Kroatien und Zypern bislang über keine nationale Investitionskontrolle.

In Bezug auf Griechenland dürfte dies mit der weitreichenden Beteiligung von *COSCO* im Hafen von Piräus und der damit verbundenen „China-Freundlichkeit" Griechenlands zusammenhängen.[81] Zypern diskutiert seit dem Jahr 2022 über einen Legislativvorschlag, der ab einer Stimmrechtsbeteiligung von 10 % eine Notifizierungspflicht vorsieht und sich im Übrigen eng an der EU-Screening-VO orientiert, d.h. auch die dort benannten Sektoren in den Blick nimmt.[82] Auch Kroatien strebt den Erlass eines nationalen Investitionskontrollgesetze an.[83] Einen Schritt weiter ist inzwischen Irland, wo mit dem „Screening of Third Country Transactions Act 2023" ein Rechtsakt geschaffen wurde, der seit dem 1. Januar 2025 An-

80 Siehe dazu bereits Abschnitt B.I.

81 Chinese Investments in European Maritime Infrastructure, PE 747.278, September 2023, S. 25.

82 Siehe dazu *Papadopoulos, Christofides*, CELIS Briefing Note: Cyprus – Republic of Cyprus' FDIS Bill: State of Play, Oktober 2022, abrufbar unter: https://www.celis.institute/celis-news/celis-briefing-note-cyprus-republic-of-cyprus-fdis-bill-state-of-play/ (letzter Abruf am 15.01.25).

83 Siehe den Hinweis unter https://www.linklaters.com/en/insights/blogs/foreigninvestmentlinks/2024/march/eu-member-states-without-an-fdi-regime (letzter Abruf am 15.01.25).

wendung findet und der sich ebenfalls an den von Art. 4 Abs. 1 EU-Screening-VO benannten Sektoren orientiert (Art. 9 Abs. 1 lit. d).[84]

Die Abwesenheit eines Prüfmechanismus bedeutet eine regulatorische Lücke im europäischen Investitionskontrollsystem. Als Konsequenz können investitionsbezogenen Sicherheitsrisiken für maritime Infrastrukturen (und andere kritische Sektoren) in dem betreffenden Mitgliedstaat nicht identifiziert und effektiv adressiert werden, woraus sich zugleich negative Folgen für die übrigen EU-Mitgliedstaaten ergeben können. Dies betrifft gerade auch diejenigen Mitgliedstaaten, die selbst über keinen Küstenabschnitt verfügen und daher zur eigenen Versorgung auf die Häfen anderer Mitgliedstaaten angewiesen sind.

Die *OECD* hat in ihrer Evaluation zur EU-Screening-VO darüber hinaus zu Recht auch den teils stark voneinander abweichenden Anwendungsbereich sowie Prüfungsmaßstab bestehender nationaler Kontrollen kritisiert.[85] Teilweise übernehmen die nationalen Gesetzgeber den Katalog des Art. 4 Abs. 1 EU-Screening-VO und beziehen dadurch auch maritime Infrastrukturen mit ein.[86] Andere benennen ihren eigenen Bereich sensitiver Sektoren, was indes nicht zugleich bedeutet, dass maritime Infrastrukturen nicht erfasst wären.[87] Vor allem aber bestehenden Unterschiede bei der Eingriffsschwelle und der administrativen Ausstattung der Behörden.[88] Eine weitere Folge der dezentralen Ausgestaltung ist zwangsläufig auch die mögliche politische Einflussnahme, wie der Fall *COSCO* zeigt. Hier können sich zugleich Risiken durch ein starkes Engagement Chinas in einzelnen europäischen Mitgliedstaaten ergeben.

Insgesamt zeigt sich damit, dass europaweit Unterschiede hinsichtlich des Schutzes maritimer Infrastrukturen durch die Mitgliedstaaten bestehen, bis hin zu offenen Schutzlücken. Letztere sollen durch die geplante Reform der EU-Screening-VO endgültig geschlossen werden. Ebenso dürfte die

84 Siehe dazu den Überblick zum Bereich des „Inward investment screening" durch das Department of Enterprise, Trade and Employment, abrufbar unter: https://enterprise.gov.ie/en/what-we-do/trade-investment/investment-screening/#:~:text=Ireland%20is%20introducing%20an%20inward,security%20and%20public%20order%20criteria. (letzter Abruf am 15.01.25).

85 *OECD*, Framework for Screening Foreign Direct Investment into the EU – Assessing effectiveness and efficiency, 2022, S. 52 ff.

86 So bspw. Belgien, Bulgarien, Italien, Malta, Slowenien und andere.

87 So bspw. Frankreich, Spanien, Slowakei und auch Deutschland. Dabei gilt bspw. für Spanien eine Erwerbsschwelle von 10 % für alle Sektoren. Siehe *OECD* (Fn. 85), S. 142.

88 Siehe dazu den Länderüberblick in *OECD* (Fn. 85), S. 84 ff.

verpflichtende Berücksichtigung kritischer Infrastrukturen dazu führen, dass diese in allen mitgliedstaatlichen Kontrollregimen – wo nicht ohnehin bereits – eine Rolle spielen. Es bleiben damit jedoch in jedem Fall Unterschiede im Hinblick auf die Prüfungsintensität, die mitunter auch politisch motiviert sein können.

D. Notwendige Anpassungen des Investitionskontrollrechts zum effektiveren Schutz maritimer Infrastrukturen

Aus dem Vorstehenden ergeben sich Fragen im Hinblick auf ggf. notwendige Anpassungen für einen effektiveren Schutz maritimer Infrastrukturen durch die Investitionskontrolle, wobei allerdings nicht das deutsche Kontrollregime, sondern die europäische Dimension in den Blick zu nehmen ist. Bereits nach derzeitigem Stand der EU-Screening-VO werden einzelne Unionsprojekte und -programme benannt (Art. 8 Abs. 3), die ein europäisches Sicherheitsinteresse betreffen. Gleichwohl bleiben die Prüfungsmöglichkeiten der Kommission bislang – und dies auch bei unveränderter Annahme des neuen Reformvorschlags – beschränkt.

Die Fusionskontrollverordnung[89] knüpft die Zweistufigkeit der Prüfung an eine „gemeinschaftsweite Bedeutung" von Zusammenschlüssen (Art. 1). Die Investitionskontrolle vollzieht diese Trennung bislang nicht. Dies mag mit der Sensibilität insbesondere von kritischen Infrastrukturen zusammenhängen. Gleichwohl zeigt bspw. das Beihilfenrecht, dass auch in Bereichen, in denen vorrangig die Mitgliedstaaten eine aktive Rolle einnehmen, eine unionsrechtliche Genehmigungspflicht bestehen kann (Art. 108 AEUV). Das Beihilfenrecht erfasst dabei gerade auch staatliche Investitionen in Infrastruktureinrichtungen.[90]

Eine mit dem Beihilfenrecht vergleichbare Genehmigungspflicht wäre theoretisch auch für die Zulassung ausländischer Direktinvestitionen in mitgliedstaatliche maritime Infrastrukturen als einem Bereich von unionsweiter Bedeutung denkbar. So könnte die Kommission die Interessen der übrigen Mitgliedstaaten bündeln und im Sinne eines europäischen Sicherheitsinteresses eine von einem Mitgliedstaat geplante Genehmigungsent-

89 Verordnung (EG) Nr. 139/2004 des Rates vom 20. Januar 2004 über die Kontrolle von Unternehmenszusammenschlüssen, ABl. L 24 vom 29.1.2004, S. 1–22.

90 Siehe dazu bspw. *Schrotz*, Investitionen in Infrastruktureinrichtungen, in: Bungenberg, Heinrich (Hrsg.), Beihilfenrecht, 2. Auflage 2024, S. 270.

scheidung überprüfen und im Wege einer eigenen Vereinbarkeitsprüfung steuern. Diese könnte wiederum gerichtlich überprüft werden, was eine Steigerung des effektiven Rechtsschutzes gegenüber dem derzeitigen Stand bedeuten würde.[91] Ob gerade diejenigen Mitgliedstaaten, die über europaweit bedeutsame maritime Infrastrukturen verfügen, einer entsprechenden Genehmigungspflicht zustimmen würden, ist allerdings sehr zweifelhaft. Überdies würde sich bei einer generellen Genehmigungspflicht die Frage der Verhältnismäßigkeit stellen.

Außerhalb einer zentralen Prüfungskompetenz könnten die nationalen Kontrollregime stärker harmonisiert werden, um einen einheitlicheren Schutz maritimer Infrastrukturen zu erreichen. Dazu würde eine stärkere Konkretisierung der zu berücksichtigen Fallgruppen, aber auch der Meldeschwellen gehören. Hierfür könnten die Notwendigkeit der Sicherstellung eines *level playing field* im Binnenmarkt sprechen. In der gegenwärtigen Situation könnte es zu einem *race to the bottom* kommen, da sich durch eine weniger strenge Kontrolle die eigene Position als Investitionsstandort fördern lässt. Das muss freilich nicht per se negativ sein, da regulativer Systemwettbewerb durchaus Bestandteil des Binnenmarktkonzeptes ist.[92]

Überhaupt keine Beachtung hat bislang auf EU-Ebene die Frage gefunden, inwieweit Möglichkeiten einer nachträglichen Kontrolle eine Vorabprüfung begrenzen und die Unternehmen dadurch entlasten könnten. Aufgrund der Tatsache, dass bei aller Sicherheitsrelevanz die EU grds. auf ausländische Investitionen angewiesen ist, wäre dies zumindest erwägenswert. Hierdurch könnten Effektivität und Effizienz womöglich in ein besseres Verhältnis gebracht werden.

E. Ausblick

In den letzten ca. 20 Jahren hat sich in vielen Staaten, insbesondere auch in den Mitgliedstaaten der Europäischen Union sowie auf Ebene der EU selbst ein komplexes Investitionskontrollrecht herausgebildet. Dieses hat bedeutende Wurzeln im Bereich von Sicherheitsinteressen, gerade mit Bezug auf maritime Infrastrukturen. Das heutige Investitionskontrollrecht findet dem Grunde nach vollumfänglich Anwendung auf Investitionen aus Drittstaa-

91 Siehe dazu *Bungenberg, Reinhold* (Fn. 20), Rn. 207.

92 *Tietje*, in: Grabitz/Hilf/Nettesheim, Das Recht der EU, 80. EL August 2023, Art. 114 AEUV Rn. 25 ff.

ten bzw. von Drittstaatsunternehmen in maritime Infrastruktur. Soweit es diesbezüglich zur Anwendung des Investitionskontrollrechts kommt, sind die entsprechenden Verfahren regelmäßig mit hoher politischer Sensibilität und öffentlicher Aufmerksamkeit verbunden. Schutzlücken bestehen hier womöglich – von einzelnen Mitgliedstaaten abgesehen – eher innerhalb der behördlichen Praxis.

Allerdings sollte bei der Diskussion um die Anwendung des Investitionskontrollrechts im Bereich maritimer Infrastruktur auch berücksichtigt werden, dass Staaten gewisse, sicherlich nicht umfassende, aber immerhin bestehende völkerrechtliche Pflichten zur Sicherung der entsprechenden Infrastruktureinrichtungen haben. Das Investitionskontrollrecht ist dabei nur eines von mehreren Instrumenten, die eingesetzt werden können. Innerhalb staatlicher Regelungshoheit kann auch mit anderen Mitteln, in letzter Konsequenz durch Treuhand und gegebenenfalls sogar Verstaatlichung die entsprechende Infrastruktur im öffentlichen Interesse gesichert werden. Aktuelle Beispiele aus dem Energiesektor zeigen dies. Insofern bleibt das Investitionskontrollrecht eines unter mehreren Optionen zur Gewährleistung maritimer Sicherheit, dessen Effektivität gegenüber der regulatorischen Mehrbelastung abgewogen werden muss.

Maritime Cyberresilienz – Standardisierung und Implementierung von Cybersicherheit in internationalisierten Infrastrukturen am Beispiel von Seehäfen

Katharina Reiling[*]

Der Beitrag untersucht am Beispiel von Seehäfen, wie in internationalisierten Regelungsbereichen Cyberresilienz sichergestellt werden kann. Die Kernthese lautet, dass sich die Herstellung von Cyberresilienz in besonderem Maße als ein Orchestrierungsproblem erweist, was sich im regulatorischen Zugriff widerspiegelt. Nachdem die tatsächlichen Herausforderungen der Cyberresilienz von Seehäfen illustriert werden, wird gezeigt, dass sich ein Regulierungsansatz herausgebildet hat, der sich aus völkerrechtlichen, selbstregulativen und regional-staatlichen Ansätzen zusammensetzt, die insgesamt die hafenbezogene Cyberresilienz abzusichern versuchen. Die einzelnen Regelungsbemühungen sind indes noch wenig durchdacht und unabgestimmt. Abschließend werden daher auf der Grundlage der Untersuchungserkenntnisse Perspektiven einer internationalisierten Cyberresilienz aufgezeigt, indem ausgehend von dem Konzept der Orchestrierung zentrale Rechtsinstrumente und -prinzipien benannt werden, um diese zu stärken und abzusichern.

A. Einführung

I. Cybersicherheitsrecht als entgrenztes Sicherheitsrecht

Der zunehmende Einsatz digitaler Technologien – bezeichnet als digitale Transformation[1] – eröffnet neue Möglichkeiten, erhöht aber auch die Vulnerabilität von Gesellschaft, Wirtschaft und Staat. Die Einsicht in die Zweischneidigkeit dieser Entwicklung hat zur Herausbildung neuer Rechts-

* Die Verfasserin ist Inhaberin des Lehrstuhls für Öffentliches Recht, insb. Verwaltungsrecht, internationales Recht und maritimes Recht an der UniversitätKonstanz.

1 Siehe nur *Cole*, Transformation, 2018; *Schwab,* Digitale Revolution, 2016; *Miebach*, Digitale Transformation, 2020.

gebiete geführt.[2] Während das Datenschutzrecht die negativen Folgen der Digitalisierung für die informationelle Selbstbestimmung adressiert,[3] widmet sich das Cybersicherheitsrecht, auch Informationssicherheits- oder IT-Sicherheitsrecht genannt, dem Schutz vor Cyberrisiken mittels einer Stärkung der Resilienz von IT-Systemen (Cyberresilienz).[4] Das Datenschutzrecht nimmt demnach – subjektivbezogen – den Einzelnen in den Blick, das Cybersicherheitsrecht widmet sich – objektivbezogen – der Funktionsfähigkeit informationsverarbeitender Systeme und ihrer Komponenten.

Im Vergleich mit dem vertrauten Sicherheitsrecht, das auf die Abwehr von Gefahren zielt, zeichnet sich das Cybersicherheitsrecht, dessen Anliegen die Stärkung von Cyberresilienz bildet, durch drei, miteinander zusammenhängende Bewegungen der Entdifferenzierung aus:[5]

– Ein erstes Moment der Entdifferenzierung liegt darin, dass Resilienz bedeutet, Sicherheit nicht ausgehend von konkreten Gefahrenlagen zu denken. Die Grundannahme bildet stattdessen eine generelle Vulnerabilität von IT-Systemen. Denn gerade ihre Verdichtung und Verflechtung gilt als Quelle gesteigerter Verwundbarkeit.[6] Die erste Bewegung der Entdifferenzierung zeigt sich mithin am Fehlen einer klaren Zuordnung von Cyberbedrohungslagen zu bestimmten Akteuren. Deutlich wird dieser Verlust an eindeutigen Zurechnungszusammenhängen auch daran, dass unter den Bedingungen einer umfassenden Vernetzung von IT-Systemen die herkömmliche – an die Schadensursache anknüpfende – Unterscheidung zwischen dem Schutz vor betriebsbedingten Gefahren (safety) und dem Schutz vor absichtlich erzeugten Gefahren durch Externe (security) unscharf wird. Der enge Zusammenhang zwischen safety und security

2 Allgemein zu den rechtlichen Konsequenzen der digitalen Transformation *Hoffmann-Riem*, Recht im Sog der digitalen Transformation, 2022.

3 Siehe etwa *Veit*, Einheit und Vielfalt im europäischen Datenschutzrecht, 2023; *Marsch*, Das europäische Datenschutzgrundrecht, 2018; *Schneider*, Regulierte Selbstregulierung im europäischen Datenschutzrecht, 2022.

4 Monographisch *Wischmeyer*, Informationssicherheit, 2023; *Freimuth*, Gewährleistung der IT-Sicherheit kritischer Infrastrukturen, 2018; *Leuschner*, Sicherheit als Grundsatz, 2018; *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, 2019. Aus der Handbuch-Literatur *Kipker*, Cybersecurity, 2. Aufl. 2023.

5 Resilienz als Reaktion auf und Konzept für Entgrenzungen verstanden, Resilienz etwa als „Grundlage einer vernetzten und integrativen Sicherheitspolitik" bezeichnend *Barczak*, Der nervöse Staat, 2. Aufl. 2023, S. 607; aus der Soziologie zudem *Kaufmann*, in: Endreß/Maurer, Resilienz im Sozialen, 2015, S. 295.

6 *Kaufmann*, a.a.O., S. 296; *Bartsch, Frey*, Cyberstrategien für Unternehmen und Behörden, 2017, S. 57 f.

im Cybersicherheitskonzept zeigt sich etwa daran, dass ein wesentliches Anliegen des IT-Sicherheitsrechts darin besteht, Schutzmaßnahmen (im Sinne der safety) gegen Angriffe auf die Verfügbarkeit und Integrität (im Sinne der security) zu schützen.[7] Aufgrund dieser Perspektivenverschiebung – im Vergleich zum gewohnten polizeirechtlichen Verständnis – wird das Cybersicherheitsrecht auch als „neues" bzw. „modernes" Sicherheitsrecht bezeichnet oder dem Gebiet des Risikorechts zugeordnet.[8] Andere grenzen Fragen der rechtlichen Steuerung von Resilienz hingegen scharf von der Risikovorsorge ab, da Resilienz erfordere, dass Prävention und Vorsorge in zeitlicher Hinsicht noch deutlich vorverlagert werde und die gesamtgesellschaftlichen Folgen in den Blick nehme.[9] Dieses entgrenzende Moment von Resilienz verdeutlicht die weite Definition maritimer Cyberrisiken durch die Internationale Seeschifffahrts-Organisation: „*Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.*"[10]

- Eine zweite Bewegung der Entdifferenzierung betrifft die organisatorischen Folgen dieser Aufgabenstellung. Sind Ausgangspunkt Effekte miteinander vernetzter IT-Systemen, bildet die Aufgabe der Stärkung von Cyberresilienz ein Gemeinschaftsanliegen. Das gemeinsame Moment besteht in einem regelmäßigen Austausch kritischer Informationen über Cyberaktivitäten und -angriffe sowie eine wechselseitige Investition in Cyber-Kompetenzen über Akteure, Ebenen und Branchen hinweg.[11]
- Als weitere Bewegung der Entdifferenzierung tritt die internationale Dimension der Cybersicherheit hinzu.[12] IT-Systeme sind in Teilbereichen globalisiert. In dem Maße, in dem lokale Bedrohungslagen aufgrund der

7 *Fischer, Messerschmidt*, Ohne Security keine Safety in Kritischen Infrastrukturen — Begriffliche Trennung und Zusammenführung, AG KRITIS, Mai 2020, S. 3 f. (https://ag.kritis.info/2020/04/03/ohne-security-keine-safety-in-kritischen-infrastrukturen-begriffliche-trennung-und-zusammenfuehrung/), abgerufen am 17.2.2025.

8 *Freimuth*, Gewährleistung der IT-Sicherheit kritischer Infrastrukturen, S. 114 ff., 425; *Wischmeyer*, a.a.O., S. 75 ff.

9 Insb. *Rixen*, in: Die Verwaltung 55 (2022), 345, 349; ausführlich ders., in: VVDStRL 80 (2021), 37, 46 ff.

10 *IMO*, Guidelines on Maritime Cyber Risk Management, 7.6.2022, MSC-FAL.1/Circ.3/Rev.2, unter 1.1.

11 *Schwab*, Die Zukunft der Vierten Industriellen Revolution, 2019, S. 32.

12 *Hoffmann-Riem*, Recht im Sog der digitalen Transformation. 2022, S. 214 ff.

Vernetzung der IT-Systeme auch globalen Ursprungs sein können, wird die Sicherstellung von Resilienz ein grenzüberschreitendes Unterfangen.

Die zuletzt genannte internationale Dimension der Cybersicherheit wird bislang primär völkerrechtlich gedeutet. In der völkerrechtswissenschaftlichen Forschung zur Cybersicherheit widmet man sich im Kern der Frage, ob und unter welchen Umständen eine die IT-Sicherheit eines anderen Landes beeinträchtigende Handlung eines Staates völkerrechtlich relevant ist, v.a. ob dadurch das Gewaltverbot (Art. 2 Nr. 4 UN-Charta) verletzt ist.[13] Im Falle eines bewaffneten Angriffs gegen ein Mitglied der Vereinten Nationen statuiert Art. 51 UN-Charta eine Ausnahme vom Gewaltverbot: Es besteht ein Recht zur Selbstverteidigung bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat. Sicherheit im „Cyberraum" geht aber über Möglichkeiten der Selbstverteidigung gegen und Staatenverantwortlichkeit für Cyberattacken hinaus. Ist, wie gesehen, Cyberresilienz eine grenzüberschreitende Herausforderung, dann stellen sich notwendigerweise auch Fragen eines internationalen Verwaltungsrechts. Das internationale Verwaltungsrecht bildet eine Forschungsperspektive, die die Folgen einer die staatlichen Grenzen überschreitenden Erfüllung von Verwaltungsaufgaben für gängige verwaltungsrechtliche Kategorien untersucht, etwa für administrative Instrumente, Verwaltungsorganisation und Metaregeln für Verwaltungshandeln.[14]

II. Maritime Cyberresilienz als Orchestrierungsproblem

Der Beitrag widmet sich vor diesem Hintergrund der Cyberresilienz aus der Perspektive des internationalen Verwaltungsrechts und untersucht diese

13 Aus der deutschen Literatur *Walter*, in: JZ 2015, 685 ff.; *Lahmann*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2021, § 6 Rn. 15 ff.; *Schmahl*, in: AVR 47 (2009), 284 ff.; *Krieger*, in: AVR 50 (2012), 1 ff.; aus der internationalen Literatur *Finnemore*, *Hollis*, in: Beyond Naming and Shaming: Accusations and International Law in Cybersecurity, European Journal of International Law, Volume 31, Issue 3, August 2020, Pages 969–1003; *Schmitt*, *Watts*, in: Beyond State-Centrism: International Law and Non-state Actors in Cyberspace, Journal of Conflict and Security Law, Volume 21, Issue 3, Winter 2016, Pages 595–611; weiter aber *Fidler*, Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection, 16 Geo. J. Int'l Aff. 8 (2015).

14 *Reiling*, Seeverwaltungsrecht, 2024.

am Beispiel von Seehäfen.[15] Die Wahl ist auf Seehäfen gefallen, da gerade die Regulierung maritimer Cyberresilienz durch die ausgeprägte Globalität des maritimen Bereichs erschwert wird.[16] Innerhalb des maritimen Kontexts nehmen Seehäfen eine hervorgehobene Position ein, denn trotz der örtlichen Radizierung dieser Infrastruktur vermischen sich in den smarten Netzwerken die Grenzen zwischen national und international sowie, typisch für internationalisierte Arenen, zwischen privat und öffentlich, zwischen Recht und Nicht-Recht.

Anhand von Seehäfen wird gezeigt, dass die Sicherstellung von Cyberresilienz in besonderem Maße ein Orchestrierungsproblem darstellt, was sich damit erklären lässt, dass das Cybersicherheitsrecht auch weltweit vernetzte Systeme zum Gegenstand hat.

Der Begriff der Orchestrierung stammt ursprünglich aus dem Bereich der Musik.[17] Er wurde von anderen Disziplinen aufgegriffen. In der IT steht Orchestrierung etwa für die Komposition mehrerer Einzeldienste zu einem Gesamtservice.[18] Hier wird in Anlehnung an die Global Governance-Forschung[19] mit Orchestrierung die Frage der Lenkung internationalisierter Regelungsstrukturen ohne zentralen Akteur angesprochen.[20] Das analytische Konzept der Orchestrierung reagiert damit auf die übermäßige Vervielfachung und Fragmentierung transnationaler Governance-Systeme,

15 Über den Hafenbereich hinausgehende Beobachtungen bei *Stamme*, in: KlimR 2024, 16 ff.

16 *Karim*, in: Marine Policy 143, 2022, 105138, unter 4.

17 *Von Ahn Carse*, History of Orchestration, 1964.

18 *Misra*, *Cook*, in: Computation orchestration: A basis for wide-area computing. Software & Systems Modeling, 6(1), 2007, 83-110.

19 Grdl. *Abbott, Snidal,* in: Strengthening international regulation through transmittal new governance: overcoming the orchestration deficit, Vanderbilt Journal of Transnational Law, 2009, *42(2),* 501-578; *Abbott*, *Genschel, Snidal, Zangl,* Orchestration: Global governance through intermediaries, Spectrum of International Institutions, 2021 (pp. 140-170), Routledge; *Abbott*, *Genschel*, *Snidal, Zangl*, Two logics of indirect governance: Delegation and orchestration, British Journal of Political Science, 2016, 46(4), 719-729; *Henriksen*, *Ponte*, in: Public orchestration, social networks, and transnational environmental governance: Lessons from the aviation industry, Regulation & governance, 2018, 12(1), 23-45.

20 „Orchestration includes a wide range of directive and faciliative measures designed to convene, empower, support and steer public and private actors engaged in regulatory activities", *Abbott*, & *Snidal, Duncan*., Strengthening international regulation through transmittal new governance: overcoming the orchestration deficit, Vanderbilt Journal of Transnational Law, 2009, *42(2),* 501, 509 f.

auch im Cyberspace.[21] Der Beitrag widmet sich dem aus einer rechtswissenschaftlichen Sicht. Die maritime Cyberresilienz oder digitale Hafengovernance[22] stellt danach ein Themenfeld dar, anhand dessen es gilt, rechtliche Möglichkeiten und Strategien der Orchestrierung zu erforschen.

Der Beitrag geht dazu in drei Schritten vor. Nachdem die tatsächlichen Herausforderungen der Cyberresilienz von Seehäfen illustriert werden (B.), wird gezeigt, dass sich im Sinne des internationalen Verwaltungsrechts ein Regulierungsansatz herausgebildet hat, der sich aus völkerrechtlichen, selbstregulativen und regional-staatlichen Ansätzen zusammensetzt, die insgesamt die hafenbezogene Cyberresilienz abzusichern versuchen (C.). Die einzelnen Regelungsbemühungen sind indes noch wenig durchdacht[23] und unabgestimmt. Abschließend werden daher auf der Grundlage der Untersuchungserkenntnisse Perspektiven einer internationalisierten Cyberresilienz aufgezeigt, indem ausgehend von dem Konzept der Orchestrierung zentrale Rechtsinstrumente und -prinzipien benannt werden, um diese zu stärken und abzusichern (D.).

B. Cybersicherheit in Seehäfen: ein tatsächlicher Befund

Der Begriff Cyberresilienz beschreibt die Fähigkeit eines Systems, einer Organisation oder eines Netzwerks, nach einem Cyberangriffen in den status quo ante oder einen gleichwertigen Zustand zurückzukehren bzw. sich entsprechend zu transformieren.[24] Im maritimen Bereich wird Cyberresilienz auf den drei Ebenen Schiff, Meer und Hafen virulent.[25] Der Blick auf die hafenseitige Cybersicherheit ist dabei aus mehreren Gründen loh-

21 Aus der Global Governance-Forschung zum Cyberspace *Weiss*, *Jankauskas*, Securing cyberspace: How states design governance arrangements, Governance, 2009, *32*(2), 259-275; zur Bedeutung von Orchestrierung für das Klimarecht *Franzius*, in: KlimaR 2022, S. 2, 3 f.

22 Zur Regulierung von Häfen als Governance-Problem *Brooks, Cullinane*, Introduction, Kap. 1, in: dies., Devolution, Port Governance and Port Performance, 2007, S. 3 ff.

23 Zur NIS-2-Richtlinie *ESPO*, Position of the European Sea Ports Organisation on the proposal for a Directive on measures for high common level of cybersecurity across the Union, 2021 (https://www.espo.be/media/2021.03.10%20Position%20of%20the%20European%20Sea%20Ports%20Organisation%20on%20the%20NIS%202.0%20proposal_1.pdf), S. 2 f, abgerufen am 17.2.2025.

24 *Gassmann, Sutter*, Digitale Transformation gestalten, 2023, S. 95; für die Bundeswehr BT-Drs. 19/6503, S. 1.

25 *Karim*, in: Marine Policy 143, 2022, 105138, unter 3.

nenswert. Seehäfen sind einerseits ein Paradebeispiel für eine besonders digitalisierte (II., III.) und zugleich schutzwürdige kritische Infrastruktur (IV.), auf der anderen Seite weisen Seehäfen wegen ihrer transnationalen, nur teils rechtlich basierten Organisationsstruktur (I.) Besonderheiten auf, die eine Stärkung ihrer Resilienz erschweren. Diese Charakteristika werden zunächst erläutert, bevor die spezifischen Cyberrisiken in Seehäfen dargestellt werden (V.).

I. Seehäfen als transnationale Netzwerke

Ein Seehafen stellt räumlich ein Gebiet dar, dessen Anlagen und Befestigungen dem gewerblichen Seeverkehr dienen (Art. 3 Abs. 1 Richtlinie 2005/65/EG). Auch organisatorisch lässt sich ein Hafen nicht als ein Akteur im Sinne einer geschlossenen Einheit konzipieren.[26] Strukturell handelt es sich bei ihm vielmehr um eine Verflechtung vielfältiger Akteure mit Bezug zur Seefahrt, die jeweils eigene Interessen verfolgen. Zu den Akteuren gehören insbesondere Terminalbetreiber, Reeder, Spediteure, Telematikanbieter, Packingfirmen, Hafen- und Zollbehörden. Man spricht in der Praxis wegen dieser Vernetzung auch vom Hafenökosystem (Port Ecosystem).[27] Dieses Netzwerk weist, auch wenn seine Infrastruktur ortsfest ist, starke ausländische Bezüge auf. Intern zeigt sich das daran, dass viele der Beteiligten Bezüge zu unterschiedlichen Nationen aufweisen, man denke an Terminalbetreiber und / oder Reedereien, und extern daran, dass das Management des Hafens oft und auf vielfältige Weise selbst im Ausland tätig wird.[28] Das Zusammenwirken dieser Akteure basiert im Unterschied zu anderen Industrien nicht maßgeblich auf vertraglicher Grundlage – man denke an die Vertragsnetze in der Automobilbranche –, sondern ist auch faktisch-informell ausgestaltet. Das Hafennetzwerk stellt sich insofern als heterogen dar, als neben Multiplayern wie großen Reedereien auch kleinere und mittelständische Unternehmen teilnehmen, im Durchschnitt zwischen 50 bis 200 Unternehmen, in den größten Häfen bis zu 900.

---

26 *Trimble, Monken* and *Sand*, "A framework for cybersecurity assessments of critical port infrastructure," 2017 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, USA, 2017, pp. 1-7.

27 *ESPO*, Trends in EU Ports´ Governance, 2022.

28 *Polemi*, Port Cybersecurity, 2017, S. 3; *Dooms, van der Kugt, Parola, Satta, Song*, in: Maritime Policy & Management 45, 2019, 585 ff.

Das Hafennetzwerk weist zudem durch die Einbindung sowohl öffentlicher als auch privater Akteure hybride Züge auf. Beim Landlord-Hafen, dem inzwischen häufigsten Hafenmodell,[29] scheint die Aufgabenteilung zwischen öffentlicher Hand und Privatwirtschaft klar zu sein: Die zuerst Genannte agiert als Eigentümerin der Hafenflächen und der Infrastruktur, während die dort geleisteten Hafendienste, etwa der Güterumschlag, von privaten Unternehmen durchgeführt werden. Das herkömmliche Landlord-Modell ist seit den 1990er Jahren insbesondere in Europa durch auf Dezentralisierung und (Teil-)Privatisierung der Häfen ausgerichtete Reformen unter Beschuss geraten.[30] Insbesondere wurde die Verwaltung der Häfen reorganisiert, indem z.B. privatrechtlich organisierte Stellen geschaffen wurden, um die Effizienz des Hafenbetriebs zu steigern und im Hafenwettbewerb mithalten zu können. Für andere Häfen wie den Hamburger blieb man bei einer öffentlich-rechtlichen Organisationsform.[31] Für die Bremer Häfen, die die Hafengebiete Bremen und Bremerhaven umfassen, ist man einen Mittelweg gegangen, wie die Gründung der privatrechtlich organisierten Hafenmanagementgesellschaft bremenports GmbH & Co. KG im Jahre 2002 verdeutlicht.[32] Bremenports verwaltet als „Hausmeister des Hafens"[33] einen Großteil der Hafeninfrastruktur, nimmt die Hafengebühren ein, vermietet Terminals, betreibt Marketing und entwickelt die Bremer Häfen weiter. Mehrere hoheitliche Aufgaben wie die Hafensicherheit, Schiffslenkung und Zulassung von Serviceanbieter wurden hingegen nicht an bremenports übergeben, sondern sind maßgeblich beim Hansestadt Bremisches Hafenamt (HBH) sowie der senatorischen Behörde (Senatorin für Wirtschaft, Häfen und Transformation) angesiedelt. Angesichts dieser diversen Organisationsformen wird auf EU-Ebene das sog. Leitungsorgan des Hafens weit definiert als „eine öffentliche oder private Stelle, die gemäß den nationalen Rechtsvorschriften oder Instrumenten die Aufgabe hat oder

29 *World Bank*, Port Reform Toolkit, S. 83.

30 Zum Wandel von Hafenorganisationen *Brooks*: The Governance Structure of Ports, in: Review of Network Economics 3(2), 2004, S. 168-183.

31 § 2 Abs. 1 Gesetz über die Hamburg Port Authority (HPAG) vom 29. Juni 2005 (HmbGVBl. S. 256).

32 Diese wurde maßgeblich durch die prekäre Bremer Haushaltslage angestoßen Bremische Bürgerschaft-Drs. 15/1203, S. 41.

33 Siehe die Übersicht bei *Moros-Daza, Amaya-Mier, Paternina-Arboleda*, in: Transportation Research 133 (2020), 27 ff.

dazu ermächtigt ist, die Hafeninfrastrukturen auf lokaler Ebene – gegebenenfalls neben anderen Tätigkeiten – zu verwalten und zu betreiben".[34]

II. Smart Ports

Die digitale Transformation von Seehäfen ist weiter fortgeschritten als die auf Schiffsseite, was auch die Angriffsfläche von Hafenanlagen für Cyberattacken vergrößert. Diese Entwicklung beschreibt das Konzept „Smart Ports". Das Konzept ist ein Produkt der Industrie 4.0,[35] die die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologie beschreibt. Ein Smart Port ist ein Hafen, der mit neuen Technologielösungen, etwa einem hafenweiten Echtzeit-Ortungssystem, intelligenten Lösungen für die Hafensicherheit wie Drohnen, verbesserten Track-and-Trace-Systemen, Radiofrequenz-Identifikation, GPS-Systemen, dreidimensionalen Scannern und autonomen Robotern ausgestattet ist.[36] Häfen wie Rotterdam oder Hamburg glänzen durch die Automatisierung ihrer gesamten Container-Routing-Prozesse. Dahinter steht der Wunsch nach einer Optimierung von Lieferketten und der Förderung von Effizienz. Die Herausbildung von Smart Ports wird daher auch politisch gefördert,[37] etwa in der EU durch die Einführung eines European Maritime Single Window Environment (EMSWe),[38] welches das Verkehrsmanagement zwischen Schiff und Hafen verbessert, sowie durch staatliche und lokale Initiativen. Auf Bundesebene bildet eine solche Initiative der Nationale Masterplan Maritime Technologien unter

34 Verordnung 2017/352 vom 15. Februar 2017 zur Schaffung eines Rahmens für die Erbringung von Hafendiensten und zur Festlegung von gemeinsamen Bestimmungen für die finanzielle Transparenz der Häfen.

35 *De la Peña Zarzuelo* et al., in: Journal of Industrial Information Integration 20 (2020) 100173.

36 *Douaioui, Fri, Mabrouki, Semma*, Smart port: Design and perspectives, 4th International Conference on Logistics Operations Management (GOL), 2018, S. 1 ff.; *Li* et al., in: Transportation Research Part E: Logistics and Transportation Review 174, 2023, 103098.

37 *ESPO*, Position of the European Sea Ports Organisation on a Strategy for Sustainable and Smart Mobility, 22 September 2020, S. 4 https://www.espo.be/media/2020.09.29%20Transport%20Strategy%20ESPO%20Position%20Paper.pdf, abgerufen am 17.2.2025.

38 Verordnung (EU) 2019/1239 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Einrichtung eines europäischen Umfelds zentraler Meldeportale für den Seeverkehr und zur Aufhebung der Richtlinie 2010/65/EU.

dem Dach der Maritimen Agenda 2025.[39] In Bremen hat der Senat 2023 die sog. SMART-Ports-Strategie beschlossen, die den digitalen Austausch zwischen Hafenakteuren erleichtern soll.[40]

III. Hafeninformationssystem (Port Community System)

Die elektronische Kommunikation zwischen den Akteuren des Hafennetzwerks erfolgt über zentrale Plattformen, v.a. die Port Community Systems. In Bremen heißt das zentrale Hafeninformationssystem beispielsweise "BrePos" (Bremen Port Operating System). Dieses dient auch vielen hafennahen Bundes- und Landesbehörden und Firmen wie Zoll, Wasserschutzpolizei, BG Verkehr oder Schleppergesellschaften als zentrales Informationsinstrument, da es ihnen etwa Zugriff auf den Verkehrsplan, Brückenbewegungen, geplante Schleusungen oder Schiffsstammdaten und Schiffsbewegungen erlaubt.[41] Die Digitalisierung des Hafennetzwerks bedeutet mithin, dass Häfen zu zentralen Kommunikationsverbünden (digitale Plattformen, one-to-many-Plattformen) werden. Im Rahmen dieser digitalen Plattformen werden Daten für Verkehrskontrolle und Logistik, offizielle Deklarationen gegenüber Behörden oder anderen Akteuren der Hafen- und Cargo-Community, Unternehmensdaten, Daten für den Betrieb von Terminals sowie Daten zur Herstellung von Sicherheit generiert, analysiert, gespeichert und weitergegeben.[42]

IV. Kritikalität von Hafeninfrastrukturen

Seehäfen sind Schnittpunkte internationaler Güterströme. Die logistischen und finanziellen Folgen von Cyberattacken auf internationale Häfen –

39 Siehe: https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/nationaler-masterplan-maritime-technologien-maritime-branche-flyer.html, abgerufen am 17.2.2025.

40 Siehe https://www.senatspressestelle.bremen.de/pressemitteilungen/senat-beschliesst-smart-ports-strategie-421878, abgerufen am 17.2.2025.

41 Verordnung über das Verfahren zum Anschluss an das Hafeninformationssystem Bremen Port Operations System (Hafeninformationsverordnung - HaInfoV), Brem. GBl. S. 339.

42 *Borchert, Rühlig, Weber*, in: Toxische Türöffner – Smart Ports als geoökonomisches Handlungsfeld, SIRIUS – Zeitschrift für Strategische Analysen, vol. 7, no. 2, 2023, 150 (153).

Schleusen verwehren ihren Dienst. Schiffe, Lkw und Züge können nicht mehr be- und entladen werden etc. Sie sind damit in besonderem Maße destruktiv und können die gesamte Lieferkette und damit die Wirtschaft eines Landes massiv stören. Den Schaden, den Lieferkettenangriffe anrichten können, verdeutlicht das Beispiel einer Attacke auf den Weltmarktführer im Containersektor: Maersk, der im Jahr 2017 Opfer des NotPetya-Virus wurde. Infolge des Angriffs wurden zwölf Hafenterminals, die die Reederei weltweit betreibt, stillgelegt; offiziell verzeichnete Maersk Verluste in Höhe von 300 Millionen US-Dollar.[43] Nach Anhang 7 der KRITIS-VO können daher etwa Umschlaganlagen in See- und Binnenhäfen, Hafenleitungsorgane und Hafeninformationssystem bei Überschreiten der Schwellenwerte kritische Infrastrukturen darstellen, für die die Cybersicherheitsanforderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) gelten.

V. Cyberrisiken für Seehäfen

Cybersicherheit zielt im Kern darauf, die Vertraulichkeit (confidentiality), Integrität (integrity) und Verfügbarkeit (availability) von Informationen zu schützen (sog. CIA-Triade).[44] Im deutschen Recht wird diese Zielsetzung in § 2 Abs. 2 S. 4 BSIG legaldefiniert. Die Risiken für die so konkretisierte Cybersicherheit sind vielfältig.[45] Im Hafensektor lassen sich die Risiken im Kern drei Angriffsszenarien zuordnen:[46]

– *Denial of Service*: Eine große Gefahr für die Verfügbarkeit von Informationen im Hafenkontext geht von Ransomware aus, eine Art von Malware. Bei dieser Angriffsmethode verweigert ein Computer gegenüber berechtigten Nutzern den Dienst, nachdem der Angreifer auf dem Zielrechner eine Schadstoffsoftware eingeschleust hat. An den eigentlichen

43 Siehe https://www.stormshield.com/de/news/cybersicherheit-im-seeverkehr-und-hafeninfrastrukturen-wie-lassen-sich-betriebliche-modernitaet-und-cybersicherheit-in-einklang-bringen/, abgerufen am 17.2.2025.

44 *Hornung, Schallbruch*, IT-Sicherheitsrecht, 2021, § 1 Rn. 13.

45 Siehe https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emergingthreats?&at_campaign=20234Digital&at_medium=Google_Ads&at_platform=Search&at_crea-tion=RSA&at_goal=TR_G&at_audience=cyber%20security%20threats&at_topic=Cybersecurity&at_location=DE&gclid=EAIaIQobChMI__-9s-nNggMVwheiAx2tGAzHEAAYAiAAEgIy__D_BwE, abgerufen am 17.2.2025.

46 *ENISA*, Port Cybersecurity, 2019, S. 27 f.

Angriff schließt sich meist eine Erpressung an. So wurde Ende 2022 der Hafen von Lissabon von der Ransomwaregruppe Lockbit gehackt, die mit der Veröffentlichung aller kopierten Daten drohte, sollte nicht ein Lösegeld über 1,5 Millionen US-Dollar entrichtet werden. Dadurch können im Ernstfall die Abläufe des ganzen Hafens oder Teile zum Erliegen kommen.

- *Spionage*: Die Vertraulichkeit von Informationen wird durch Spionage gefährdet, die im Unterschied zur offen agierenden Ransomeware heimlich erfolgt. Eine Angriffsmethode zur unautorisierten Kenntnisnahme stellen etwa Keylogger dar. Eingesetzt wurden Keylogger 2011 bis 2013 in Antwerpen bei der ersten großen Cyberattacke auf einen Hafen. Eine Bande schmuggelte jahrelang Drogen aus Lateinamerika nach Antwerpen und versteckte die Drogen in Containern verschiedener Unternehmen. Bevor die Eigentümer ihre (legale) Fracht in Antwerpen abholen konnten, stahlen die Täter die Container. Die Entwendung wurde dadurch ermöglicht, dass Hacker die Standorte dieser Container ausspähten, indem sie sich über Spionagesoftware Zugriff auf die Computersysteme des Hafens verschafften. Anders als bei Ransomeware droht bei diesem Szenario nicht der Ausfall von Hafendienstleistungen; adressiert wird hier vielmehr ein anderes Thema, nämlich der Seehafen als Umschlagsplatz für den Drogenhandel. Cyberangriffe sind damit auch ein Mittel der Drogenkriminalität.
- *Politisch motivierte Cyberangriffe*: Eine weitere Unterscheidung ist die nach dem Motiv der Angreifer. Neben den erwähnten finanziell und kriminell motivierten Cyberangriffen nehmen politisch motivierte Cyberattacken auf Häfen zu. Ein größeres Problem als offen motivierte politische Überlastungsangriffe, etwa die DDos-Angriffe (DDoS, Distributed Denial-of-Service) durch die pro-russische Gruppe NoName057(16), stellen dabei staatlich unterstützte, hybride Bedrohungen dar, auch wenn diese nur selten an die Öffentlichkeit gelangen.

Die Gefährdungslage durch Cyberangriffe wird durch die Professionalisierung der Angreiferseite erhöht, gleichzeitig nimmt die Anfälligkeit von Häfen durch ein zu geringes Sicherheitsbewusstsein und die ökonomische Prioritätensetzung zu.[47] Die Wartung oder das Einspielen von Sicherheitsupdates erzwingt sehr oft eine Verlangsamung oder sogar einen kompletten Stillstand der Geschäftsprozesse. Nach dem Cyberangriff auf den Tanklo-

47 *ENISA*, Guidelines on Port Cybersecurity, 2022, S. 17; 2019, S. 30.

gistiker Oiltanking in mehreren westeuropäischen Häfen im Jahr 2022 zeigten Untersuchungen, dass in einigen Fällen nicht alle erforderlichen Softwareaktualisierungen installiert wurden.[48]

Der Verletzlichkeit von Seehäfen durch Cyberangriffe wird zudem durch ihre spezifische Struktur erhöht.[49] Die Einbindung einer Vielzahl heterogener Akteure in das digitalisierte Hafennetzwerk setzt Seehäfen zunehmend Cyberangriffen aus. Die Digitalisierung vervielfältigt potenzielle Eintrittspunkte in Netzwerke und steigert die Porosität zwischen Informations- (IT) und operativen (OT) Systemen. Da sich viele Akteure, darunter auch kleine und mittelständische Unternehmen mit geringen Cybersicherheitskapaziäten, über das Port Community System mit ihren Informationssystemen verbinden, reicht es aus, dass ein Hafenakteur Sicherheitsvorgaben nicht einhält und damit eine Lücke öffnet. Seit Beginn der Pandemie, die die Digitalisierung weiter vorangetrieben hat, sollen Cyberattacken auf Häfen um 400 % zugenommen haben.[50]

Gleichzeitig fehlt den Entscheidungsträgern in Seehäfen oft ein differenziertes Wissen über die kaskadenartigen Auswirkungen von Störungen, was die langfristige Resilienzplanung erschwert. Die komplexen Eigentumsverhältnisse und die nicht stets vertraglich fundierten Governance-Regelungen in den Häfen lähmen den Aufbau von Resilienz potentiell und verschleiern das Verständnis für Verantwortlichkeiten für das Risikomanagement sowie die Umsetzung von Strategien zur Verbesserung der Widerstandsfähigkeit. Die Kontrolle der Cybersicherheit im digitalisierten Hafennetzwerk wird durch die Einbindung einer Vielzahl heterogener Akteure, die mitunter in einem Konkurrenzverhältnis zueinander stehen, erschwert.[51]

C. Regelansätze

Die Regelung der Cyberresilienz von Seehäfen erfolgt durch Maßnahmen auf internationaler (I.) und regional-staatlicher Ebene (III.) sowie im selbstregulativen Bereich (II.). Gezeigt wird, dass die internationalen und

48 Siehe https://www.thb.info/rubriken/maritime-sicherheit/detail/news/hacker-attacken-auf-oelterminals.html, abgerufen am 17.2.2025.

49 MTS Resilience Assessment Guide, 2023, S. 121 https://www.cisa.gov/sites/default/files/2023-03/Marine%20Transportation%20System%20Resilence%20Assessment%20Guide.pdf abgerufen am 17.2.2025; *ENISA*, Port Cybersecurity, 2019, S. 31.

50 Siehe https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent, abgerufen am 17.2.2025.

51 *ENISA*, Port Cybersecurity, 2019, S. 31.

selbstregulativen Ansätze einerseits unzulänglich sind, andererseits vermögen regionale Regelwerke und staatliche Bemühungen dieses Vakuum nicht gänzlich auszufüllen.

I. Völkerrecht

Auf völkerrechtlicher Ebene fallen Fragen rund um den Seeverkehr in die Kompetenz der Internationalen Schifffahrts-Organisation (IMO), die ein Forum der internationalen maritimen Standardsetzung bildet (Art. 1 a), Art. 2 b) IMO-Konvention). Die IMO hat die hafenbezogene Cybersicherheit bislang indes nicht direkt geregelt. 2020 forderte die IMO stattdessen den internationalen Seehafenverband (International Association of Ports and Harbors, IAPH) zum Handeln auf und nahm im Anschluss daran zwei Jahre später durch einen Beschluss ihres Ausschusses für Erleichterungen im Seeverkehr (Facilitation Committee, FAL) hafenseitige Cyberrisiko-Leitlinien der IAPH in die IMO-Leitlinien für das Management von Cyberrisiken im Seeverkehr in Bezug.[52] Danach sollen kraft dynamischer Verweisung in internationalem Soft Law die IAPH-Guidelines in ihrer jeweils relevanten Fassung berücksichtigt werden (Ziffer 4).

Unmittelbar und rechtsverbindlich tätig geworden ist die IMO hinsichtlich physischer Bedrohungslagen für Häfen. Im Rahmen der IMO wurde die SOLAS-Konvention um ein Kapitel XI-2 über „Special Measures to Enhance Maritime Security" und den Internationalen Code für die Gefahrenabwehr auf Schiffen und in Hafenanlagen (International Ship and Port Facility Security Code, ISPS Code) als Anhang ergänzt. Damit wurde zugleich der Anwendungsbereich der SOLAS-Konvention, dem zentralen Schiffssicherheitsabkommen der IMO, zum ersten Mal auf Landungsanlagen ausgeweitet. Der ISPS Code ist durch diese Einbindung in einen völkerrechtlichen Vertrag hinsichtlich seines ersten Teils verbindlich, allein die Umsetzungshilfen im zweiten Teil des Codes (Teil B) haben bewusst Empfehlungscharakter. In der EU wurde der ISPS Code durch die Verordnung 725/2004 und die Richtlinie 2005/65/EG umgesetzt. Inhaltlich verlangt der ISPS Code von den Vertragsstaaten die Vornahme eines Port Facility Security Assessment (PFSA) und die Erstellung eines entsprechenden Plans (Port Facility Security Plan, PFSP). Für die Öffentlichkeit bemerkbar macht sich der ISPS Code v.a. durch die Zunahme von Videoüberwachung

52 MSC-FAL. 1/Circ. 3./Rev.1.

und Zaunanlagen, die den Zugang zu Hafenanlagen erschweren und diese von der Allgemeinheit abschotten. Cyberrisiken werden im ISPS Code nur punktuell und nur im unverbindlichen Teil B angesprochen, der die Hafenanlagen auffordert, „Funk- und Telekommunikationsanlagen, einschließlich Computersysteme und Netzwerke" bei der PFSA zu berücksichtigen (Ziffer 15.3.5 Teil B). In der Umsetzungspraxis hat der punktuelle Bezug auf Cyberrisiken im Teil B des ISPS Codes eine zweitrangige Bedeutung, denn die Behörden („designated authorities", Teil A Ziffer 2.3 ISPS Code) der Vertragsstaaten, die für die nationale Umsetzung des ISPS Codes zuständig sind, überprüfen Cyberrisiken oftmals nicht.

Dieses regulatorische Gefälle zwischen physischen und digitalen Sicherheitsrisiken für Hafenanlagen lässt sich damit erklären, dass die Terroranschläge vom 11. September 2001 die rasche – der ISPS Code wurde 2002 beschlossen und schon 2004 für die SOLAS-Vertragsstaaten verbindlich – Einführung eines völkerrechtlich verbindlichen Regelungswerks erleichterten. Ein solches tragisches Ereignis fehlt im Bereich der Cybersicherheit, so dass es an einer Drucksituation fehlt, die die schwerfällige Rechtssetzung auf internationaler Ebene beschleunigt.

II. Selbstregulativer Bereich

Klassifizierungsgesellschaften gelten als die privaten Standardsetzer im maritimen Bereich. Ihre Rechtssetzungsaktivitäten beziehen sich aber auf die Sicherheit von Schiffen, nicht Seehäfen. In Bezug auf diese hat der internationale Seehafenverband (International Association of Ports and Harbors, IAPH) neben den Cybersecurity Guidelines for Ports and Port Facilities[53], die die einzelnen Seehäfen bzw. ihre Anlagen adressieren, ein Port Community Cyber Security White Paper[54] herausgegeben, das sich spezifisch mit dem systemischen Cybersicherheitsrisiko beschäftigt, welches die Vernetzung der Akteure in einem Hafenverbund bedeutet. Diese freiwilligen verbandsseitigen Vorgaben sollen zunächst zentrale Elemente der maritimen Cyberresilienz abstecken und ein Bewusstsein für Cybersicherheit schaffen. Sie beinhalten hingegen keine detaillierten Vorgaben.

53 https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf, abgerufen am 17.2.2025.

54 https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf, abgerufen am 17.2.2025.

Insbesondere nach dem Maersk-Vorfall 2017 (s.o.) begannen einzelne Seehäfen damit, Cybersicherheit auch institutionell sichtbar zu machen. In Bremen (bremenports) und Niedersachsen (JadeWeserPort) wurden Cybersicherheitsbeauftragte (Port Cyber Security Officer) geschaffen. Auch die IAPH plädiert für die Bestellung eines solchen Beauftragten (Chief Information Security Officer).[55] Die Aufgabe dieser Beauftragten besteht im Kern in der Koordinierung, indem sie einen Erfahrungsaustausch zu Cyberrisiken und dem Umgang damit zwischen den Akteuren des jeweiligen Hafennetzwerks initiieren und Problembewusstsein schaffen. Die IAPH sieht auch eine direkte Kommunikation mit der Geschäftsleitung vor. Über echte Durchsetzungsbefugnisse verfügen die Beauftragten hingegen nicht; stattdessen agieren sie auf Vertrauensbasis.

Versicherungen stellen an ihre Versicherungsnehmer seit gut fünf Jahren infolge der steigenden Schadenshöhe von Cyberattacken auf Häfen entsprechende Anforderungen an die IT-Sicherheit, deren Einhaltung sie vor Ort durch Experten überprüfen lassen.[56] Allerdings fehlen bislang Anreize auf Hafenseite, solche Versicherungen abzuschließen.[57] Bei der maritimen Cybersicherheit entwickeln sich erst langsam mit der Verschärfung des Cyberresilienzregimes auf regional-staatlicher Ebene entsprechende Anreize (siehe C.III.).

Insgesamt fehlt es mithin auf völkerrechtlicher Ebene und im selbstregulativen Bereich an harten Instrumenten für die Cybersicherheit in Seehäfen.

55 https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf, S. 18, abgerufen am 17.2.2025.

56 *Cremer* et al., in: The Geneva Papers on Risk and Insurance – Issues and Practice 47 (2022), 698 ff.

57 Zur Bedeutung solcher Anreize *OECD*, Enhancing the Role of Insurance in Cyber Risk Management, 2017, S. 135 ff.; *Baskin, Bobys*, in: Johansson et al., Smart Ports and Robotic Systems, 2023, S. 249, 262. Die IAPH empfiehlt ihren Mitgliedern nur den Abschluss einer solchen Versicherung, Guidelines, S. 15 f. Das Fehlen eines solchen Anreizregimes für die maritime Cyberresilienz stellt einen Unterschied zum Bereich der schiffsseitigen Ölverschmutzungen dar, bei denen die USA mit dem Oil Pollution Act von 1990 nach der Exxon Valdez-Havarie 1989 ein Haftungsregime mit einer Versicherungspflicht etablierte, das Anreize für einen Versicherungsmarkt schuf, zu diesem Altfuldisch, Haftung und Entschädigung nach Tankerunfällen auf See, 2007, 109 f.

III. Regional-nationale Ebene

Sowohl in den USA als auch in der Union wurde in den letzten Jahren die Regulierung der Cybersicherheit verschärft. Im US-amerikanischen Recht wurde ein prononciert sektoraler Ansatz maritimer Cybersicherheit entwickelt, bei dem die entsprechenden Zuständigkeiten im Kern bei der Küstenwache liegen und der sich am Recht der physischen Hafensicherheit orientiert. Anders ist das in der EU und in Deutschland. Dort werden ausgehend von Referenzvorgaben erst allmählich spezifische Anforderungen und Instrumente für die Cyberresilienz von Seehäfen entwickelt; auch ist dort noch unklar, ob und inwiefern maritime Fachbehörden Zuständigkeiten für die Cybersicherheit von Seehäfen haben.

1. US-Recht

Seehäfen werden in den USA von einer Vielzahl von Behörden auf Bundes-, Landes- und kommunaler Ebene reguliert. Innerhalb dieses Wirrwarrs ist die Küstenwache (U.S. Coast Guard, USCG) als Teil des U.S. Department of Homeland Security (DHS) mit der Regelung und Durchsetzung der Gefahrenabwehr in Seehäfen betraut.[58] Die USCG hat den weitreichenden Auftrag, „Gesetze zu verwalten und Vorschriften zur Förderung der Sicherheit von Leben und Eigentum auf und unter der hohen See und den Gewässern, die der Gerichtsbarkeit der Vereinigten Staaten unterliegen, zu erlassen und durchzusetzen" (U.S. Code, Title 14, § 102). Die USCG nimmt diese Aufgabe durch spezielle Bundesgesetze zur Gefahrenabwehr in Häfen wahr, darunter v.a. der Maritime Transportation Security Act von 2002 (MTSA). Der MTSA (U.S. Code, Title 46, § 701, implementiert im Code of Federal Regulations, Title 33) dient der Umsetzung des ISPS Codes der IMO. Er ermächtigt die USCG dazu, weitere Anforderungen, insbesondere in Form von sog. MARSEC-Richtlinien (Code of Federal Regulations, Title 33, §§ 101.405; 105.145), zu erlassen und durchzusetzen (U.S. Code, Title 46, § 70116). Die Durchsetzung der MARSEC-Richtlinien im Seehafen und gegenüber Schiffen erfolgt maßgeblich durch den örtlichen Hafenkapitän

58 *Lidinsky Jr.*, *Colson*, The Federal Regulation of American Port Activities, 7 Md. J. Int'l, 1981, L. 38.

(Captain of the Port, COTP)[59], einem in den jeweiligen Häfen ansässigen, hochrangigen Offizier der Küstenwache mit Zuständigkeiten für Reaktion (einschließlich Durchsetzung), Prävention und Regulierung (Code of Federal Regulations, Title 33, §§ 101.105; 101.400).

Der MTSA konzentrierte sich ursprünglich auf die physische Sicherheit, nicht die Cybersicherheit.[60] In den letzten Jahren wurde die Zuständigkeit der USCG aber auch auf die Abwehr von Cyberattacken erstreckt (U.S. Code Title 46, § 70116). Das primäre Ziel der USCG besteht darin, das Risikobewusstsein und das Risikomanagement in Seehäfen zu fördern und ein Maritime Cybersecurity Compliance Regime zu etablieren, um die Verwundbarkeit für Cyberangriffe zu reduzieren. Dazu hat sie zunächst freiwillige Leitlinien für die maritime Cybersicherheit erlassen, die erste Vorgaben machen. Die USCG knüpft dabei an die Regulierung der physischen Sicherheit in Häfen an (Navigation and Vessel Inspection Circular (NVIC) 01-20).[61] Ihr Maritime Cybersecurity Assessment & Annex Guide (MCAAG) sieht dementsprechend vor, dass die Anlagenbetreiber im Hafen, einen Sicherheitsbeauftragten für die Anlage (Facility Security Officer, FSO) benennen, eine Sicherheitsbewertung für die Anlage (Facility Security Assessment, FSA) durchführen, um Schwachstellen bei der physischen Sicherheit und der Cybersicherheit zu ermitteln und einen Sicherheitsplan für die Anlage (Facility Security Plan, FSP) entwickeln, um diese Schwachstellen zu beseitigen. Zusätzlich soll ein Cybersicherheitsbeauftragter (Cybersecurity Officer, CSO) bestellt werden, der den FSO mit seiner Expertise in Cybersicherheitsfragen unterstützt. Auch wird an Risikobewertungsinstrumenten für die maritime Cybersicherheit gearbeitet.[62] Zentraler behördlicher Anknüpfungspunkt, auch für die Cybersecurity, ist der Captain of the Port.[63] Die USCG koordiniert sich zudem mit der allgemein für die Cybersicherheit zuständigen Agentur, der Cybersecurity

59 Zu ihm *Ma, Loomis*, Full Steam Ahead: Enhancing Maritime Cybersecurity, 2023, S. 5.; Der COPT hat auch jenseits der Cybersicherheit weitreichende Befugnisse, The Coast Guard Journal of Safety & Security at Sea Proceedings 75, Heft 2, 2018, S. 5 f.

60 *Kramek*, The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities, 2013, S. 2.

61 *USCG*, Cyber Strategic Outlook, 2021, S. 5.

62 Zum Maritime Cyber Risk Assessement Model (MCRAM), *USCG*, Office of Port and Facility Compliance, 2019 (https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Year%20in%20Review/CG-FAC%20YearInReview%202019_Final.pdf?ver=2020-05-21-081529-687, abgerufen am 17.2.2025), S. 10.

63 *USCG*, Cyber Strategic Outlook, 2021, S. 7, 12.

and Infrastructure Security Agency (CISA). Die CISA hat anschließend an den MCAAG der USCG die Anforderungen an die Sicherheitsbewertung durch einen Marine Transportation Security Resilience Assessment Guide konkretisiert.[64]

Entsprechend den allgemeinen Vorgaben der CISA wird auch im maritimen Sektor der Austausch von Informationen gefördert[65]: Innerhalb der Verwaltung koordiniert sich die USCG mittels des Maritime Modal Government Coordinating Council (MMGCC); seitens der Betreiber dient der Koordinierung der Maritime Modal Sector Coordinating Council (MMSCC).[66] Der staatlich-private Informationsaustausch erfolgt über das Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC).[67] MTS-ISAC soll den Austausch von Informationen über Sicherheit, kritische Infrastrukturen und Bedrohungen mit Regierungen und Industriepartnern im Bereich der maritimen Sicherheit und der kritischen Infrastruktur erleichtern.

2. Unionsrecht und deutsches Recht

Auf EU-Ebene wird die Cybersicherheit zunehmend durch verbindliche und scharfe Vorgaben geregelt. Für diese Herangehensweise steht die zweite Netz- und Informationssicherheitsrichtlinie (NIS-2-Richtlinie)[68], die für öffentliche und private Einrichtungen gleichermaßen gilt, die ihre Dienste in der Union erbringen oder ihre Tätigkeit dort ausüben, grundsätzlich vorausgesetzt, sie überschreiten bestimmte Schwellenwerte (Art. 2).[69] Die Einrichtungen, die von der NIS-2-Richtlinie erfasst werden können, sind in den Anhängen I und II der Richtlinie für verschiedene Sektoren aufgelistet. Nach Anhang I Nr. 2 c) zählen „Leitungsorgane von Häfen, einschließlich

64 https://www.cisa.gov/sites/default/files/2023-03/Marine%20Transportation%20System%20Resilence%20A-ssessment%20Guide.pdf, abgerufen am 17.2.2025.

65 Siehe *CISA*, Critical Infrastructure Threat Information Sharing Framework, 2020.

66 DHS, Transportation Sector-Specific Plan (https://www.dhs.gov/xlibrary/assets/Transportation_Mari-time_Modal_Annex_5_16_07.pdf, abgerufen am 17.2.2025), S. 1 f., 26.

67 https://www.mtsisac.org/, abgerufen am 17.2.2025.

68 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates v. 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS2-RL), ABl. 2022 L 333, ABl 2022 L 333, 80.

69 Der Cyber Resilience Act der EU erfasst im Unterschied dazu alle digitalen Produkte und Software mit einer digitalen Komponente.

ihrer Hafenanlagen, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betrieben" zu den Sektoren mit hoher Kritikalität und unterfallen damit im Ausgangspunkt dem Anwendungsbereich der Richtlinie. Die enge Bereichsausnahme für bestimmte Einrichtungen der öffentlichen Verwaltung (Art. 2 Abs. 7, Abs. 8) trifft auf den Bereich der Seehäfen nicht zu.

Die Mitgliedstaaten müssen nach der NIS-2-Richtlinie eine entsprechende Behördenstruktur schaffen und ihre Behörden innerstaatlich sowie grenzüberschreitend abstimmen. Die Behördenstruktur setzt sich aus Aufsichtsbehörden, Anlaufstellen, Behörden für das Cyberkrisenmanagement und den Computer-Notfallteams (CSIRTs) zusammen (Art. 8 ff.) und wird durch ein (freiwilliges) Peer Review unionsrechtlich begleitet (Art. 19). Auf EU-Ebene übernimmt die Agentur der Europäischen Union für Cybersicherheit (ENISA) die zentrale Koordinierungsaufgabe.

Das Pflichten- und Durchsetzungskorsett der NIS-2-Richtlinie ist danach abgestuft, ob es sich um „wesentliche" oder nur „wichtige" Einrichtungen handelt (Art. 3), was sich nach dem Erreichen von Schwellenwerten und Einstufungsentscheidungen der Mitgliedstaaten richtet. Art. 21 NIS-2-RL verpflichtet wesentliche und wichtige Einrichtungen zu Risikomanagementmaßnahmen im Bereich der Cybersicherheit, wie ein Back-up-Management, Schulungen im Bereich Cyber-Hygiene oder eine Multi-Faktor-Authentifizierung. Die Richtlinie nimmt explizit die Geschäftsleiter („Leitungsorgan der wesentlichen oder wichtigen Einrichtung") in die Verantwortung, die Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße durch die betreffenden Einrichtungen verantwortlich gemacht werden können muss (Art. 20). Hinzu treten Berichtspflichten für erhebliche Sicherheitsvorfälle mit abgestuften Fristen von 24 bis 72 Stunden (Art. 23) sowie ein Informationsaustausch auf freiwilliger Ebene (Art. 29, 30). Ein strenges Aufsichts- und Sanktionsregime der mitgliedstaatlichen Behörden sichert die Cybersicherheitsanforderungen ab (Art. 31 ff.). Die maximale Geldbuße für wesentliche Einrichtungen beträgt 7 bzw. 10 Mio. Euro oder 1, 4 % bzw. 2 % des weltweiten Jahresumsatzes (Art. 34). Zusätzlich können die Leitungsorgane der erfassten Einrichtungen von ihren Aufgaben ausgeschlossen werden, es sei denn es handelt sich bei der Einrichtung um eine solche der öffentlichen Verwaltung (Art. 32 Abs. 5).

In Deutschland soll die NIS-2-Richtlinie auf Bundesebene durch das sog. NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

als Artikelgesetz umgesetzt werden.[70] Dieses wandelt das BSIG zu einem IT-Sicherheitsgesetz um, was sich auch in einer Änderung seines Namens niederschlägt: Das BSIG wird in Zukunft „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Betreibern und Einrichtungen" heißen anstatt wie bisher „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik". Damit bildet das BSI (weiterhin)[71] die zentrale Behörde für Cybersicherheit in Deutschland (§ 1 S. 2 BSIG-E). Der Bund hat allerdings nicht die Kompetenz, die Cybersicherheit der öffentlichen Verwaltung von Ländern und Kommunen zu regeln. Damit bedarf es auch IT-Sicherheitsgesetze der Bundesländer bzw. diese müssen angepasst werden.[72] Das wird Bedeutung für Seehäfen haben, da die Hafenbehörden Teil der Verwaltung der Küstenländer sind und damit die Regelung ihrer Cyberresilienz, wie von der NIS-2-Richtlinie gefordert, nicht vom BISG erfasst wird, sondern den IT-Sicherheitsgesetzen der Bundesländer unterliegt. Die Landesgesetze werden sich aber wohl nur auf die Sicherstellung der eigenen Cybersicherheit der Hafenbehörden beziehen können und nicht auf die der Cybersicherheit des ganzen Hafensystems, da man dieses Netzwerk kaum zur öffentlichen Verwaltung zählen kann. Neben den Kompetenzen wird voraussichtlich faktisch der Hafenwettbewerb verhindern, dass weitergehende Hafensicherheitsgesetze erlassen werden, sprich die den Hafenverwaltungen umfassende Befugnisse für die Cybersicherheit im Hafen verleihen. Auch das Bundesamt für Seeschifffahrt und Hydrographie (BSH) ist nicht direkt für den Hafenbereich zuständig, so dass in Deutschland die behördlichen Kompetenzen für die hafenseitige Cybersicherheit zwischen Hafenverwaltungen und BSI aufgeteilt sein werden.

Die NIS-2-Richtlinie stellt letztlich einen Referenzrahmen der Cybersicherheit dar,[73] der sich nicht spezifisch auf den maritimen Bereich bezieht. Weder das Unionsrecht noch das deutsche Recht kennen bislang Cyberresilienzvorgaben für Seehäfen. Die ENISA hat in Leitfäden bislang immerhin die praktischen Erfahrungen zusammengetragen, Herausforderungen be-

70 Zum Gesetzesentwurf der Bundesregierung BT-Drs. 20/13184; siehe zudem das Diskussionspapier vom September 2023 https://ag.kritis.info/wp-content/uploads/2023/09/Anlage-2-Diskussionspapier.pdf, abgerufen am 17.2.2025.

71 *Wischmeyer*, a.a.O., S. 222.

72 Zu den Plänen der Bundesländer (Stand Februar 2024) https://it-sicherheit-und-recht.de/wo-stehen-die-laender-hinsichtlich-der-umsetzung-der-nis-2-richtlinie/, abgerufen am 17.2.2025.

73 Siehe Art. 4 NIS-2-RL.

schrieben und ein Vier-Phasen-Modell des maritimen Risikomanagements entwickelt.[74] Im Unterschied zum US-Recht fällt weiter auf, dass auf Unionsebene und in Deutschland maritime Fachbehörden weniger stark in die Regulierung integriert sind.

D. Perspektiven internationalisierter Cyberresilienz

Der Blick auf die Regelungsansätze hat gezeigt, dass es bislang im Hafenbereich keine in sich stimmige inhaltliche Regelung der Cybersicherheit gibt. In Bezug auf die Verwaltungsorganisation fehlt es an klaren Zuständigkeiten; vielmehr bestehen viele institutionelle Anknüpfungspunkte. Richtschnur der daher erforderlichen Orchestrierung (siehe A.II.) ist die Überlegung, dass eine Steuerung im Sinne einer Lenkung durch eine Spitze in dezentralen, internationalisierten Regelungsstrukturen nicht möglich ist. Machbar ist allenfalls eine Lenkung im Sinne einer gegenseitigen Abstimmung und Unterstützung der beteiligten Akteure. Ausgehend von diesem Konzept werden im Folgenden perspektivisch rechtliche Instrumente und Prinzipien einer Orchestrierung diskutiert.

I. Gesamtrisikoanalyse im Seehafen

Das Recht wird gewöhnlich ausgehend von den Kategorien der Zurechnung und Verantwortung konstruiert. Demgegenüber lässt sich bei der Regelung der hafenseitigen Cybersicherheit der Adressat von Cyberresilienzanforderungen nicht sicher bestimmen. Das Adressatenproblem rührt daher, dass Seehäfen sich nicht als Akteure im Sinne geschlossener Einheiten begreifen lassen, sondern transnationale Netzwerke darstellen, in die eine Vielzahl eigenständiger und heterogener Akteure mit ausländischen Bezügen eingebunden sind. Rechtliche Fragen, die aus der Adressatenstellung resultieren, können etwa sein: Treffen die Pflichten, etwa die Pflicht zu organisatorischen und technischen Maßnahmen der Cyberresilienz („Risikomanagement") oder Meldepflichten, die einzelnen Betreiber der Anlagen im Hafen und / oder die Hafenverwaltung? Wie weit reichen die jeweiligen Verantwortlichkeiten und wie können die Pflichten gegenüber den Adressa-

74 Etwa *ENISA*, Port Cybersecurity, 2019; *ENISA*, Cyber Risk Management for Ports, 2020.

ten durchgesetzt werden? Die Regulierungsansätze (s.o., C.) geben darauf unterschiedliche und nicht immer eindeutige Antworten:

- Der internationale Hafenverband IAPH adressiert in seinen Leitlinien sowohl die Häfen („ports") als auch die Hafeneinrichtungen („port facilities");[75] er betont die Bedeutung einer akteursübergreifenden Abstimmung und betrachtet die Hafenverwaltungen dabei als Vermittler („orchestrator") mit einer übergreifenden Cybersicherheitsverantwortung.[76]
- Das US-Recht setzt entsprechend der Regulierung der physischen Sicherheit von Häfen an den einzelnen Anlagen an (Code of Federal Regulations, Title 33, § 105.105). Der Captain of the Port ist auch für Fragen der maritimen Cybersicherheit zuständig und übernimmt dafür eine übergreifende, überwachende und koordinierende Rolle im jeweiligen Hafen.[77]
- Das Unionsrecht ist unklar. Nach dem dritten Spiegelstrich in Nr. 2 c) des Anhangs I der NIS-2-RL werden „Leitungsorgane von Häfen (…), einschließlich ihrer Hafenanlagen (…), sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben" als Sektoren mit hoher Kritikalität eingestuft, die der Richtlinie unterfallen. Das Wort „einschließlich" ließe sich im Sinne von „unter Einschluss" so lesen, dass das gesamte Hafenökosystem die wesentliche bzw. wichtige Einrichtung ist, so dass die Hafenverwaltung eine Gesamtverantwortlichkeit für die Cyberresilienz im ganzen Hafen träfe. Diese Interpretation im Sinne eines ganzheitlichen Ansatzes unterstreicht die systematische Zuordnung der Häfen unter einem Spiegelstrich im Anhang I. Die Kommasatzung in Nr. 2 c) des Anhangs I der NIS-2-RL und das Wort „sowie" legen hingegen einen punktuellen Ansatz nahe, der an den jeweiligen Anlagen und Einrichtungen ansetzt. Das „sowie" soll danach klarstellen, dass auch die Hafenverwaltung unter den Anwendungsbereich der Richtlinie fällt.
- Die KRITIS-VO setzt bislang an den einzelnen Einrichtungen und Anlagen im Hafen an, indem sie in Anhang Nr. 7 die relevanten Einrichtungen im Hafen jeweils gesondert aufzählt (Nr. 1.7-1.19: Umschlaganlage, Hafenleitungsorgan, Hafeninformationssystem).

75 https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf, S. 17, abgerufen am 17.2.2025.
76 https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-20-20.pdf, S. 5, abgerufen am 17.2.2025.
77 *USCG*, Cyber Strategic Outlook, 2021, S. 7, 12.

Cyberrisiken sind Systemrisiken. Das hat Konsequenzen für die Frage nach dem Adressaten von Rechtspflichten. Adressat ist danach gerade nicht der oftmals schwer fassbare polizeiliche Störer, sondern Adressat ist,[78] wer die Funktionsherrschaft, sprich die Möglichkeit eines wirksamen Zugriffs auf die jeweilige Infrastruktur hat.[79] Diese Funktionsherrschaft haben die jeweiligen Betreiber, etwa Terminalbetreiber, und die Hafenverwaltung für ihren jeweiligen Machtbereich. Der Hafenverwaltung eine Gesamtverantwortlichkeit für die Cybersicherheit im Hafenökosystem zuzuschreiben, scheint zwar den Vorteil zu haben, dass die Hafenverwaltung vor Ort der zentrale Anknüpfungspunkt wäre anstatt zahlreicher, auch ausländischer Betreiber, die sich zudem untereinander in ihren Resilienzanstrengungen koordinieren müssten, was wegen ihrer heterogenen Interessen und ihres Konkurrenzverhältnisses u.U. schwierig sein kann. Bezogen auf das Unionsrecht hätte dieser ganzheitliche Ansatz aber zur Konsequenz, dass der Hafenkapitän als das „Leitungsorgan" i.S.d. Art. 20 NIS-2-RL der wesentlichen oder wichtigen Einrichtung Seehafen die Governance-Verantwortung (Art. 20 NIS-2-RL) für das gesamte Hafenökosystem träfe; er könnte demnach für Defizite in der maritimen Cyberresilienz im gesamten Hafenökosystem haftbar gemacht werden. Zudem könnte er wohl[80] von seinen Aufgaben ausgeschlossen werden, Art. 32 Abs. 5 NIS-2-RL. Der Hafenkapitän hat jedenfalls in deutschen Häfen keinen Einblick in alle Anlagen und Anlagen im Hafengebiet; er hat auch keine Weisungsbefugnisse oder sonstigen rechtlichen Befugnisse in Bezug auf die Cybersicherheit gegenüber den Betreibern der jeweiligen Anlagen und Einrichtungen im Hafen und könnte die Sicherheitsanforderungen auch nicht extraterritorial durchsetzen. Den Einbezug ausländischer Akteure in das Pflichten- und Aufsichtsregime der Cyberresilienz sichern die regional-staatlichen Regelungen nur partiell über extraterritoriale Jurisdiktionen und Vertreterlösungen ab.[81]

78 Bezogen auf die Ebene der System- und Netzwerksicherheit, zu den drei Ebenen und ihren Adressaten *Wischmeyer*, S. 237 ff.

79 *Freimuth*, S. 218 f.; *Schneider*, Meldepflichten, 2017, S. 383.

80 Diese Ausschlussmöglichkeit soll nicht bei „Einrichtungen der öffentlichen Verwaltung" (Art. 6 Nr. 35) bestehen, aber die NIS-2-RL zählt in Anhang I die Hafenverwaltung als das „Leitungsorgan von Häfen" zum Sektor „Verkehr" und nicht zum Sektor „öffentliche Verwaltung".

81 Für zentrale Internet-Infrastrukturdienste, wie DNS-Dienstleistungen, siehe die breite Jurisdiktionsregelung in Art. 26 I, II NIS-2-RL und die Normierung von Vertreter- und Registrierungspflichten (Art. 26 III, Art. 27 I NIS-2-RL), zum Ganzen *Wischmeyer*, S. 212 ff., 216; ferner *Schneider*, S. 428 ff., nach dem die Meldeplichten im BSIG auch extraterritorial gelten; siehe zudem die extraterritorialen Ansätze im BSIG in

Daher ist im Ausgangspunkt von einem punktuellen Ansatz auszugehen, der an den jeweiligen Einrichtungen und Systemen im Seehafen ansetzt. In dem Maße, in dem die jeweiligen Akteure im Seehafen untereinander vernetzt sind, muss aber auch dieses Hafenökosystem im Sinne einer Gesamtrisikoanalyse in die Regulierung der Cybersicherheit einbezogen werden.[82] Die Regulierungsansätze der IAPH und im US-Recht unterstreichen die Notwendigkeit einer solchen Gesamtrisikoanalyse.[83] Deswegen muss der Hafenverwaltung aber keine Gesamtverantwortung zugesprochen werden, der sie kaum nachkommen kann. Wichtig ist vielmehr, eine Koordinierung, v.a. einen Erfahrungsaustausch, im jeweiligen Hafenökosystem zu initiieren, wie er von der IAPH eingefordert wird und in einigen Häfen selbstregulativ erfolgt (siehe C.II.). Einen organisatorischen Anknüpfungspunkt für die Gesamtrisikoanalyse bilden dabei die Cybersicherheitsbeauftragten in den jeweiligen Häfen (siehe C.II.).

II. Rezeption transnationaler maritimer Cyberresilienzstandards

Seehäfen unterscheiden sich in ihren Strukturen und Sicherheitsrisiken stark voneinander. Gleichwohl bedarf es eines branchenspezifischen und v.a. auch international abgestimmten Kanons von Cybersicherheitsanforderungen. Die IAPH und die USCG betonen in diesem Sinne, dass es der Entwicklung einer „gemeinsamen globalen Sprache" bedürfe.[84] Diese gemeinsame globale Sprache, sprich grenzüberschreitende Cybersecuritystandards für Seehäfen, gibt es aber noch nicht,[85] sondern nur Vorstufen

Bezug auf die Komponentensicherheit (§ 8b VI); zur Extraterritorialität im US-Recht (MTSA) *Cox*, National Security Law Journal 1 (2013), 77, 86 ff.

82 Siehe zu diesem ganzheitlichen Ansatz den einen Marine Transportation Security Resilience Assessment Guide der CISA https://www.cisa.gov/sites/default/files/2023-03/Marine%20Transportation%20System%20Re-silence%20Assessment%20Guide.pdf, abgerufen am 17.2.2025.

83 Siehe dazu aber auch *ENISA*, Port Cybersecurity, S. 47.

84 https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf; *USCG*, Maritime Cybersecurity Assessment & Annex Guide (MCAAG) S. 3, abgerufen am 17.2.2025.

85 Zum Problem *McCready, Callahan, Mayhew*, and *Heckman*, "Toward a Maritime Cyber Security Compliance Regime." Paper presented at the SNAME Maritime Convention, Providence, Rhode Island, USA, October 2018; zu Ansätzen *Progoulakis, Nikitakos, Dalaklis, Yaacob*, Cyber-physical security for ports infrastructure, 2022.

v.a in Form von Leitlinien von Verbänden und Behörden.[86] Die ISO hat nur Anforderungen allgemeiner Art entwickelt[87] und im Rahmen der IMO ist, wie gesehen (siehe C.I.), nicht zu erwarten, dass in absehbarer Zeit verbindliche Vorgaben zustande kommen. Angesichts der Hemmnisse völkerrechtlicher Koordination sowie der privaten Expertise bilden Ausgangspunkt selbstregulative Standards für die maritime Cybersicherheit.

Diese selbstregulativen Standards können dann vom staatlich-regionalen Recht und vom Völkerrecht rezipiert werden. Eine solche Rezeption sieht im nationalen Kontext § 8a Abs. 2 BSIG (§ 30 Abs. 12 BSIG-E) vor, wonach von Betreiber- und Verbandsseite aus branchenspezifische Standards (sog. B3S) vorgeschlagen werden können. Das Unionsrecht betont, dass sich die Europäische Kommission bei der Konkretisierung der Anforderungen an das Risikomanagement „so weit wie möglich an europäischen und internationalen Normen" zu orientieren hat (Art. 21 Abs. 5 NIS-2-RL; auch Art. 21 Abs. 1 UAbs. 2 NIS-2-RL). Die IMO verweist in ihrem Soft Law auf die Standards des internationalen Hafenverbands IAPH (siehe C.I.).

III. Transnationale hybride Kommunikationsnetzwerke

Cyberrisiken sind Systemrisiken mit grenzüberschreitendem Bezug. Sie zu bewältigen, stellt daher ein Gemeinschaftsprojekt dar. Eine rechtzeitige Erkennung von Bedrohungen und das Ergreifen adäquater Resilienzmaßnahmen hängen in hohem Maße von einem regelmäßigen Informationsaustausch über Bedrohungen und Schwachstellen und von einer rechtzeitigen und strukturierten Weitergabe von Risikoinformationen ab. Dieser Erfahrungsaustausch muss zum einen einmal im jeweiligen Hafenökosystem stattfinden (D.I.), zum anderen aber auch zwischen Seehäfen und unter Einschluss der behördlichen Ebene sowohl auf nationaler als auch auf regionaler und internationaler Ebene. Transnationale Netzwerke, die private und staatliche Akteure einbinden und insofern als hybride bezeichnet werden können, stellen eine Lösung dar, um diese Kommunikationsprozesse zu verfestigen.

86 Siehe oben unter III.

87 ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements.

Dafür stehen im Cybersicherheitsrecht v.a. die sog. Information Sharing and Analysis Centers (ISACs).[88] ISACs sind sektorspezifische, privatrechtlich organisierte Einrichtungen, um zeitnah Bedrohungsinformationen zu sammeln, zu analysieren und zu filtern und diese Bedrohungsinformationen an die Betreiber der kritischen Infrastrukturen, an andere Sektoren und an staatliche Stellen weiterzugeben. ISACs stellen ihren Mitgliedern zudem Instrumente und bewährte Verfahren zur Verfügung, um Risiken digitaler und physischer Natur zu mindern und die Widerstandsfähigkeit der Anlagen zu verbessern. Jede ISAC setzt demnach ihr spezielles Branchenwissen und ihre Erfahrung ein, indem sie als Clearingstelle für staatliche und private Informationen dient und den Mitgliedern hilft, Risiken zu erkennen.

Ihr Verhältnis zu den IT-Notfallteams (CERTs bzw. CSIRTs)[89], einem weiteren organisatorischen Instrument im Cybersicherheitsrecht, ist unklar. Teilweise werden ISACs durch ihren sektorspezifischen Bezug von den übergreifend agierenden CERTs unterschieden,[90] teils werden ISACs als sektorspezifische Ausprägung und damit Unterkategorie von CERTs betrachtet.[91] Ein wesentlicher Unterschied dürfte darin liegen, dass ISACs von vorneherein als Plattformen des Erfahrungsaustauschs zwischen privaten und öffentlichen Akteuren gedacht sind,[92] während CERTs zunächst bei den jeweiligen Organisationen angesiedelt sind und sich ggf. in eigenen nationalen, europäischen und internationalen Verbünden vernetzen.[93]

ISACs wurden in den USA unter Präsident Clinton entwickelt und stehen dort oftmals unter einem starken staatlichen Einfluss.[94] Im maritimen

88 *CISA*, https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf, S. 26, abgerufen am 17.2.2025; *ENISA*, Information Sharing and Analysis Center (ISACs) - Cooperative models (https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, abgerufen am 17.2.2025), 2018.

89 Die Entwicklung von IT-Notfallteams wird auf das Jahr 1988 zurückdatiert. Ihre Aufgabe besteht im Umgang mit IT-Notfällen, wozu sie operativ und analysierend vorgehen, *Fox*, in: DuD 2002, 493 ff.

90 *Liska*, Building an Intelligence-Led Security Program, 2014, Kap. 8.

91 *Kruidhof*, in: Hathaway, Best Practices in Computer Network Defense: Incident Detection and Response, 2014, S. 86.

92 *ENISA*, Information Sharing and Analysis Center (ISACs) – Cooperative Models, 2018, S. 7.

93 Etwa zwischen den EU-Mitgliedstaaten als CSIRTs-Netzwerk, Art. 15 NIS-2-RL.

94 Presidential Decision Directive 63, 1998 (https://irp.fas.org/offdocs/paper598.htm), abgerufen am 17.2.2025; weiterentwickelt unter Präsident Bush, Homeland Security Presidential Directive 7, 2003 (https://www.cisa.gov/news-events/directives/homela

Bereich regte die USG 2020 an, das MTS-Information Sharing and Analysis Center (MTS-ISAC)[95] zu gründen, das viele US-amerikanische Häfen umfasst. ISACs werden aber zunehmend weltweit gegründet,[96] wobei ihre Entwicklung in Europa im maritimen Bereich noch im Anfangsstadium ist.[97] Solche nationalen und regionalen ISACs stellen den ersten Schritt zu internationalen ISACs dar.[98] Teilweise versuchen sich örtliche ISACs auch über staatliche Grenzen hinweg zu öffnen und bieten sich der internationalen Community an. Im europäischen Raum ist das Maritime Computer Security Incident Response Team zu nennen, das Informationen zu maritimen Cyberrisiken analysiert und mit anderen privaten und öffentlichen Stellen teilt. Diese französische Initiative richtet ihre Dienstleistungen an den weltweiten maritimen Sektor.[99]

IV. Recht als Anreizsetzer

Die Regulierung der maritimen Cybersicherheit basiert, wie gesehen, maßgeblich auf selbstregulativen Strukturen. Das Grundproblem selbstregulativer Standardsetzung und -durchsetzung ist das mitunter fehlende Engagement zu einem umfassenden Sicherheitsengagement. Das regionale bzw. staatliche Recht kann diese selbstregulativen Ansätze abstützen. Ansätze dazu gibt es im Unionsrecht und im US-Recht:

- So verlangt die NIS-2-Richtlinie in Art. 29 Abs. 2, dass die Mitgliedstaaten sicherstellen, dass der Informationsaustausch innerhalb Gemeinschaften wesentlicher und wichtiger Einrichtungen und gegebenenfalls ihrer Lieferanten oder Dienstleister stattfindet (siehe auch § 6 BSIG-E). Dieser Auftrag kann die Entwicklung einer Gesamtrisikoanalyse in Seehäfen abstützen.
- Für die Standardsetzung ist Art. 25 NIS 2-RL zu nennen, der die Mitgliedstaaten und die Union auffordert, Normsetzungsaktivitäten der

nd-security-presidential-directive-7, abgerufen am 17.2.2025); eingehend *He, Devine, Zhuang*, Risk Analysis 38 (2018), 215 ff.

95 https://www.mtsisac.org/, abgerufen am 17.2.2025.

96 *ENISA*, S. 7.

97 *ENISA*, S. 17.

98 *ENISA*, Information Sharing and Analysis Center (ISACs) - Cooperative models (https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, abgerufen am 2.9.2024), 2018, S. 22 ff.

99 https://m-cert.fr/index_en.html, abgerufen am 17.2.2025.

europäischen und internationalen Normungsorganisationen zu fördern, wobei die ENISA eine Koordinationsrolle übernehmen soll.
– Dem staatlichen bzw. regionalen Recht kommt auch bei den ISACs eine begleitende Rolle zu.[100] So wird die MTS-ISAC maßgeblich von der USCG begleitet und die NIS-2-RL sichert das Entstehen von ISACs ab, indem sie den Informationsaustausch zwischen den Einrichtungen betont (Art. 26) und Meldepflichten statuiert (Art. 23).[101]

V. Vertrauen als Direktive

Die akteursübergreifende und v.a. grenzüberschreitende Zusammenarbeit zum Zwecke der Cyberresilienz bedarf entsprechender Vertrauenskonzepte.[102] Das Recht kann ein solches Vertrauen fördern, aber auch die Bildung von Vertrauen hemmen:

– Für die Zwecke der Orchestrierung innerhalb der jeweiligen Seehäfen (siehe D.I.) ist es etwa unter Vertrauensgesichtspunkten tendenziell kontraproduktiv, die Cybersicherheitsbeauftragten, die sich zunächst selbstregulativ herausgebildet haben, mit Durchsetzungsbefugnissen oder direkten Meldepflichten gegenüber Behörden auszustatten, da dies die Gesamtrisikoanalyse im jeweiligen Seehafen hemmen kann.
– Andererseits verlangt eine rechtliche Rezeption transnationaler selbstregulativer Cyberresilienzstandards einer kritischen rechtlichen Begleitung. In diesem Sinne sieht § 8a Abs. 2 BSIG (§ 30 Abs. 12 BSIG-E) vor, dass Betreiber bzw. Verbände branchenspezifische Standards (sog. B3S) vorgeschlagen können, die anschließend behördlicherseits auf ihre Eignung geprüft werden. Bei dieser kritischen Begleitung unter der Ägide des BSI besteht aber noch Verbesserungspotential.[103] Auch auf europäischer und internationaler Ebene haben sich noch keine kritischen Rezep-

100 Zur Bedeutung von Anreizsetzung *ENISA*, Incentives and Barriers to Information Sharing (https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing), abgerufen am 17.2.2025, 2010, S. 16 ff.
101 Dazu *ENISA*, ISAC, 2018, S. 7.
102 *Pohlmann*, Cyber-Sicherheit, 2019, S. 22; ENISA, ISACs, 2018, S. 7.
103 Kritisch *Hoffmann, Müllmann*, DV 2022, 467 ff. und *Dürig, Fischer*, DuD 2018, 209 ff.

tionsmechanismen herausgebildet. Insofern könnte man sich an anderen Bereichen des maritimen Rechts orientieren.[104]

E. Fazit

Seehäfen lassen sich als infrastrukturelle und digitale Netzwerke begreifen, die in vielen Fällen ausländische Akteure einbinden und damit transnationale Strukturen ausgebildet haben. Cyberresilienz in diesem maritimen Ökosystem sicherzustellen, ist ein Anliegen, das vom staatlichen Recht oder Völkerrecht nicht allein bewältigt werden kann, sondern der Einbeziehung selbstregulativer Regelungsstrukturen bedarf. Ausgehend vom Konzept der Orchestrierung wurden daher die Fragen internationalisierter Cyberresilienz theoretisch eingebettet. Vor diesem Hintergrund ließen sich Konturen eines Rechts der Cyberresilienz von Seehäfen aufzeigen. Diese Konturen umfassen erstens eine institutionalisierte Abstimmung im jeweiligen Seehafen, um eine Gesamtrisikoanalyse zu ermöglichen, zweitens das Bedürfnis, selbstregulative transnationale Standards in das Recht einzubinden, sowie drittens transnationale Kommunikationsnetzwerke zwischen privaten und öffentlichen Akteuren zu fördern, wie insbesondere spezifische ISACs. Das nationale bzw. regionale Recht hat in diesem Regelungsgewirr die Aufgabe, selbstregulative Mechanismen anzuregen und zugleich im Sinne einer Vertrauensbildung zu unterstützen.

104 *Reiling*, Seeverwaltungsrecht, S. 346 f.

Die Gewährleistung maritimer Sicherheit und der Schutz maritimer kritischer Infrastruktur aus gesamtstrategischer Perspektive

Moritz Brake[*]

Das Maritime und die maritime Sicherheit sind von zentraler Bedeutung für Deutschlands Souveränität und rücken aus guten Gründen stärker in den Fokus der gesamtstrategischen Betrachtung. Deutschland wird sich dabei immer mehr bewusst, dass maritime Interessen auch im 21. Jahrhundert immer noch Gegenstand rivalisierender globaler Machtpolitik sind. Die bereits erfolgten Sabotageakte an marKRITIS, aktuelle Angriffe auf Handelsschiffe sowie zunehmende maritime Ressourcenkonflikte von Fischerei bis zur Ausbeutung von Öl- und Gasvorkommen verdeutlichen dabei, dass sich maritime Sicherheit nicht nur in Unfallverhütung, Umweltschutz oder Ordnungsfunktionen gegen Kriminalität erschöpft. Gleichzeitig gibt es große Lücken in der maritimen Resilienz und Sicherheitsarchitektur der Bundesrepublik, um mit den gegenwärtigen Herausforderungen umzugehen – vor allem im Hinblick auf hybride Bedrohungen.

Dieser Beitrag verfolgt daher das Ziel, die Bedeutung maritimer Sicherheit für die Gesamtstrategie Deutschlands aufzuzeigen. Ein besonderes Augenmerk liegt auf dem Schutz von marKRITIS. Diese Auseinandersetzung mit der gesamtstrategischen Bedeutung maritimer Sicherheit ist dabei von besonderem Wert für Deutschland. Sie hilft, die Bedeutung maritimer Interessen in einen größeren Kontext gesamtgesellschaftlicher Relevanz zu stellen. Nicht zuletzt bietet das Maritime aber auch seit jeher ein politisches „Experimentierfeld", auf dem vieles leichter und früher zur Umsetzung kommt, was an Land – in Sichtweite der meisten Menschen – größere innen- und außenpolitische Widerstände mit sich bringt.

* Dr. Moritz Brake ist Senior Fellow am Center for Advanced Security, Strategic and Integration Studies (CASSIS) der Rheinischen Friedrich-Wilhelms-Universität Bonn. Sein Forschungsschwerpunkt ist maritime Sicherheit und Strategie. Er ist außerdem Mitgründer und Geschäftsführer der Firma Nexmaris GmbH und Reserveoffizier der Deutschen Marine. Mailadresse: mbrake@uni-bonn.de Stand des Beitrags: 05. Januar 2025.

Im Zusammenhang mit maritimer Sicherheit können möglicherweise auch leichter politische Hürden übersprungen werden, die anderweitig eine gesamtstrategische Zusammenführung ziviler und militärischer Informationsquellen und Einsatzmittel erschweren. Um integrierte Sicherheit in der Praxis zu erreichen, bietet der maritime Kontext deshalb ein wertvolles Experimentierfeld zur Weiterentwicklung der gesamtstrategischen Handlungsfähigkeit Deutschlands in der Zeitenwende. Letztlich erfordern die internationale Verantwortung und eigenen Interessen, dass maritime Sicherheit umfassend und global gedacht wird.

A. Einleitung

Das Maritime und maritime Sicherheit sind von zentraler Bedeutung für Deutschlands Souveränität und rücken aus guten Gründen stärker in den Fokus der gesamtstrategischen Betrachtung. Mit den Umbrüchen, die vom ehemaligen Bundeskanzler Scholz als „Zeitenwende" bezeichnet wurden,[1] gehen auch Konsequenzen für die maritimen Existenzgrundlagen der Bundesrepublik, die Globalisierung und das bisherige System des international vernetzten Seehandels einher. Sabotageakte an maritimer kritischer Infrastruktur (marKRITIS), wie im September 2022 an den Nordstream Pipelines, im Oktober 2023 an Telekommunikationskabeln und einer Gaspipeline zwischen Estland, Finnland und Schweden, weiteren – allem Anschein nach mutwillig – mit Handelsschiffen verursachten Schäden an Daten- und Stromkabeln im November und Dezember 2024 in der Ostsee,[2] sowie die

1 *Scholz*, Zeitenwende Rede, Regierungserklärung von Bundeskanzler Olaf Scholz, 27.02.2022.

2 Verursacher, bzw. unter dringendem Verdacht stehende Handelsschiffe jeweils mit Verbindung zu, bzw. Flagge Chinas (Hong-Kong, 08.10.2023; China, 18.11.2024) und/oder Russland (Eigner der Schiffe und russische Besatzungsmitglieder (18.11.2024; 25.12.2024). Vgl. das Ergebnis der Recherche eines investigativjournalistischen Konsortiums aus dem September 2024, u.A. eingeflossen in den NDR-Beitrag, „Putins Flotte: Russische Spionage in der Ostsee", 24.09.2024, zuletzt eingesehen am 05.01.2025, unter: https://www.ndr.de/nachrichten/info/Russische-Spionageschiffe-in-der-Ostsee-Teil-der-hybriden-Angriffe,spionageschiffe102.html; jüngere Vorfälle, *Tagesschau*, „Datenkabel zwischen Deutschland und Finnland defekt", 18.11.2024, zuletzt eingesehen am 05.02.2024, unter: https://www.tagesschau.de/ausland/europa/finnland-deutschland-datenkabel-100.html; *Handelsblatt*, „Estlink 2: Finnische Ermittler – Kilometerlange Spur am Meeresboden", 29.12.2024, zuletzt eingesehen am 05.02.2024 unter: https://www.handelsblatt.com/politik/international/estlink-2-finnische-ermittler-kilometerlange-spur-am-meeresboden/100097510.html

Angriffe der jemenitischen Houthi-Rebellen auf die Handelsschifffahrt im Roten Meer, zeigen, wie leicht Deutschland und Europa auf dem Meer in ihren wirtschaftlichen und gesellschaftlichen Lebensgrundlagen verwundbar sind.

Deutschland wird sich immer mehr bewusst, dass maritime Interessen auch im 21. Jahrhundert immer noch Gegenstand rivalisierender globaler Machtpolitik sind. Die bereits erfolgten Sabotageakte an marKRITIS, aktuelle Angriffe auf Handelsschiffe sowie zunehmende maritime Ressourcenkonflikte von Fischerei bis zur Ausbeutung von Öl- und Gas-Vorkommen verdeutlichen dabei, dass sich maritime Sicherheit nicht nur in Unfallverhütung, Umweltschutz oder Ordnungsfunktionen gegen Kriminalität erschöpft. Was vor wenigen Jahren noch abstrakte Szenarien waren, denen außerhalb von Expertenkreisen keine besondere Aufmerksamkeit geschenkt wurde, sind heute reale Gefahren mit beträchtlichem potenziellem Schadensausmaß. Hybride Angriffe auf maritime Interessen sind längst glaubwürdige Drohkulissen, die schwerwiegende Ausfälle erzeugen können und strategisches Erpressungspotenzial bieten.

Gleichzeitig gibt es große Lücken in der maritimen Resilienz und Sicherheitsarchitektur der Bundesrepublik, um mit den gegenwärtigen Herausforderungen umzugehen – vor allem im Hinblick auf hybride Bedrohungen. Schon vor zehn Jahren, zu Zeiten ihres Schwerpunkts auf maritimer Terrorismus- und Kriminalitätsbekämpfung, wurde die maritime Gefahrenabwehr Deutschlands als lückenhaft bewertet.[3] Zusätzlich zur fehlenden klaren Führungsverantwortung gilt das gesamte System an Zuständigkeiten und beteiligten Akteuren als „außerordentlich kompliziert".[4] Außerdem fehlt es an strategisch geplanten Redundanzen, um Störungen in den maritimen Versorgungsgrundlagen aufzufangen, sowie an einem integrierten

3 Vgl. Positionspapier zur Schaffung einer „Deutschen Küstenwache", Unterzeichner: Schutzgemeinschaft Deutsche Nordseeküste e.V. V., Insel und Hallig Konferenz, Nautischer Verein Wilhelmshaven Jade e.V., Nautischer Verein Nordfriesland e.V., Nautischer Verein Lübeck e.V., Nautischer Verein Neustadt in Holstein e.V., Nautischer Verein Rostock e.V., Nautischer Verein zu Kiel e.V., 2017.

4 Patricia Schneider kommt in zwei Studien mit zehn Jahren Abstand zu einem jeweils ernüchternden Urteil. *Schneider*, Staatliche Strukturen Deutschlands zur Abwehr von maritimem Terrorismus, in *Ehrhart/Petretto/Schneider/Blecker/Engerer/Koenig* (Hrsg.), Piraterie und maritimer Terrorismus als Herausforderung für die Seehandelssicherheit Deutschlands, Nomos, 2013, S. 227; *Schneider*, Maritime Terrorism and Piracy: The Development of Maritime Security and its Governance, Habilitationsschrift übermittelt an die Fakultät für Wirtschafts- und Sozialwissenschaften der Universität Hamburg, 2023, S. 185.

globalen Lagebild unter Berücksichtigung sich abzeichnender Trends und Abhängigkeiten, um Chancen und Risiken frühzeitig zu erkennen.[5] Über alle staatlichen Akteure hinweg mangelt es an Mitteln für Überwachung, Präsenz und Gegenmaßnahmen, während für den Einsatz der Marine gegen nicht eindeutig militärische Bedrohungen auch die klare Rechtsgrundlage fehlt.[6] Die „Zeitenwende" mit hybriden Bedrohungen durch feindliche Machtpolitik bringt daher die vernachlässigten und reformbedürftigen Strukturen maritimer Sicherheit in Deutschland an ihre Grenzen.

Dieser Beitrag verfolgt das Ziel, die Bedeutung maritimer Sicherheit für die Gesamtstrategie Deutschlands aufzuzeigen. Ein besonderes Augenmerk liegt dabei auf dem Schutz von marKRITIS. Die hiesige Entwicklung der öffentlichen und politischen Wahrnehmung der strategischen Bedeutung des Maritimen und der maritimen Sicherheit wird dabei anhand der jüngeren Einsatzgeschichte der Deutschen Marine und der begleitenden politischen Debatte hergeleitet. Auf eine Beschreibung des Hintergrundes zur Bedeutung maritimer Sicherheit nach der „Zeitenwende" folgt eine Erklärung des Begriffes „Gesamtstrategie", bevor über die Einsätze der Marine die Entwicklung des politischen Stellenwertes maritimer Sicherheit in Deutschland aufgezeigt wird. Abschließend wird die maritime Sicherheitsarchitektur Deutschlands zum Schutz maritimer kritischer Infrastruktur im Kontext gesamtstrategischer Verantwortung für maritime Sicherheit der Bundesrepublik näher betrachtet.

Der Auseinandersetzung mit der gesamtstrategischen Bedeutung maritimer Sicherheit ist dabei von besonderem Wert für Deutschland. Diese Perspektive hilft, die Bedeutung maritimer Interessen in einen größeren Kontext gesamtgesellschaftlicher Relevanz zu stellen. Zusätzlich eröffnet der Blick auf den Entwicklungsprozess, der hinter dem gewachsenen weltpolitischen und maritimen Bewusstsein der Bundesrepublik steht, ein besseres Verständnis für Herausforderungen und Chancen bei der Lösung erkannter Probleme.

Nicht zuletzt bietet das Maritime aber auch seit jeher ein politisches „Experimentierfeld", auf dem vieles leichter und früher zur Umsetzung kommt, was an Land – in Sichtweite der meisten Menschen – größere in-

5 Vgl. *Baldauf, Brake, Finger* (et.al.), Gutachten zur Maritimen Souveränität in der Zeitenwende, Bundesamt für Seeschifffahrt und Hydrographie, Hamburg, 2024, S. 11-12.

6 Vgl. *Ehlers*, Rechtlicher Schutz von Einrichtungen aus See (in diesem Band), S. 29 ff.; *Walter*, Der Schutz der maritimen Kritischen Infrastruktur nach den Anschlägen auf die Nord-Stream-Pipelines, NordÖR 2023, S. 304-305.

nen- und außenpolitische Widerstände mit sich bringt. Historisch betrachtet überwinden sich Staaten auf See leichter, mit Rivalen zu kooperieren, kommen aber auch mit aggressiven Maßnahmen durch, die ihnen anderweitig zum Nachteil hätten werden können.[7] In den drei Jahrzehnten seit Ende des Kalten Krieges bot die Marine beispielsweise eine mit geringeren innenpolitischen Widerständen und Risiken versehene Möglichkeit, sich an internationalen militärischen Einsätzen zu beteiligen, als dies mit Heer oder Luftwaffe der Fall war.[8]

„Alles, was schwimmt, geht" lautet ein Bonmot, das dem früheren Außenminister Genscher zugeschrieben wird.[9] Es trifft – wie in seinem ursprünglichen Zusammenhang – nicht nur auf geringere Schwierigkeiten bei anderweitig restriktiv gehandhabten Waffenexporten zu, sondern auch bei der politischen Bereitschaft, die Marine als Instrument der Außenpolitik einzusetzen.[10] So könnten auch im Zusammenhang mit maritimer Sicherheit möglicherweise leichter politische Hürden übersprungen werden, die anderweitig eine gesamtstrategische Zusammenführung ziviler und militärischer Informationsquellen und Einsatzmittel erschweren.

B. Die Bedeutung maritimer Sicherheit nach der Zeitenwende

Maritime Sicherheit ist das Fundament der modernen globalisierten Weltwirtschaft – und damit unverzichtbar für Deutschlands und Europas Sicherheit, Wohlstand und Souveränität. In einer Welt, in der über 90% des Warenverkehrs über Seewege verläuft, 95% des weltweiten Datenverkehrs Kabel auf dem Meeresgrund durchströmt, ein stetig wachsender Anteil der Energieversorgung nicht nur über das Meer geliefert, sondern auch dort erzeugt wird, ein erheblicher Teil der globalen menschlichen Ernährungsgrundlage aus dem Meer stammt und das gesamte Ökosystem des Planeten von intakten Ozeanen abhängt,[11] ist die Gewährleistung maritimer

7 Vgl. *Cable*, Gunboat Diplomacy: 1919 - 1991 (3rd ed.); Palgrave MacMillan, 1994, S. 97.
8 Vgl. *Brake*, The Contemporary German Navy as an Instrument of Foreign Policy; Springer VS, Wiesbaden, 2024, S. 287-288.
9 Zitiert in *Brake* (Fn. 8), S. 288.
10 *Brake* (Fn. 8), S. 288-289.
11 Ergänzend dazu: ca. 15% des weltweiten Bedarfs an tierischem Protein in der menschlichen Ernährung wird aus dem Meer gedeckt; möglicherweise bis zu 80% des Sauerstoffs in der Atmosphäre wird durch Meeresorganismen erzeugt. Vgl. *World Ocean Review*, The Ocean, Guarantor of Life – Sustainable Use, Effective

Sicherheit ein zentrales Element der gesamtstrategischen Verantwortung moderner Staaten.

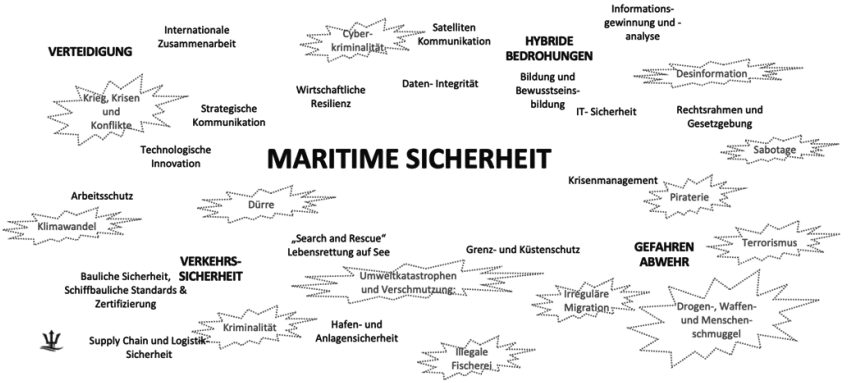

Abb. 1: Eine große Bandbreite von Unterthemen, Risiken und Aufgaben fallen gemeinhin unter ‚Maritime Sicherheit' (Quelle: Moritz Brake & Bertrand Mignot)

Grundsätzlich ist „Maritime Sicherheit" ein vager Begriff, für den es keine allgemeingültige Definition gibt. Die Bedeutung von „Sicherheit" im Deutschen umfasst im Englischen sowohl „safety" (Unfallverhütung, Arbeitssicherheit) als auch „security" (Gefahrenabwehr). Dieses schon sprachlich angelegte breitere Verständnis von „maritimer Sicherheit" hilft, die Komplexität des Themas zu erfassen. Maritime Sicherheit umfasst eine Vielzahl von Elementen, Bedrohungen und möglichen Akteuren oder Maßnahmen (siehe Abb. 1). Diese Elemente sind miteinander vernetzt und nicht trennscharf zu kategorisieren, dennoch lassen sie sich grob zuordnen zu den Bereichen „Verkehrssicherheit", „Gefahrenabwehr", „hybride Bedrohungen" und „Verteidigung". Die Schreibweise von „Maritimer Sicherheit" mit zwei Großbuchstaben – und die implizite Bedeutung dahinter – wird von Geoffrey Till als „Rezept für Verwirrung" angesehen, der im Allgemeinen

Protection, maribus, 2021, S. 14-7; 80; je nach Rechnung verläuft 80 %-90 % des Weltwarenverkehrs über maritime Transportwege, vgl. *Rodrigue & Notteboom*, Maritime Shipping and International Trade. In *Notteboom, Pallis & Rodrigue* (Hrsg.), Port Economics, Management and Policy, Routledge, 2022; zu Daten bzgl. Unterwasser-Kabeln vgl. *Morcos & Wall*, Invisible and Vital: Undersea Cables and Transatlantic Security, www.csis.org. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security, 2021, abgerufen am 15.03.2024.

die ältere Bezeichnung „gute Ordnung auf See" (good order at sea) für das bevorzugt, was sie als gewünschten Endzustand oder eine Reihe von Aufgaben für z.B. Seestreitkräfte beschreibt.[12]

Für die Bundesrepublik ist maritime Sicherheit, abgeleitet auch aus ihrem umfassenden Verständnis von integrierter Sicherheit,[13] mehr als nur ein Synonym für Ordnungsfunktionen oder maritime Kriminalitätsbekämpfung. Sie ist eine gesamtstaatliche Aufgabe und umfasst das ganze Spektrum an potenziellen Bedrohungen für die Gesamtheit der maritimen Lebensgrundlagen moderner Gesellschaften. Damit schließt dies den Schutz der Meeresumwelt und Meeresnutzung vor militärischen und nichtmilitärischen Bedrohungen (Kriminalität, Terrorismus, Schmuggel von Menschen, Waffen oder Drogen, illegale Fischerei) ein. Im internationalen Vergleich wird allerdings unter „Maritimer Sicherheit" sehr Unterschiedliches verstanden. Für die US Navy beispielsweise bezeichnet maritime Sicherheit (maritime security) die Kriminalitätsbekämpfung auf See.[14] Damit grenzt sie „maritime security" von „warfighting", der Kriegführung und Abschreckung etwaiger Gegner als Marineaufgabe, ab.

Die Bedeutung des Maritimen ist an Land oft erklärungsbedürftig, dennoch ist maritime Sicherheit für das als drittgrößte Volkswirtschaft tief in der Globalisierung verankerte Deutschland Teil der wirtschaftlichen und gesellschaftlichen Existenzgrundlage. Dabei befindet sich die traditionell kontinental geprägte Bundesrepublik vor allem seit der Wiedervereinigung und dem Ende des Kalten Krieges in einem steten weltpolitischen Lernprozess – ein Lernprozess mit starker maritimer Dimension: Nicht nur wurde Deutschland immer europäischer und weltgewandter, vor allem aber wurde es auch – selbst von vielen Deutschen unbemerkt – im Zuge wirtschaftlicher Globalisierung und gestiegener außenpolitischer Verantwortung immer maritimer.[15] Andere Staaten, deren maritimes Bewusstsein stärker ausgeprägt ist, sehen die Nutzung der Meere und den Schutz des Seehandels seit Jahrhunderten ganz selbstverständlich als vitale nationale Interessen.[16]

12 *Till*, Seapower, A Guide for the 21st Century (3rd ed.), Routledge, 2023, S. 25.
13 Vgl. *Bundesregierung*, nationale Sicherheitsstrategie, 2023, Vorwort von Außenministerin Baerbock, S. 11.
14 Vgl. *US Secretary of the Navy,* Advantage at Sea. 2020 US Naval Strategy, Arlington County, VA, 2020, S. 3.
15 Vgl. *Brake* (Fn. 8), S. 101-104.
16 Für ein einschlägiges US-amerikanisches Beispiel, vgl. *Stavridis,* Sea Power – The History and Geopolitics of the World's Oceans, Penguin, New York, 2017, S. 314-316.

I. Ein aufgeklärtes Verständnis von Sicherheit als Grundlage maritimer Sicherheit

Ein aufgeklärtes Verständnis von maritimer Sicherheit beschreibt nicht einfach die Abwehr von Gefahren für den Seehandel, sondern die Gewährleistung der umfassenden maritimen Beiträge zu menschlicher und gesellschaftlicher Entwicklung. In Übereinstimmung mit einem an Menschenwürde ausgerichteten Verständnis von Sicherheit und staatlicher Verantwortung,[17] müssen alle mit dem Meer verbundenen Beiträge zu menschlicher und gesellschaftlicher Entwicklung betrachtet, geschützt und gefördert werden. Dabei ist auch die ganze Bandbreite staatlicher Handlungsfähigkeit – der vollständige politische, wirtschaftliche und gesellschaftliche „Instrumentenkasten" – in einem gesamtstrategischen Ansatz aus „*hard*" und „*soft power*" gefordert.[18]

Die globalisierte Weltwirtschaft des 21. Jahrhunderts fußt auf einem internationalen System des Seehandels, das außerhalb der unmittelbaren Kontrolle einzelner Staaten liegt und in dem multilateral organisierte Seemacht maritime Sicherheit gewährleistet – nicht zuletzt auch mit Ordnungsfunktionen zur Kriminalitätsbekämpfung.[19] Allerdings entwickelte sich parallel mit China wieder eine bedeutende national ausgerichtete Seemacht, die dieses internationale System in Frage stellt und mit machtpolitischer Zielsetzung herausfordert.[20] Ohne Seehandel funktioniert keine moderne Wirtschaft, auch und insbesondere die chinesische nicht. Allerdings verfügt China heute immer mehr über die Werkzeuge, um seine eigene Abhängigkeit von diesem internationalen System zu reduzieren. Gleichzeitig kann es selbst auf verschiedene Weise Einfluss auf die Weltpolitik und einzelne Staaten nehmen. Chinas Seemacht ist ein wesentlicher Baustein zur Freiheit von externer Einflussnahme, beispielsweise in Gestalt von

17 Vgl. „human security", wie sie 1994 durch die Vereinten Nationen eingeführt wurde, *United Nations Development Programme* (UNDP) Human Development Report 1994, Oxford University Press, Oxford, 1994, S. 22-24.

18 Vgl. „smart power" *Nye*, Soft Power. The Means To Success in World Politics, Public Affairs: New York, 2004, S. 32.

19 Vgl. Tills Konzept der „post-modern navy", allerdings treffender als „cosmopolitan navy" zu bezeichnen; *Till* (Fn. 12), S. 35, *Brake* (Fn. 8), S. 33-36; im Kontext deutscher Außenpolitik und Marine, S. 55, 253, 279.

20 China als „systemischer Rivale" und Herausforderer der bestehenden internationalen Ordnung, vgl. *Europäische Union* (EU), A Strategic Compass for Security and Defence, 2022, S. 17-18; *North Atlantic Treaty Organisation* (NATO), Strategic Concept, 2022, S. 4-5; *Bundesregierung* (Fn. 13), S. 11-12.

drohenden Sanktionen als Antwort auf eine militärische Eskalation der Taiwan-Frage.

Geopolitische Spannungen stehen als eigenständige Bedrohung auch in Wechselwirkung mit dem sich verschärfenden Klimawandel und der Notwendigkeit zur globalen nachhaltigen, gerechten Meeresnutzung – Ocean Governance.[21] Paramilitärische staatliche chinesische Fischereiflotten bedrohen die Fischbestände und Ernährungsgrundlage vieler Küstenregionen.[22] Daher hat die US Navy Ocean Governance längst als Bereich des geopolitischen Wettbewerbs identifiziert.[23] Bei aller systemischer Rivalität beuten auch einfache Kriminelle die Ressourcen aus, nutzen vielfältige Akteure Grauzonen, Rechtslücken und fehlende Durchsetzung bereits bestehender Abkommen. So leidet unter mangelndem internationalem Einsatz für den Schutz des Ozeans ultimativ sein Beitrag zu den Lebensgrundlagen der Menschen.

II. Maritime Sicherheit und disruptive Technologien

Mit der „Zeitenwende" hat sich nicht nur politisch die Bedrohungslage verändert, für die Gewährleistung maritimer Sicherheit zeigt sich außerdem, dass sowohl „künstliche Intelligenz" (KI) als auch ferngelenkte und (teil)autonome Systeme zunehmend zum Einsatz kommen. Diese Technologien erweisen sich auch hier als „disruptiv", sie führen zu Umbrüchen im Denken und Handeln, da sie bisherige Machtverhältnisse im maritimen Kontext erschüttern können. Mit einfachen, kostengünstigen Mitteln gelang es einer maritim militärisch unterlegenen Ukraine, der russischen Marine schwere Verluste zuzufügen. Ebenso gelingt es den jemenitischen Houthi-Rebellen, über Monate erfolgreich Handelsschiffe im Roten Meer zu attackieren, die internationalen und regionalen Handelsströme empfindlich zu treffen und eine sehr ressourcenintensive internationale Kriegsschiffpräsenz zu binden. Es ergeben sich durch disruptive Technologien neue taktische Vorteile im Kampf, für hybride Angriffe und kriminelle Unterfangen –

21 *EU* (Fn. 20), S. 2.
22 Vgl. *Analysis and Research Team European Council*, The EU: From Maritime Actor to Sea Power, Europäischer Rat, Brüssel, 2023, S. 9.
23 Vgl. *US Secretary of the Navy* (Fn. 14), S. 3.

aber auch den Umgang mit diesen Bedrohungen.[24] Eine große Zahl kleiner, kostengünstiger Angriffs- und Sensorplattformen, eröffnen neue Möglichkeiten, mit entgrenzten Konfliktschauplätzen, riesigen Datenmengen, sehr kurzen Reaktionszeiten und ihrem Einsatz auf der Seite möglicher Gegner umgehen zu können.

III. Die Gewährleistung maritimer Sicherheit als nationales und internationales Interesse

Aufgrund der besonderen Situation der weltpolitischen Lage nach der Wiedervereinigung konnte sich Deutschland zwar zum wirtschaftlich bedeutenden maritimen Akteur aufschwingen – zeitweilig mit der drittgrößten Handelsflotte der Welt und heute noch größten Containerschiffsflotte –,[25] ohne aber den im historischen Vergleich üblichen machtpolitischen Instrumentenkasten zu entwickeln.[26] Mit seinem zunehmenden wirtschaftlichen Erfolg in der Globalisierung wurde Deutschland immer stärker abhängig von maritimer Sicherheit, ohne aber parallel die Mittel zu entwickeln, seine globalen maritimen Interessen eigenständig schützen zu können. Die Überzeugung der Jahre des Kalten Krieges, wonach die Seemächte unter seinen Alliierten, diese Aufgabe für Deutschland im Gegenzug für kontinentale Beiträge seiner Bundeswehr zu kollektiver Abschreckung übernehmen würden,[27] verlor im Zuge der militärischen Fähigkeitsverluste der „Friedensdividende" und geopolitischen Veränderungen in den letzten drei Jahrzehnten einen Großteil seiner Substanz. Darüber hinaus scheinen die USA als zentrale Seemacht im westlichen Bündnis nicht weiter bereit zu sein, die Interessen ihrer Verbündeten mit militärischen Mitteln abzusichern.

Im Gegensatz zu den EU-Mitgliedsstaaten, deren Marinen zahlenmäßig seit über dreißig Jahren schrumpfen, spielt sich in Asien ein durch China

24 Vgl. *Bossong/Rieks/Koch*, Künstliche Intelligenz für die Landesverteidigung, Gastbeitrag Frankfurter Allgemeine Zeitung, 02.02.2022.

25 Vgl. *Brake* (Fn. 8), S. 61-64; 2005-2010, drittgrößte Handelsflotte nach „beneficial ownership", Daten der United Nations Conference on Trade and Development (UNCTAD).

26 Die alte Logik, dass nationale Seemacht eigenen Seehandel erst ermögliche, war u.A. eine der Begründungen für die Flottenrüstung in Deutschland seit 1848, vgl. *Brake* (Fn. 8), S. 42, 296-297.

27 Vgl. *Bundesministerium der Verteidigung* (BMVg), Verteidigungspolitische Richtlinien, Bonn, 1992, Art. 8 Nr.3.

getriebener massiver maritimer Rüstungswettlauf ab.[28] Gemessen an der Zahl der Schiffe, allerdings (noch) nicht anhand der Feuerkraft, verfügt China über die größte Marine der Welt – größer als die Flotte der USA.[29] Gleichzeitig baute China zielgerichtet mit Staatskonzernen die weltgrößte Schiffbauindustrie, Fischereiflotte und Handelsflotte auf.[30] Eine machtpolitische Dimension dieser Entwicklungen ist nicht nur möglich, sondern bereits zu beobachten.

Russlands und Chinas Herausforderung der internationalen regelbasierten Ordnung und ihre eskalierende Rivalität mit den westlichen Demokratien hat eine zentrale maritime Dimension.[31] Dies wiegt besonders schwer, weil das Maritime von existentieller Bedeutung für die Souveränität Deutschlands und Europas ist, während diese maritimen Interessen gleichzeitig – vor allem mit den knappen verfügbaren Einsatzmitteln – in ihrer globalen Gesamtheit unmöglich zu verteidigen sind.[32] Nicht nur bestehen kriminelle Bedrohungen fort, machtpolitische Rivalität äußert sich längst im Einsatz staatlicher Ressourcen gegen maritime Versorgungswege.

Die durch Russland, den Iran – und zumindest indirekt – auch China unterstützten Houthi-Rebellen im Jemen zeigen, dass es mit verhältnismäßig einfachen Mitteln möglich ist, großen strategischen Effekt über Angriffe auf Handelsschiffe zu bewirken. Kostengünstige, leicht zu exportierende Drohnen und selbst schlagkräftigere Marschflugkörper können gewaltbereiten Akteuren an den unterschiedlichsten Orten zur Verfügung gestellt werden. Weit unterhalb der Schwelle zu einem offenen Krieg ist es über die Bewaffnung politisch-militärischer Stellvertreter sowie mit hybriden Methoden möglich, deutsche und europäische Interessen empfindlich auf dem Meer zu treffen.

---

28 Europa: vgl. *Stöhs*, The Evolution of European Naval Power 1989-2019: Strategy – Force Structure – Operations, Promotionsschrift, Christian-Albrechts-Universität zu Kiel, 2019, S. 432; Asien: vgl. Analysis and Research Team European Council (Fn. 22), S. 6.

29 Vgl. *Tangredi*, Bigger Fleets Win, US Naval Institute Proceedings, January 2023, Vol. 149/1/1,439.

30 Es gibt keinen Grund, aus strategischer Sicht Hongkong und China als separate Handelsflotten zu betrachten. Damit führt China die Statistik an, vgl. *United Nations Conference on Trade and Development* (UNCTAD), Review of Maritime Transport 2023, S. 34; Analysis and Research Team European Council (Fn. 22), S. 9.

31 Zu dieser Herausforderung und Rivalität, vgl. *Bundesregierung* (Fn. 13), S. 12.

32 Zu den Grenzen des Schutzes (maritimer) Infrastruktur, vgl. EU-NATO Task Force On The Resilience Of Critical Infrastructure, Final Assessment Report, 2023, S. 3.

Aber nicht erst mit den Angriffen der jemenitischen Houthi-Rebellen auf Handelsschiffe im Roten Meer zeigt sich, dass maritime Wirtschaft und globale Machtpolitik eng miteinander verwoben bleiben. Die traditionelle enge Wechselwirkung zwischen einer starken maritimen Wirtschaft und starken Seestreitkräften verlor auch in den letzten Jahrzehnten nicht ihre Gültigkeit – Seemacht wurde nur anders organisiert: Kollektiv und multilateral zahlten einige Nationen mit ihren Seestreitkräften, allen voran die USA, in die Sicherheit des globalen Handelssystems ein.[33] Der Zusammenhang zwischen Wirtschaftskraft und Seemacht[34] blieb im Zuge kooperativ multilateral organisierter maritimer Sicherheit und eines Seehandelssystems, in dem nationale Flaggen für Handelsschiffe vor allem „Geschäftsmodelle" zu sein schienen,[35] im 21. Jahrhundert außerhalb von Expertenzirkeln in Deutschland weitgehend unbeachtet.

Bei der beabsichtigten Stärkung der strategischen Handlungsfähigkeit der Europäischen Union (EU) ist maritime Souveränität – Seemacht – ein entscheidendes Element. Die EU zu einem „geopolitischen Akteur" zu entwickeln, ist u.A. ein Ziel der Nationalen Sicherheitsstrategie (NSS) Deutschlands.[36] Die Bedeutung von Seemacht dabei wird aber bisher vor allem in Frankreich diskutiert,[37] findet sich aber auch in einem Forschungspapier aus dem vergangenen Jahr des wissenschaftlichen Dienstes des Europäischen Rats, das aufzeigt, dass sich die EU zur Stärkung ihrer strategischen Handlungsfähigkeit von einem „maritimen Akteur" zur „Seemacht" entwickeln müsse.[38]

Letztlich macht die Natur der globalisierten Weltwirtschaft und des modernen Seehandels den Schutz des ganzen internationalen maritimen Systems zum aufgeklärten Eigeninteresse und zur gemeinschaftlichen Verantwortung eines jeden Staates. Menschen – auch fern der Küste – können nicht auf ihre maritimen Lebensgrundlagen verzichten, keine moderne Wirtschaft kommt ohne maritime Sicherheit, ohne Zugang zum Weltmarkt

33 Vgl. Konzept der „1000-Ship-Navy", sowie die Beiträge auch der Deutschen Marine in ihren vergangenen über 30 Jahren Einsatzgeschichte seit 1990, *Rahman*, Evolving U.S. Framework for Global Maritime Security from 9/11 to the 1000-ship Navy, in *Herbert-Burns, Bateman & Lehr* (Hrsg.), Lloyd's MIU Handbook of Maritime Security, (S. 39-51) CRC Press Taylor and Francis, 2009, S. 40; *Brake* (Fn. 8), S. 281-28.

34 Vgl. *Till* (Fn. 12), S. 17-21.

35 Vgl. *Till* (Fn. 12), S. 35; *Brake* (Fn. 8), S. 33-36, 253-256.

36 *Bundesregierung* (Fn. 13), S. 13.

37 Vgl. Centre d'études stratégiques de la Marine (CESM), Europe, cooperating for a naval ambition, Etudes Marines n°21 (english version), 2022.

38 Vgl. Analysis and Research Team European Council (Fn. 22).

aus – und dieser Zugang erfolgt über das Meer. Wer die eigene Wirtschaft und Versorgung der Bevölkerung sichern will, muss dies im Verbund mit anderen Staaten und im Einsatz für das Gesamtsystem tun. Zumindest gilt dies für alle Staaten, die die internationale Ordnung, ihre wirtschaftliche Leistungsfähigkeit und Vernetzung nicht riskieren wollen.

C. Gesamtstrategie

„Gesamtstrategie" ist der deutsche Begriff für das, was im Englischen „grand strategy" genannt wird. Helmut Schmidt verwendete ihn und verstand darunter das Zusammenführen sämtlicher gesellschaftlich relevanter Informationen und politischen Handlungsmöglichkeiten zur Erreichung übergeordneter Ziele.[39] Dabei ist Strategie die Kunst, „potenziell unbegrenzte Ziele, mit notwendigerweise begrenzten Mitteln in Einklang zu bringen."[40] Die gesamtstrategische Entscheidungsebene ist die jeweilige nationale Regierung eines Landes, analog – für nicht-staatliche Organisationen – die höchstmögliche Entscheidungsebene.

Teil- oder Ressortstrategien z.B. für die Verteidigungs-, Wirtschafts- oder Außenpolitik fügen sich in die Gesamtstrategie ein. Die letztendliche „operative" und „taktische" Umsetzung der Gesamtstrategie und ggf. mehrerer in einer Aufgabe zusammenwirkender Ressortstrategien erfolgt im Idealfall lokal mit rasch anpassungsfähiger dezentraler Entscheidungsbefugnis in Übereinstimmung und im Zusammenspiel mit den übergeordneten Zielsetzungen auf höchster Ebene.[41]

---

39 Wie Harald Kujat, sein früherer Mitarbeiter im Kanzleramt und spätere Generalinspekteur der Bundeswehr berichtete, zitiert in *Brake* (Fn. 8); zur englischen Entsprechung, „grand strategy: the orchestration and employment of any or all the assets of a security community (a wide, rather comprehensive list), including its military instruments, for political purposes", *Gray & Johnson,* The Practice of Strategy, in *Baylis, Wirtz & Gray* (Hrsg.), Strategy in the Contemporary World (4th ed., S. 358-376), Oxford University Press, Oxford, 2013, S. 364.

40 Vgl. *Gaddis*, On Grand Strategy (1st ed.) Penguin Press, 2018, S. 21.

41 In der Wissenschaft unterscheidet man i.d.R. zwischen Abstufungen strategischer Entscheidungsebenen: Gesamtstrategie, Ressortstrategien, operationsbezogen (z.B. für eine größere Teilaufgabe oder geographische Region) und der taktischen Umsetzungs-Ebene (militärisch, das einzelne Gefecht; zivil, z.B. konkretes Verwaltungshandeln oder Umsetzung einer unternehmerischen Entscheidung). Vgl. *Gray & Johnson* (Fn. 39), S. 359-360.

Als wichtigstes gesamtstrategisches Ziel von Staaten gilt die Gewährleistung nationaler Sicherheit. So drückt es auch der ehemalige Bundeskanzler Olaf Scholz für die Bundesrepublik in der NSS aus.[42] „Nationale Sicherheit" lässt sich dabei inhaltlich nur schwer eingrenzen. Die Kategorien umfassender menschlicher Sicherheit machen allerdings deutlich, dass hier auf Basis der Verwirklichung von Menschenwürde sehr breit gedacht werden muss. Wirtschaft, Ernährung, Gesundheit, Umwelt, Schutz von Individuen vor Gewalt, Schutz der Gemeinschaft (inkl. Ausdruck von Kultur, Religion) und politische Freiheiten (inkl. aktivem und passivem Wahlrecht, Presse-, Versammlungs-, Religions- und Meinungsfreiheit)[43] gehören dazu. Grundsätzlich muss in die gesamtstrategische Betrachtung nationaler Sicherheit nicht nur das physische menschliche Überleben und das Funktionieren staatlicher Institutionen, sondern die Gesamtheit der Lebensgrundlagen moderner Gesellschaften einfließen.

In der politischen Praxis kann man sich der Bedeutung konkreter Themen für „Nationale Sicherheit" gut über das Konzept der „Versicherheitlichung" annähern.[44] Entwickelt zur Analyse politischer Kommunikationsprozesse bietet es die Möglichkeit zur Unterscheidung zwischen *Themen allgemeinen Interesses* (z.B. der Wassertemperatur an den Badestränden deutscher Küstenorte), *politischen Interesses* (Diskussionsthemen in Wahlkämpfen, Parlamenten und an Kabinettstischen; z.B. der Klimawandel und die Energiewende) und *sicherheitsrelevanten Themen* (außerordentliche Maßnahmen werden möglich, inklusive des Einsatzes der Streitkräfte, z.B. beim Schutz von marKRITIS).[45]

Grundsätzlich kann jegliches Thema von gesellschaftlicher Relevanz in den Fokus gesamtstrategischer Betrachtung und Maßnahmen rücken – je nach kritischer Bedeutung und Bedrohungswahrnehmung. Anpassungsfähigkeit ist auch hier ein Merkmal von Resilienz, von Wettbewerbsfähigkeit: Je besser ein System oder eine Organisation auf Veränderungen in Relevanz und Bedrohung reagieren kann, je besser ist seine strategische Handlungsfähigkeit. Auf gesamtstrategischer Ebene muss deshalb eine möglichst große Bandbreite an Themen erfasst und ein möglichst flexibel einsetzbarer politischer Instrumentenkasten entwickelt werden, um bei Veränderungen

42 Scholz in *Bundesregierung* (Fn. 13), S. 5.
43 UNDP (Fn. 17), S. 22-24.
44 „Securitization", *Buzan/Waever/de Wilde*, Security: A New Framework for Analysis. Lynne Rienner, Boulder, 1998, S. 26-27.
45 *Buzan, Waever & de Wilde* (Fn. 44), S. 26-27.

rasch mit gesteigerter Aufmerksamkeit und geeigneten Maßnahmen reagieren zu können.

Handlungsfähigkeit, Macht, Souveränität sind die Grundlage für die Umsetzung jeglicher Strategie. Im innerstaatlichen Kontext beschreibt Souveränität die „Letztentscheidungsbefugnis über Personen und Sachen auf dem staatlichen Hoheitsgebiet", international die „Befehlsunabhängigkeit von anderen Staaten".[46] Macht, so wie Max Weber sie definierte, „bedeutet jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht.[47] Somit hängt Souveränität von der glaubwürdigen Fähigkeit ab, mit der Kombination aus unterschiedlichen Mitteln der „soft" und „hard power", Interessen und Werte notfalls „auch gegen Widerstreben", im Idealfall aber multilateral und kooperativ durchsetzen zu können.[48]

Maritime Sicherheit ist bei traditionellen Seemächten selbstverständlicher Teil nationaler Sicherheit und wird als solcher auch in Deutschland im politischen und gesellschaftlichen Diskurs zunehmend wahrgenommen. Zwar konnte es noch im Jahr 2010 gelingen, mit innenpolitischem Kalkül einen Bundespräsidenten mit dem Vorwurf der „Kanonenbootdiplomatie" aus dem Amt zu treiben, der den Schutz von Seewegen als militärische Aufgabe bezeichnete.[49] Allerdings war diese Aufgabe für Streitkräfte damals schon seit Jahren Teil offizieller strategischer Dokumente der Bundesregierung und die Empörung der Opposition fand in Bundespräsident Horst Köhler lediglich ein offenbar günstiges Ziel.[50]

Die direkte Verknüpfung von vitalen wirtschaftlichen und gesellschaftlichen Interessen mit dem Meer, Zugang zum Weltmarkt über ungehinderten internationalen Seeverkehr, die Nutzung maritimer Ressourcenquellen und die Bedeutung des Ozeans als Ökosystem für das Überleben der

46 *Wissenschaftlicher Dienst des Bundestages*, Zum Begriff der Souveränität und zur Übertragung von Hoheitsrechten, Deutscher Bundestag, WD 3 - 3000 - 124/23, Berlin, 2023, S. 4.

47 *Weber*, Wirtschaft und Gesellschaft – Grundriss der verstehenden Soziologie, 5. Auflage, Herausgegeben von Johannes Winkelmann, Mohr Verlag, Tübingen, 1985, S. 28.

48 Macht als wechselseitige Beziehung, als System von Glaubwürdigkeit und Netzwerk gegenseitiger Anerkennung; vgl. *Foucault*, Überwachen und Strafen – die Geburt des Gefängnisses, (1. Deutsche Taschenbuchauflage des Textes von 1974), Suhrkamp, Frankfurt a.M., 1994, S. 38; zur Nutzung der Kombination aus „hard" und „soft power": „smart power", vgl. *Nye* (Fn. 18), S. 32.

49 *Köhler*, Interview Deutschlandradio, 22.05.2010; „Kanonenbootdiplomatie" wurde ihm daraufhin von Jürgen Trittin im Bundestag vorgeworfen, vgl. *Brake* (Fn. 8).

50 *BMVg*, Weißbuch 2006, S. 95-96; vgl. *Brake* (Fn. 8).

Menschheit kommt seit Jahrzehnten mit zunehmendem Stellenwert, größerer Selbstverständlichkeit und Prominenz zum Ausdruck.[51] Beachtenswert ist im Sinne der „Versicherheitlichungs"-Theorie auch, dass die Deutsche Marine seit Ende des Kalten Krieges in wachsender Bandbreite und operativer Intensität (mit sog. robusten Mandaten zum Waffeneinsatz) zu Aufgaben im Rahmen der Gewährleistung maritimer Sicherheit zum Einsatz kommt.[52]

Nicht zuletzt auch die Anträge „Maritime Souveränität" der Regierungsfraktionen im Bundestag, SPD, Grüne und FDP, sowie „Zukunft der maritimen Wirtschaft sichern" der CDU/CSU Fraktion (beide vom 04.07.2023) unterstreichen die hohe Bedeutung, die das Maritime mittlerweile im politischen Diskurs erreicht hat.[53] Nationale Souveränität steht dort in direktem Zusammenhang mit glaubwürdiger maritimer Handlungsfähigkeit – oder, wie es im Englischen leichter über die Lippen ginge: mit Seemacht.[54] So deckt sich das für Deutschland geforderte Streben nach „Maritimer Souveränität" mit dem, was für die EU als die Notwendigkeit zur Entwicklung vom bloßen (kommerziellen) „maritimen Akteur" zur umfassend handlungsfähigen Seemacht in einem Bericht für den Europäischen Rat beschrieben wurde.[55]

Nach dem durch die Regierungsfraktionen formulierten Verständnis von maritimer Souveränität umfasst diese vier Dimensionen: Resilienz und Unabhängigkeit, Wettbewerbsfähigkeit und Finanzierung, sozial-ökologische Transformation sowie maritime Infrastrukturen.[56] In allen vieren ist ge-

51 Vgl. *BMVg* (Fn. 27); *Bundesregierung*, Maritime Agenda 2025 – die Zukunft des maritimen Wirtschaftsstandortes Deutschland, Berlin, 2017; *Bundesregierung*, Nationale Strategie für die nachhaltige Nutzung und den Schutz der Meere, Berlin, 2008; *Vertragsgesetz Seerechtsübereinkommen*, 1994.

52 Vgl. *Brake* (Fn. 8), S. 278-284.

53 *Fraktion BÜNDNIS 90/DIE GRÜNEN, Fraktion der FDP, Fraktion der SPD*, Antrag „Maritime Souveränität in der Zeitenwende", Deutscher Bundestag, BT-Drucksache 20/7571, Berlin, 2023; *Fraktion CDU/CSU*, Antrag „Zukunft der maritimen Wirtschaft sichern", Deutscher Bundestag, BT-Drucksache 20/7582, Berlin 2023.

54 Das Wort „Seemacht" wird im Antrag nicht verwendet und ist im politischen Diskurs in Deutschland nicht gebräuchlich. Es könnte aber im Zuge der bereits erfolgten „Rehabilitierung" des Begriffes „Geopolitik" (z.B. in der NSS), eine ähnliche Entwicklung erleben.

55 Titel einer aktuellen Studie des wissenschaftlichen Dienstes des Europäischen Rats; Analysis and Research Team European Council (Fn. 22).

56 *Fraktion BÜNDNIS 90/DIE GRÜNEN, Fraktion der FDP, Fraktion der SPD* (Fn. 53), S. 1.

samtstaatliches, ressortübergreifendes Handeln erforderlich.[57] Dies umfasst diplomatische, ordnungspolitische und militärische Handlungsfelder und setzt sich zusammen aus sehr breitgefächerten Beiträgen staatlicher, wirtschaftlicher und zivil-gesellschaftlicher Handlungsfähigkeit.[58]

Deutschlands maritime Handlungsfähigkeit umfasst bedeutende Einfluss- und Gestaltungsmöglichkeiten im internationalen maritimen Kontext. Aufgrund des Verhältnisses zum Einsatz militärischer Gewalt sowie der Bindung an Menschenwürde im Grundgesetz kann man die maritime Souveränität und Seemacht der Bundesrepublik als zwingend multilateral oder kosmopolitisch bezeichnen.[59] Deutschland ist nicht nur verpflichtet, die universelle Menschenwürde zu wahren und sich jeglicher machiavellistischer, exklusiver Eigeninteressen zu enthalten, sondern benötigt in den meisten Fällen, in denen es den Einsatz von Seestreitkräften für angebracht hält, einen multilateralen Rahmen.[60]

Mit dem Konzept der „integrierten Sicherheit" mobilisiert die Bundesregierung die gesamte Bandbreite staatlicher Handlungsfähigkeit um der Verschärfung der komplexen Bedrohung durch systemische Rivalität mit offener militärischer Gewalt und hybrider Kriegführung, sowie fortbestehenden Risiken aus internationalen Risiken, Terrorismus und Kriminalität zu begegnen.[61] Dabei trifft die Bedrohung alle Bereiche von Staat, Gesellschaft und Wirtschaft. In ihrer Sicherheitsstrategie führt die Regierung zivile und militärische Instrumente zusammen.[62]

D. Die Deutsche Marine als Instrument der Sicherheits- und Außenpolitik

Die Bundesrepublik Deutschland wurde erst nach der Wiedervereinigung zu einem bedeutenden maritimen Akteur, als militärische Seemacht keine Bedeutung mehr für wirtschaftlichen und weltpolitischen Erfolg zu haben

57 Ebd.

58 Der „vernetzte Ansatz" der Sicherheitspolitik kann auch hier als Vorbild dienen. Vgl. *Auswärtiges Amt*, Krisen verhindern, Konflikte bewältigen, Frieden fördern - Leitlinien der Bundesregierung, 2017, S. 14.

59 Geoffrey Till nannte diese Art Seemacht „post-modern", „kosmopolitisch" trifft es aber in der Tradition der längst nicht abgeschlossenen Aufklärung als großem Projekt der Moderne (Habermas) besser, *Till* (Fn. 12), S. 35-41; zu dieser Diskussion vgl. *Brake* (Fn. 8), S. 33-36.

60 Art. 1, Art 24 Abs. 2. GG.

61 *Bundesregierung* (Fn. 13), S. 11.

62 Ebd.

schien.[63] Nach 1990 ließ die „Friedensdividende" Streitkräfte und Marinen in Europa und auch in Deutschland schrumpfen,[64] während gleichzeitig die wirtschaftliche Entwicklung und Globalisierung die Bedeutung des Seehandels – und maritimer Ressourcen – immer weiter verstärkte.

Allerdings spielte Seemacht nicht nur in der weiter zurückliegenden Geschichte, sondern auch in den beiden Weltkriegen, im Kalten Krieg und in den drei Jahrzehnten nach dessen Ende eine zentrale Rolle in der Weltpolitik.[65] Vor allem anfangs britische, später US-amerikanische und alliierte Seemacht bestimmten maßgeblich den Verlauf der Geschichte der letzten hundert Jahre.[66] Bis in die Konflikte des 21. Jahrhunderts hinein spielen Seestreitkräfte, die Fähigkeit über See Macht zu projizieren, große Mengen an Fracht, militärischem Material und Versorgungsgütern zu transportieren eine entscheidende Rolle.[67]

I. Die zunehmende Bedeutung maritimer Sicherheit und die Rolle der Marine

Die Art und Weise, wie Deutschland seine Marine einsetzt, lässt seit 1990 bis heute einen Lernprozess und eine Weiterentwicklung des gesamten Diskurses zu maritimer Sicherheit erkennen. Auch wenn es kaum möglich wäre, sämtliche Einflüsse und Motive für Einsätze der Marine zu ermitteln und zu analysieren, liegen genügend offene Quellen vor, um aus ihnen Rückschlüsse auf die Entwicklung des Diskurses zu maritimer Sicherheit und auch der Gesamtstrategie der Bundesrepublik ziehen zu können.[68] Dies gilt auch umgekehrt. Beachtenswert hierbei ist außerdem, dass die traditionell starke Rolle der Bundeskanzler in der deutschen Außenpolitik, sich auch deutlich anhand des Einflusses der jeweiligen Amtsinhaber auf Einsätze der Marine nachvollziehen lässt.[69]

63 Vgl. *Brake* (Fn. 8), S. 61-62; 281-285.
64 Vgl. *Stöhs* (Fn. 28), S. 432.
65 Vgl. *Cable* (Fn. 7), S. 162-174.
66 Vgl. *Till* (Fn. 12), S. 1-6.
67 Vgl. *Coutau-Bégarie*, L'Océan Globalisé – Géopolitique des Mers au XXIe Siècle (1st ed.) Economica, 2007, S. 67; *Brake* (Fn. 8), S. 4-5; Analysis and Research Team European Council (Fn. 22), S. 1-3.
68 Vgl. *Brake* (Fn. 8)
69 Zur Marine, *Brake* (Fn. 8), S. 290-291; zur Rolle der Bundeskanzler in der Außenpolitik, vgl. *Bierling*, Vormacht wider Willen: Deutsche Außenpolitik von der Wiedervereinigung bis zur Gegenwart, Bundeszentrale politische Bildung, C.H. Beck, 2014, S. 13.

Seit Gründung der Bundeswehr 1955 bis zum Ende des Kalten Krieges war die Deutsche Marine – wie die gesamte Bundeswehr – vollständig in die NATO-Streitkräfte integriert und erfüllte inhaltlich und regional sehr begrenzte Aufgaben an der sogenannten „Nordflanke" des Bündnisses.[70] Außerdem war die Rolle der Marine des damals deutlich kleineren Deutschlands auf eine rein militärische Abschreckungsstrategie ausgerichtet. Maritime Ordnungsfunktionen, zum Schutz globaler maritimer Interessen, spielten keine Rolle. In der Strategie der Bundesregierung erwartete man noch bis in die 1990er Jahre, dass der Schutz der eigenen nationalen maritimen Interessen durch die Seemächte unter den Verbündeten übernommen würde.[71]

Einsätze und Teilnahme an NATO-Verbänden der Deutschen Marine nach dem Kalten Krieg			
Mission	**Ort**	**Typ/Charakter der Mission**	**Multilateraler Rahmen**
1991 *Südflanke*	Persischer Golf	Minenräumen, post-Konflikt	National/WEU (später)
1992-1996 *Sharp Guard*	Adria, Mittelmeer	Durchsetzen UN-Embargo	WEU/NATO
1994 *Southern Cross*	Somalia, Horn von Afrika	Evakuierung deutscher Blauhelme	National
1999 *Allied Force*	Adria, Mittelmeer	Beteiligung von Marinefliegern und Schiffen an den NATO-Luftangriffen gegen Serbien.	NATO
2002-2010 *Operation Enduring Freedom* OEF	Horn of Africa	Anti-Terrorismus, maritime Sicherheit, Seeraumüberwachung (Maritime Domain Awareness, MDA)	NATO
2002-2016 OAE	Mittelmeer	Anti-Terrorismus, maritime Sicherheit, MDA	NATO
2005 HumHiSOA	Banda Aceh	Humanitäre Hilfeleistung	National

70 *BMVg*, Weißbuch 1985, S. 216.
71 *BMVg* (Fn. 27), Art. 8 Abs. 3.

2006- UNIFIL	Libanon, Mittelmeer	MDA, Training von Marine & Küstenwache	UN
2008- *Atalanta*	Horn von Afrika	Anti-Piraterie, maritime sicherheit, MDA	EU
2011 Evakuierung Tunesien	Tunesien, Mittelmeer	Evakuierung Ägyptischer Bürger aus Tunesien (Arab. Frühling)	National
2014 *Cape Ray*	Mittelmeer	Eskorte für USS *Cape Ray* (Zerstörung syrischer chem. Waffen)	National
2015-2020 *Sophia*	Mittelmeer	Search and Rescue (SAR) und Vorgehen gegen Menschenschmuggel	National/EU
2015- *Counter Daesh*	Mittelmeer	Eskorte für frz. Flugzeugträger *Charles de Gaulle,* Kampf gegen den „Islamischen Staat“	EU/NATO
2016 SNMG2	Ägäis, Mittelmeer	MDA, Verbindungselement zwischen Griechenland und Türkei	NATO
2016 *SEA GUARDIAN*	Mittelmeer	Maritime Sicherheit, MDA	NATO
2020 *Irini*	Mittelmeer	Durchsetzung Embargo, MDA	EU
Durchgängig seit 1990	SNMG ½ SNMCMG ½	Nord Atlantik, Ostsee, Schwarzes Meer, Nordsee, Mittelmeer, Indischer Ozean	NATO
2024 *Aspides*	Rotes Meer	Schutz der Handelsschifffahrt vor Angriffen der Houthi aus dem Jemen	EU

Abb. 2: Übersicht zu den Einsätzen der Deutschen Marine seit 1990 (Quelle: Tabelle, Brake; Daten, Bruns; Brake & Walle)[72]

72 Tabelle: *Brake* (Fn. 8), S. 266; Daten: *Bruns*, Conceptualizing and Writing German Naval Strategy, in: Bruns, & Papadopoulos (Hrsg.), Conceptualizing Maritime & Naval Strategy, Nomos, 2020, S. 136; *Brake & Walle*, 60 Jahre Deutsche Marine im Bild. E.S. Mittler & Sohn, 2016, S. 80, 84-85, 88, 94-95, 104-109.

Der bis heute anhaltende Lernprozess zur Marine als Instrument der Außenpolitik begann mit der Wiedervereinigung und dem Ende des Kalten Krieges. Zu Beginn mussten beispielsweise die Verbündeten Deutschland davon überzeugen, seine Marine in Situationen einzusetzen, die für „boots on the ground" zu riskant oder unhaltbar erschienen (Einsätze SÜDFLANKE (1991), SHARP GUARD). Bald folgte Deutschland dem Beispiel seiner Verbündeten (SOUTHERN CROSS) und ergriff dann zunehmend die Initiative zur Nutzung der Möglichkeiten, die die Marine bot (ab OPERATION ENDURING FREEDOM (OEF)).[73]

Die Fortschritte im Einsatz seiner Marine lassen sich gut daran erkennen, dass nicht nur die Zahl, sondern auch die Vielfalt der Aufgaben der Marine seit dem Ende des Kalten Krieges stetig zunahmen (siehe Abb. 2).[74] Diese Entwicklung vollzieht sich auch in den seit dem 1985er Weißbuch veröffentlichten strategischen Schlüsseldokumenten. Hier formuliert Deutschland bereits 2006 ein ähnliches Verständnis von den Aufgaben einer Marine, wie es sich bei den Verbündeten Frankreich, Großbritannien und den USA findet.[75]

Der Wandel zeigt sich auch darin, dass die Bedeutung von nationalen Vorbehalten, sog. *Caveats* in *Rules of Engagement* (ROE), den selbst auferlegten Einschränkungen für den Einsatz der Marine bei multilateralen Missionen, abnimmt. Wurden deutsche Kriegsschiffe anfangs aus den Einsätzen der Verbündeten herausgehalten („Tankerkrieg" Iran-Irak 1987, SÜDFLANKE – nationaler Einsatz), so wurden sie zunehmend integriert (SÜDFLANKE – WEU-Teil; SHARP GUARD bis zum Urteil des Bundesverfassungsgerichts vom Juli 1994) und nach und nach in die Einsätze einbezogen (SHARP GUARD nach Juli 1994; OEF), bis nationale Vorbehalte oder Einschränkungen in Einsatzgebieten keine bedeutende Rolle mehr spielten (UNIFIL, ATALANTA, SOPHIA, SEA GUARDIAN, IRINI).[76]

Natürlich verlief dieser Prozess innerhalb der Phasen nicht linear und die Herausforderungen, mit denen sich deutsche Außenpolitik auseinandersetzen musste, häuften sich und wirkten oft zusammen, anstatt sauber aufeinander zu folgen. So dauerte die Beteiligung der Marine am „Krieg

73 Die Einsatzgeschichte der Marine bietet eine Vielzahl von Fallstudien für den außenpolitischen Wert, die Flexibilität und die vergleichsweise geringen politischen, finanziellen und militärischen Risiken. Im Detail mehr dazu in *Brake* (Fn. 8).

74 Vgl. *Brake* (Fn. 8), S. 49-54.

75 Vgl. *Brake* (Fn. 8), S. 264-267.

76 Vgl. *Brake* (Fn. 8), S. 218, 267-268.

gegen den Terror" bis 2010 am Horn von Afrika und bis 2016 im Mittelmeer – wenn auch in beiden Fällen mit begrenzten Mitteln in der Spätphase. Das deutsche Engagement bei UNIFIL im Jahr 2006 war zwar die erste Blauhelm-Mission der Marine überhaupt, ist aber untrennbar mit dem „Krieg gegen den Terror" und – später – mit der Flüchtlingskrise im Mittelmeer in den Jahren nach 2015 verbunden.[77] Auch der Aspekt der regionalen Stabilisierung und umfassenderen Gewährleistung maritimer Sicherheit bei OEF verschwand nicht, sondern verlagerte sich 2008 von der Terrorismusbekämpfung auf breitere maritime Ordnungsfunktionen durch die Bekämpfung der Piraterie mit der EU-Mission ATALANTA.

Bei der Weiterentwicklung des Einsatzes der Marine als politischem Werkzeug ist das Grundgesetz und seine Auslegung durch Politik und Bundesverfassungsgericht von zentraler Bedeutung. Während die ersten Einsätze noch als Kabinettsbeschlüsse umgesetzt wurden, etablierte sich mit den Verfassungsgerichtsurteilen von 1993 und 1994 die heute im Parlamentsbeteiligungsgesetz kodifizierte Praxis der Mandatierung durch den Bundestag.[78] Beachtenswert ist dabei, dass sich die Weiterentwicklung der Rolle der Marine als Instrument der Außenpolitik in einem Spannungsfeld der Wechselwirkungen aus Regierungspraxis, Mandatierungen, Gesetzgebung, Verfassungsgerichtsurteilen und der Möglichkeit zur Verfassungsänderung vollzieht.

Auch die innerhalb der Bundeswehr beispiellosen „Ständigen Einsatzregeln Marine" sind ein bemerkenswerter Entwicklungsschritt.[79] Weder die Luftwaffe noch das Heer haben ähnliche Regeln für den Routinebetrieb. Diese ständigen Einsatzregeln tragen dem Umstand Rechnung, dass die Marine auch bei der routinemäßigen Durchfahrt und Anwesenheit in internationalen Gewässern in Situationen geraten kann, die eine über die Selbstverteidigung hinausgehende Gewaltanwendung erfordern können.

77 Der damalige US-Präsident Bush ordnete die Hisbollah im Libanon als Gegner im „Kampf gegen den Terror" ein. So wurde UNIFIL einerseits Blauhelm- und Friedensmission für Deutschland, andererseits zählte es aber auch im Kampf gegen den Terrorismus. Erst nachdem Deutschland knapp 1.000 Marinesoldaten für den Einsatz UNIFIL bereitstellte, lehnte es öffentlich ein stärkeres Engagement in Afghanistan ab – wo sich 2006 die Kämpfe und Verlustzahlen verschärften. *Brake* (Fn. 8), S. 202.

78 Eine nähere Diskussion dieser Entwicklung muss hier aus Platzgründen entfallen, findet sich aber u.A. bei *Brake* (Fn. 8), S. 83-85.

79 *Deutsche Marine*, Ständige Einsatzregeln der Deutschen Marine, 2018.

Auch wenn diese Einsatzregeln noch sehr restriktiv formuliert sind,[80] geht Deutschland damit einen weiteren Schritt in die Richtung, seine Marine als flexibel einsetzbares Instrument der Außenpolitik zu denken.

Die aktuelle Debatte, vor allem getrieben durch hybride Bedrohungen von marKRITIS, hat auf den Entwicklungsprozess zur Rolle der Marine und zu maritimer Sicherheit große Wirkung. Weil die Qualität der Bedrohung die Möglichkeiten ziviler Ordnungskräfte übersteigt, ist der Bedarf an den spezialisierten Fähigkeiten der Marine nun auch unmittelbar vor der eigenen Küste groß. Sie kann aber nicht nur hybriden Bedrohungen militärischer Qualität gut begegnen. Nach drei Jahrzehnten Auslandseinsatzerfahrung kann die Marine auch auf einen großen Erfahrungsschatz im Umgang mit nicht-militärischen Bedrohungen zurückgreifen: Es braucht jetzt auch in Nord- und Ostsee die Fähigkeiten, verdächtige Handelsschiffe zu erkennen, aufzubringen und zu untersuchen, verhältnismäßig und rechtssicher mit Kriminellen und nicht-Kombattanten umzugehen, mit Verhaltensweisen von Handelsschiffen vertraut zu sein, Ladungspapiere und bestimmte Frachtarten zu verstehen. Allerdings tritt auch sichtbar zutage, dass der Marine die Rechtsgrundlage fehlt, um außerhalb von mandatierten Auslandseinsätzen regulär maritime Ordnungsfunktionen zu übernehmen:[81] Eine deutsche Fregatte im Mittelmeer kann unter dem Mandat SEA GUARDIAN umfassend zu maritimer Sicherheit beitragen, in Nord- und Ostsee fehlt ihr die rechtliche Handhabe.[82]

80 Ein Vorgehen gegen maritime Kriminalität nur auf ausdrücklichen Befehl – oder in Nothilfe, bzw. Selbstverteidigung, *Deutsche Marine* (Fn. 79), 2.

81 Vgl. *Ehlers* (Fn. 6); *Walter* (Fn. 6).

82 Vgl. *Brake* (Fn 8), S. 274-278.

II. Ein zeitgemäßes Update der klassischen Marineaufgaben

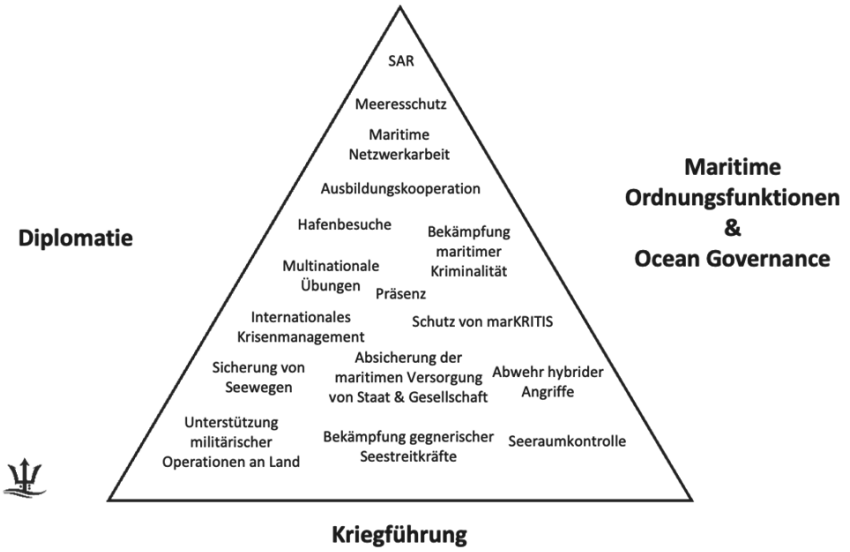

Abb. 3: Schematische Darstellung für ein zeitgemäßes Update klassischer Marineaufgaben (Quelle: Moritz Brake & Bertrand Mignot, basierend auf dem Modell von Ken Booth (1977))

Die Bandbreite an Aufgaben, die Nationen mit maritimer Handlungsfähigkeit, mit Seemacht verbinden, lassen sich an Seestreitkräften als dem zentralen Element ihrer klassischen Komponenten festmachen: Die Unterstützung eigener Diplomatie; maritime Ordnungsfunktionen und Ocean Governance (als zeitgemäße Weiterentwicklung); Kriegführung – Abschreckung oder Bekämpfung von Gegnern, die Verhinderung oder Unterstützung militärischer Operationen an Land.[83] Die obige Grafik stellt diese

83 Alle diese unterstützenden Funktionen sind auch gleichzeitig mögliche Aufgaben in der Vereitelung von Maßnahmen eines Gegners. Für die „klassische" Sicht, Vgl. *Corbett*, England in the Seven Years' War: A Study in Combined Strategy, vol 1 (reprint of the 1907 edition ed.), Cambridge University Press, 2010, S. 6; angepasst durch *Booth*, Navies and Foreign Policy, (reprint ed. of 1977 original), Routledge, Oxon, 2014, S. 15; *Grove*, The Future of Seapower, Naval Institute Press, Annapolis, 1990, S. 234-5, und um Ocean Governance ergänzt, vgl. *Mellet*, Adaptive Dynamic Capabilities and Innovation: The Key for Small Navies Protecting National Interests at and from the Sea. In *Mulqueen, Sanders & Speller* (Hrsg.), Small Navies: Strategy

Aufgaben in einem Dreieck dar, um ihre „untrennbare Dreieinigkeit" (Ken Booth, der Urheber dieses Dreiecks-Schemas) im Einsatz von Marinen als Instrumenten der Außenpolitik zu illustrieren.[84] Zusätzlich wichtig ist dabei, dass alle anderen Aufgaben von Marinen auf dem Fundament ihrer Fähigkeit zur Kriegführung ruhen – der Basis des Dreiecks.[85]

Seehandel muss nach wie vor geschützt werden, aber er ist längst nicht mehr national organisiert und wird auch nur zu geringem Teil unter der nationalen Flagge der Länder betrieben, die maßgeblich auf die dabei transportierten Güter angewiesen sind. Aus diesem Grund hat sich die früher selbstverständliche Rolle des Schutzes eigener Seewege für Seestreitkräfte weiterentwickelt. Da die globalisierte Weltwirtschaft auf Seehandel als komplexem internationalem System fußt, muss dieses als Ganzes geschützt und gestärkt werden.[86] Heute macht es für den Seehandel meist keinen großen Unterschied, wem Schiffe gehören oder wessen Flagge darauf weht, wenn sie von Piraterie, Havarie oder blockierten Kanälen und Häfen betroffen sind.

Die Bedeutung des Flaggenstaats hat allerdings jüngst mit den Angriffen der Houthis im Roten Meer eine politische Renaissance erfahren: Dadurch dass die als Stellvertreter Irans agierenden Houthis u.A. russische und chinesische Schiffe von ihrem Beschuss ausnehmen, veränderten sich die regionalen Handelsstrukturen nahezu über Nacht. Wo früher Schiffe der unterschiedlichsten Flaggenstaaten Häfen anliefen, sind mittlerweile überwiegend Schiffe chinesischer Flagge zu beobachten.[87]

„*Chinese shipping companies have stepped into the void left by other* [Western] *shipping companies in the region*", sagte der Jordanische Schifffahrtsexperte Ali Abdul Rahman im Februar 2024 über die Auswirkungen der Angriffe der Houthi-Rebellen auf Handelsschiffe im Roten Meer.[88] Hier zeigt sich somit seit November 2023, dass der Flaggenstaat eines Handelsschiffes auch heute noch bisweilen darüber entscheiden kann, ob es zum Ziel von Angreifern wird, während die direkte staatliche Kontrolle über

and Policy for Small Navies in War and Peace (1st ed., pp. 67-80) Routledge, London, 2014, S. 67.

84 *Booth* (Fn. 63), S. 16.

85 *Booth* (Fn. 63), S. 16.

86 Vgl. *Till* (Fn. 12), S. 32-41.

87 *Ali Abdul Rahman*, webinar "Shipping Disruptions" der Maritime Business Chamber South Africa, 28.02.2024.

88 Ebd.

seine global bedeutsame Handelsflotte China machtpolitische Handlungsfähigkeit verleiht.

Seemacht ist dabei mehr als nur Marine und Handelsschifffahrt, eher – ganz allgemein – die Bezeichnung für die Fähigkeit zur Einflussnahme auf Menschen und Sachen auf und von See.[89] Mit Seestreitkräften, zivilen Behörden, der maritimen Wirtschaft,[90] aber auch mit Maßnahmen der Wirtschafts- und Entwicklungspolitik, über diplomatische Mitgestaltung in internationalen Institutionen und in der Weiterentwicklung des See- und Völkerrechts, kann Deutschland auf vielfältige Instrumente zu Wahrung und Ausbau seiner und europäischer maritimer Souveränität zurückgreifen.

III. Von internationalem Krisenmanagement, über die maritime Dimension der Landes- und Bündnisverteidigung, zu umfassender maritimer Sicherheit und globaler Ocean Governance

Auch die Bundesrepublik lernte den Wert ihrer Marine als Instrument der Außenpolitik schätzen – ließ dabei aber Lücken in ihrer materiellen Ausstattung und Rechtsgrundlage für Aufgaben maritimer Sicherheit. Bei Einsätzen des internationalen Krisenmanagements bot die Marine schon unmittelbar nach der Wiedervereinigung wertvolle Handlungsoptionen, um gemäß der außenpolitischen Verantwortung Deutschlands Beiträge zu Missionen der NATO, (W)EU und UN leisten zu können.[91] Diese Einsätze führten auch zu einem zunehmenden Aufgabenspektrum der Marine in der Übernahme von Ordnungsfunktionen zur Gewährleistung maritimer Sicherheit.

Von Embargoüberwachung über Terrorismus- und Pirateriebekämpfung bis zur Flüchtlingsrettung führte dieser Weg letztendlich zur Beteiligung an der vollumfänglich auf Gewährleistung maritimer Sicherheit ausgerichteten Mission SEA GURADIAN im Mittelmeer.[92] Allerdings fehlt der letzte Schritt zu einer umfassend im Rahmen maritimer Sicherheit einsetzbaren Marine, die konsequente Umsetzung des in internationalen Mandaten voll-

89 Vgl. *Till* (Fn. 12), S. 25.
90 Die „klassischen" Elemente von Seemacht. Vgl. *Till* (Fn. 12), S. 25.
91 WEU – Westeuropäische Union; in den 1990er Jahren fand z.B. die kombinierte NATO/WEU Operation SHARP GUARD in der Adria statt. Zum Wert der Marine bei der Wahrnehmung von Deutschlands außenpolitischer Verantwortung, vgl. *Brake* (Fn. 8), S. 1-6.
92 Ebd.

zogenen Lernprozesses in eine dauerhafte Rechtsgrundlage für maritime Ordnungsfunktionen.[93]

Das Dilemma bringt Bernd Walter so auf den Punkt: „[I]m maritimen Einsatz gilt mehr noch als beim Inlandseinsatz der Gemeinspruch, dass es Sonderlagen gibt, in denen die Polizei darf, aber nicht kann, die Bundeswehr könnte, aber nicht darf. Aus der Perspektive der auf den maritimen Kontext übertragene".[94] Trennung von „innerer" und „äußerer" Sicherheit im historisch gewachsenen Verfassungsverständnis der Bundesrepublik fehlt der Deutschen Marine die Rechtsgrundlage für die reguläre Übernahme von Ordnungsfunktionen.[95] Jenseits dieser deutschen Sichtweise gehört der Dreiklang aus Diplomatie, Ordnungsfunktionen und Kriegführung zum regulären Aufgabenspektrum von Seestreitkräften.[96] In z.B. den USA, Frankreich oder Großbritannien werden seit jeher Ordnungsfunktionen selbstverständlich durch die jeweiligen Marinen wahrgenommen.[97]

Die begrenzten Rechtsgrundlagen für Ordnungsfunktionen durch die Marine stehen dabei im Widerspruch zum umfassenden deutschen Verständnis von maritimer Sicherheit und globaler Verantwortung auf See. Dies ist nicht nur logische Konsequenz und maritime Dimension der „integrierten Sicherheit" der NSS, es ergibt sich auch aus der Übernahme des internationalen Seerechtsübereinkommens (SRÜ) in nationales Recht 1994, der ersten nationalen Strategie zum Schutz der Meere aus dem Jahr 2008 und der umfassenden Betrachtung maritimer Grundlagen der deutschen Gesellschaft und Wirtschaft in der maritimen Agenda 2025.[98]

Formal sind zwar die Bundespolizei und die Polizeien der Länder für maritime Sicherheit außerhalb militärischer Bedrohungslagen zuständig,

93 *Brake* (Fn. 8), S. 57-68; *Walter* (Fn. 6), S. 303.

94 *Walter* (Fn. 6), S. 303.

95 Mehr zu dem Dilemma zwischen der ansonsten selbstverständlichen Übernahme von Ordnungsfunktionen durch Marinen und dem deutschen „Sonderweg" einer Marine, der dazu die grundsätzliche Rechtsgrundlage fehlt, vgl. *Brake* (Fn. 8), S. 57-68.

96 Vgl. *Gray*, The Navy in the Post-Cold War World. The Pennsylvania State University Press, 1994, S. 161; *Corbett* (Fn. 63), S. 6; *Booth* (Fn. 63), S. 16; *Grove* (Fn. 63), S. 234; *Till* (Fn. 12), S. 35-41.

97 Vgl. *US Secretary of the Navy* (Fn.14), 3; *Marine Nationale,* Nos Missions, https://www.defense.gouv.fr/marine/nos-missions, abgerufen am 15.03.2024; *Royal Navy,* What we do, https://www.royalnavy.mod.uk/what-we-do#:~:text=The%20Royal%20Navy%20acts%20as,as%20hurricanes%2C%20earth-quakes%20and%20epidemics, abgerufen am 15.03.2024.

98 *Bundesregierung*, (Fn. 51); *Bundesregierung* (Fn. 51); *Vertragsgesetz Seerechtsübereinkommen* (Fn. 51).

praktisch kommen diese allerdings mit ihren Mitteln qualitativ und quantitativ an Grenzen. Die geografische Ausdehnung des Ozeans, die vitale Bedeutung auch weit entfernter Seewege und die Qualität hybrider Bedrohungen übersteigen die Mittel ziviler Ordnungskräfte. Erstens kann man auf Hoher See froh sein, wenn überhaupt ein Behördenschiff in greifbarer Nähe zur Verfügung steht – es gibt sehr viel mehr an Ozean zu patrouillieren, als selbst die großen Seemächte an Schiffen in ihren Flotten haben.[99] Zweitens muss jedes Schiff, das in weiter entfernte Krisenregionen entsandt wird, nicht nur hochseetauglich sein, es muss auch über große Ausdauer in See, robusten Selbstschutz sowie leistungsfähige Überwachungs- und Kommunikationsmittel verfügen: Freundliche Häfen können schlecht erreichbar sein und die Situation in maritimen Krisenherden kann rasch eskalieren. Drittens muss bei hybriden Bedrohungsszenarien auch näher der heimischen Küsten mit Angriffen militärischer Qualität, auch unter Wasser und aus der Luft gerechnet werden: dafür sind Polizeikräfte schlecht ausgerüstet.

Aus globaler Verantwortung gedacht, fließt maritime Sicherheit weiter ein in die Notwendigkeit, die nachhaltige und gerechte Nutzung der Meere für die gesamte Menschheit und künftige Generationen sicher zu stellen – globale *Ocean Governance*. „Ocean Governance" steht in ihrer normativen Interpretation für ein System des Managements der nachhaltigen und gerechten Nutzung des Welt-Ozeans als „gemeinsames Erbe der Menschheit".[100] Dies umfasst aus Sicht der European Environment Agency (EEA) nicht nur ökologische Nachhaltigkeit, sondern auch Produktivität, Sicherheit und Resilienz im Hinblick auf (menschliche, kriminelle, gewaltsame) Gefahrenabwehr, Unfallverhütung und Naturkatastrophen.[101] Der Anspruch als „gemeinsames Erbe der Menschheit" (common heritage of mankind), für etwas, das der gesamten Menschheit (gerecht) und künftigen Generationen (nachhaltig) zugutekommen soll, findet sich in der Präambel des SRÜ von 1982, geht aber auf ein noch älteres, nie umgesetztes Konzept

99 Selbst die US Navy setzt auf Verbündete, vgl. „1000-ship-navy" (Fn. 33); Rahman (Fn. 33).

100 Vgl. *Mann Borgese*, The Oceanic Circle - Governing the Seas as a Global Resource, United Nations University Press, Tokyo, 1998, preface, S. 184-194; *Mondré & Kuhn*, Ocean Governance, in: Aus Politik Und Zeitgeschichte 2017 (51-52), S. 4–9.

101 *European Environmental Agency* (EEA), EEA Marine Roadmap, 2018, S. 1.

zu einer „Weltverfassung“ zur Neuordnung der Welt nach dem Zweiten Weltkrieg zurück.[102]

Die Marine ist mit ihrer Bandbreite an Handlungsfähigkeit ein einzigartiges wertvolles Instrument der deutschen Außenpolitik. Ihr Beitrag zu integrierter maritimer Sicherheit reicht von militärischen Szenarien über Diplomatie, humanitäre Unterstützung, Ordnungsfunktionen gegenüber kriminellen Akteuren und schließt auch den Schutz der Meeresumwelt ein. Die international bestehenden Lücken bei der Durchsetzung der nachhaltigen und gerechten Nutzung des Ozeans kann Deutschland auch mit seiner Marine schließen helfen. Außenpolitische Handlungsfähigkeit und Souveränität sind auf maritime Sicherheit angewiesen – und ein zentrales sehr flexibles Instrument der Außenpolitik ist die Marine.

E. Der Schutz maritimer kritischer Infrastrukturen

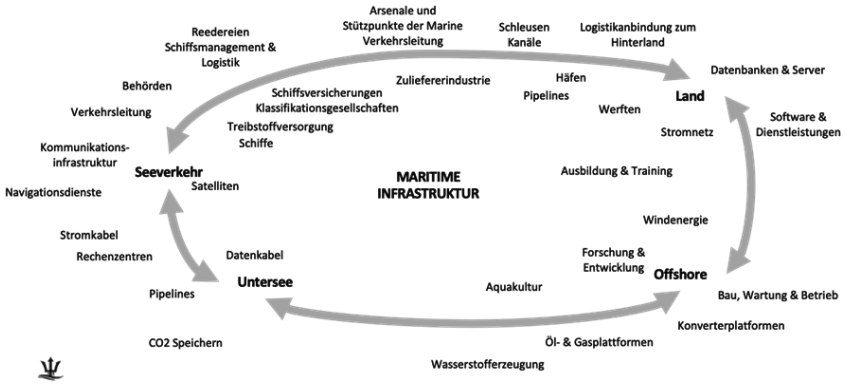

Abb. 4: Maritime Infrastruktur verbindet eine Vielzahl von Beiträgen, inkl. Seeverkehr, an Land, Offshore und unter Wasser (Quelle: Moritz Brake & Bertrand Mignot)

102 Erarbeitet in den 1940er Jahren an der Universität von Chicago, von einer Gruppe von Intellektuellen im Exil um Guiseppe Antonio Borgese und Thomas Mann. Elisabeth Mann Borgese, die spätere „Mutter [der] Verfassung der Meere“ (Holzer), des Seerechtsübereinkommens von 1982, war Thomas Manns jüngste Tochter, Borgeses spätere Ehefrau und damals Sekretärin der Gruppe, die an der „Weltverfassung“ arbeitete. Vgl. *Holzer*, Elisabeth Mann Borgese - Ein Lebensporträt (6th ed.) Fischer Taschenbuch, 2003, S. 121-123, 172, 178-181, 200-201.

Kritischer Infrastruktur (KRITIS) ist deshalb kritisch, weil ihr „Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen" nach sich zöge.[103] Im maritimen Umfeld trifft dies vor allem auf den Seeverkehr (inkl. dazu nötige Infrastruktur an Land; Häfen, Werften, Seefunkdienste, Küsten-Radaranlagen, landseitige Logistikanbindungen), sowie Unterwasser-Infrastruktur wie Pipelines oder Tiefseedatenkabel zu. Außerdem werden Offshore-Infrastrukturen zur Energiegewinnung immer bedeutsamer. Zu den schon lange bestehenden Gas- und Ölplattformen, kommt mit großen Ausbauzielen für Deutschland und Europa die Windenergie hinzu. Je nach Relevanz für die Versorgungssicherheit könnten aber auch noch andere Einrichtungen, wie z.B. Wasserstoffproduktion, unter Wasser betriebene Rechenzentren oder CO^2 Speicher, aber auch Fischerei und Aquakultur kritische Bedeutung erreichen.[104]

Wie auch im Jahr 2023 die NATO und EU KRITIS Task-Force feststellte, wird es nicht gelingen alle relevanten Infrastrukturen vollumfänglich zu schützen.[105] Der Schutz von marKRITIS stellt dabei eine besondere Herausforderung dar. Alle modernen Gesellschaften sind auf ihre maritimen Lebensgrundlagen angewiesen. Allerdings liegen viele diese Beiträge außerhalb des direkten nationalstaatlichen Zugriffs. Dies unterstreicht die Bedeutung von Resilienz – die Fähigkeit, Störungen jeglicher Art möglichst gut zu widerstehen oder zumindest rasch wieder funktionsfähig zu werden.[106] Dazu gehört auch, einer großen Bandbreite an Gefahren so gut es geht, effizient und effektiv auch durch Schutzmaßnahmen zu begegnen. Dazu braucht es Mittel zur Überwachung, der Erkennung von Unregelmäßigkeiten, Nachverfolgung von Tätern, und letztlich zur Abwehr von Angriffen gegen eine große Zahl von potenziellen Zielen, die obendrein über weite Distanzen – auch jenseits der Hoheitsgewässer, fernab von eigenen Küsten auftreten können.

Maritime Sicherheit ist für Deutschland existenziell – und verliert ihre Bedeutung auch mit der Energiewende nicht: Im Gegenteil, die langfristige Entkoppelung der deutschen Wirtschaft von fossilen Energieimporten

103 *Bundesministerium des Innern, für Bau und Heimat* (BMI): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S. 3.
104 *Baldauf, Brake, Finger et.al.* (Fn. 5), S. 31-32.
105 *EU & NATO* (Fn. 32), S. 3-6.
106 Vgl. *Bundesregierung*, Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, 2022, S. 106.

basiert zu einem großen Teil auf marKRITIS, nicht zuletzt zur Stromerzeugung auf dem Meer in Offshore-Windparks. Außerdem bleiben globale Lieferketten – inklusive derjenigen für nachhaltige Technologien – vorwiegend maritim. So wird z.B. schätzungsweise 60 % des zukünftigen Wasserstoffbedarfs für Deutschland auf dem Seewege geliefert werden.[107] In Summe aller nationalen Windparks entwickelt sich die Nordsee außerdem zum größten Kraftwerk der Welt. Die Abhängigkeit Deutschlands vom reibungslosen Betrieb der Anlagen nimmt dabei immer weiter zu. Bis 2045 will Deutschland mehr als ein Drittel seines heute benötigten Stroms auf dem Meer erzeugen.[108] Diese Stromerzeugung wird allein aus Platzgründen überwiegend außerhalb der Hoheitsgewässer Deutschlands und anderer Länder stattfinden müssen. Sowohl aufgrund der räumlichen Distanzen und der rechtlichen Situation ergeben sich dabei Herausforderungen, die sich nicht nach den bisherigen Zuständigkeiten und mit den existierenden Mitteln der Behörden lösen lassen.

Während mit dem Havariekommando in Cuxhaven im Jahr 2003 eine Bund-Länder-übergreifende Institution geschaffen wurde, die bei Seeunfällen einheitliche Führung und frühzeitige Koordination aller relevanten Akteure gewährleistet, gibt es vergleichbare Klarheit in der Gefahrenabwehr, im Umgang mit Sabotage, Terrorismus und anderen Formen maritimer Kriminalität bis heute nicht.[109] Das gilt auch für hybride Bedrohungen, die mitunter militärische Qualität unterhalb eines offenen Krieges erreichen können. Das Maritime Sicherheitszentrum in Cuxhaven bringt zwar Behörden, Polizeien und Marine unter einem Dach zusammen, löst aber nach wie vor die Probleme eines umfassenden weltweiten Lagebildes, der Integration gesamtstaatlicher Kapazitäten unter einheitlicher Führung und eines koordinierten Fähigkeitsaufbaus nicht.[110]

Neben der nötigen Integration ziviler und militärischer Fähigkeiten sind auf See auch private Akteure stärker in der Pflicht zum Eigenschutz, als dies an Land der Fall wäre. Es ist immer schwieriger, auf See Sicherheit zu gewährleisten, als an Land: Die Distanzen sind groß und Einsatzmittel im Vergleich immer dünn gesät. Deshalb ist auch zu erwarten, dass im Rah-

107 *Kröger*, Mit dem Rücken zum Meer?, Schiff&Hafen, 01/2024, S. 44-45.
108 70 GW als Ausbauziel bis 2045, vgl. Gesetz zur Entwicklung und Förderung der Windenergie auf See (Windenergie-auf-See-Gesetz – WindSeeG), zuletzt geändert am 22.03.2023.
109 Vgl. *Baldauf, Brake, Finger et.al.* (Fn. 5), S. 11-12.
110 Ebd., S. 35-36.

men des bevorstehenden neuen „KRITIS-Dachgesetzes“,[111] Beiträge privater Betreiber von maritimen kritischen Infrastrukturen stärker eingefordert werden. Im Bereich der Cybersicherheit, die zum Thema einige Parallelen aufweist, gelten bereits gesetzliche Vorgaben zur Steigerung der Resilienz, zum Eigenschutz nach „Stand der Technik“ und zu Meldepflichten.[112] Außerdem ist es auch für Schiffe unter deutscher Flagge möglich, sich mit bewaffneten Wachen vor Piraterie schützen.[113] Der Gesetzgeber setzt also auch in Deutschland voraus, dass in bestimmten Situationen von privaten Akteuren ein höheres Maß an Selbstschutz erwartet werden kann.

Eine besondere Herausforderung stellt das Spannungsverhältnis zwischen formaler ziviler Zuständigkeit für alle nicht-militärischen Anteile maritime Sicherheit dar, während hybride Bedrohungen gegen marKRITIS bewusst unterhalb der Schwelle eines kriegerischen Angriffs bleiben. Die Bundespolizei ist deshalb zwar für den Schutz vor nicht-militärischen Bedrohungen außerhalb der Hoheitsgewässer zuständig, allerdings fehlen ihr die Mittel, um dies geografisch unbegrenzt und angesichts hybrider Bedrohungen zu leisten. Die Marine ist im Gegenzug global einsetzbar und verfügt qualitativ über viele der nötigen Mittel – z.B. zur Überwachung unter Wasser oder zur Bekämpfung von Luftzielen, kämpft aber mit knappen Budgets, zu wenig Schiffen, Ersatzteilen, Munition und Personal.

Die aktuellen Kapazitäten der Marine reichen nicht aus, um regional und global vollumfänglich die maritimen Interessen der Bundesrepublik zu schützen. Als wertvolles Instrument der Außenpolitik wird sie seit Jahren an der Grenze ihrer Kapazitäten eingesetzt – auch ohne, dass sie die Bewachung von maritimer Infrastruktur in Heimatgewässern auch noch stemmen musste. Seit Jahren muss hart priorisiert werden und Einsätze der Marine schmerzhaft gegeneinander abgewogen werden. In anderen Worten: die Marine kann zwar Wertvolles zum Schutz maritimer kritischer Infrastruktur beitragen, sie wird dies aber nicht auf Dauer mit ihren hochwertigsten Einheiten leisten können. Wenn sie in Nord- und Ostsee im Ein-

111 Bis heute ist die CER-Richtlinie der EU nicht in nationales Recht übertragen worden. Deutschland hat damit den in der Richtlinie gesetzten Stichtag am 17.10.2024 überschritten. Stand 05.01.2025.

112 Vgl. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG); Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0); Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz.

113 Vgl. Gesetz zur Einführung eines Zulassungsverfahrens für Bewachungsunternehmen auf Seeschiffen.

satz ist, fehlt sie zur Flankierung deutscher Außenpolitik und zum Schutz globaler maritimer Interessen in der Welt.

Der Rechtsrahmen zum Einsatz der Marine für maritime Ordnungsfunktionen unterhalb der Schwelle eines bewaffneten Konfliktes ist lückenhaft – auch und gerade im Hinblick auf den Schutz von marKRITIS.[114] Selbst wenn im akuten Falle hoffentlich kurzfristig pragmatische Lösungen zur Reaktion auf Angriffe gefunden werden, führen unkoordinierte Präsenz und Fähigkeitsaufbau zu großen Lücken. Es fehlt sowohl bei der Marine als auch bei den zivilen Behörden an den Mitteln, um die gesamte deutsche ausschließliche Wirtschaftszone (AWZ) vom Meeresboden bis in die Luft zu überwachen und zu schützen. Außerdem ist die Gefahr groß, dass ohne Festlegung einheitlicher Führung für den Krisenfall auch die nötige Vorbereitung durch Übungsszenarien hinter der Realität zurückbleibt.

Eine weitere zentrale Aufgabe zum Schutz von marKRITIS und in der Gewährleistung von maritimer Sicherheit ist die Umsetzung der Erkenntnisse aus den Erfahrungen des Krieges in der Ukraine. Es braucht mehr als nur klassische zivilpolizeiliche Einsatzmittel und kampfstarke militärische Hochwerteinheiten und -waffensysteme, die mit großem Ressourcen- und Zeitaufwand zu bauen sind. Die Größe des zu überwachenden Raumes, aber auch die Art der Bedrohung aus ferngelenkten oder autonomen, kleinen, kostengünstigen Drohnen erfordert Gegenmaßnahmen, die genau darauf abgestimmt sind: ebenfalls rasch, kostengünstig und in großer Zahl verfügbar. Dabei wäre es obendrein technisch keine Herausforderung, ferngelenkte Systeme zwischen ziviler und militärischer Kontrolle zu übergeben. Ein wichtiger Synergieeffekt neuer Technologien besteht in der deutschen Komplexität an Zuständigkeiten darin, dass es nachrangig wird, wer im Routinebetrieb welches Überwachungs- und Einsatzmittel beschafft und betreibt. Im Rahmen einer integrierten Gesamtstrategie für maritime Sicherheit kann damit zivil-militärisch, privat und staatlich übergreifend Fähigkeitsaufbau, Präsenz und Einsatz leichter geplant und umgesetzt werden.

114 Vgl. *Ehlers* (Fn. 6); *Walter* (Fn. 6), S. 304-5.

F. Fazit

Maritime Sicherheit – inklusive des Schutzes maritimer kritischer Infrastrukturen – ist eine zentrale staatliche Verantwortung und gesamtstrategische Aufgabe für die Bundesrepublik Deutschland. Sie erfordert das Zusammenführen übergreifender Informationen und Handlungsmöglichkeiten in einem Ansatz „integrierter Sicherheit", wie er in der NSS beschrieben wird. Um längst erkannte Lücken in der Sicherheitsarchitektur zu schließen, braucht es klare Verantwortlichkeiten, einheitliche Führung, koordinierten zivilen und militärischen Fähigkeitsaufbau und nicht zuletzt eine Anpassung des Rechtsrahmens. Letzteres ist dringend notwendig, um mit den verfügbaren Mitteln bestmöglich komplexen Bedrohungen im maritimen Umfeld, mit Übergängen zwischen Hoheitsgewässern, AWZ und Hoher See gerecht zu werden.

Um integrierte Sicherheit in der Praxis zu erreichen, bietet der maritime Kontext ein wertvolles Experimentierfeld zur Weiterentwicklung der gesamtstrategischen Handlungsfähigkeit Deutschlands in der Zeitenwende. Speziell im Hinblick auf den Einsatz der Marine zur Gewährleistung umfassender maritimer Sicherheit und die Schaffung eines gemeinsamen, Bund-Länder-übergreifenden, zivil-militärischen Lagebildes – unter Einbindung privatwirtschaftlicher Akteure, scheinen die Hürden geringer und die gebotene Dringlichkeit höher als an Land.

Auch was den Ausbau dringend benötigter Fähigkeiten an ferngelenkten und (teil-)autonomen Systemen sowie die Unterstützung menschlicher Entscheidungen durch KI angeht, könnte dies für Deutschland auf dem Meer leichter fallen als an Land. Öffentliche Sorgen und politische Widerstände könnten weniger stark zur Geltung kommen, wenn es nicht um von Menschen bewohnte Gebiete geht, in denen neue Technologien zum Einsatz kommen sollen. Gesamtstrategisch wird sich Deutschland der allgemeinen Entwicklung in der Welt – vor allem auch auf ihren Schlachtfeldern – nicht entziehen können.

So sieht auch die Deutsche Marine den „Einstieg in unbemannte Systeme und künstliche Intelligenz" als notwendige Antwort auf die veränderte Bedrohungslage der Zeitenwende.[115] Die Übernahme von Aufgaben durch räumlich stärker verteilte kleine Plattformen und Verbünde aus kleinen Trägersystemen für Sensoren und Effektoren wie Waffen oder Störsendern,

115 *Deutsche Marine*, Kurs Marine 2035+, Rostock, 2023.

das Zusammenwirken innerhalb großer Systeme aus Datenerhebung, Einsatzmitteln und KI-gestützter Auswertung zur Unterstützung menschlicher Entscheidungen ist längst Realität in Gefechten – nicht nur in der Ukraine, sowie Bestandteil militärischer Planungen und verschiedener technischer Projekte.[116]

Dabei zeigt aber auch das Beispiel der Marine, dass Deutschland sehr viel mehr in maritime Sicherheit investieren muss, und wie zeitkritisch der erforderliche Kapazitätsaufbau ist. Der knappe deutsche Flottenbestand, in Verbindung mit den der NATO zugesagten Beiträgen zur regionalen Verteidigung in Nord- und Ostsee, lässt kaum Spielräume für globale Präsenz.[117] Es ist unter diesen Voraussetzungen eine Leistung, dass die Marine kurzfristig eine einsatzklare Fregatte für den ungeplanten EU-Einsatz ASPIDES zum Schutz von Handelsschiffen vor Angriffen im Roten Meer bereitstellen konnte.[118] Grundsätzlich gilt, eine ganzjährig eingeplante Einheit bindet rechnerisch – bei guter Instandhaltungsarbeit – den dreifachen Schiffsbestand in Wartung und Ausbildung.[119] Da es aber in der Flotte an Schiffen und Personal fehlt, erschöpfen beispielsweise zwei permanent in Nord- und Ostsee eingeplante Korvetten und drei Fregatten das Gros dessen, was die Marine an größeren hochseetauglichen, weltweit einsetzbaren Kampfschiffen zur Verfügung hat.

Offensichtliche Engpässe an Einsatzmitteln angesichts global und regional zunehmender Aufgaben sowie die Erkenntnisse aus dem Krieg in der Ukraine erfordern eine Neuausrichtung der Strategie zur Gewährleistung maritimer Sicherheit in Deutschland – und darüber hinaus. Dünn gesäte, teure, „maßgeschneidert" produzierte Kriegsschiffe werden in der Auseinandersetzung mit gleichwertigen Gegnern zwar immer noch benötigt, müssen aber dringend ergänzt werden um ferngelenkte oder (teil-)autonome Systeme, die kostengünstiger, in großer Zahl räumliche Lücken schließen

116 KI dabei als Werkzeug, dass den Menschen in die Lage versetzt, angesichts großer Datenmengen verantwortlich Entscheidungen zu treffen, vgl. *Koch*, Zur Causa Finalis künstlich intelligenter Waffen, in Barth, Hoff (Hrsg.), Digitale Welt – Künstliche Intelligenz – Ethische Herausforderungen, Verlag Karl Alber, 2023, S. 242-243.

117 Zu Flottenbestand und den eingegangenen Verpflichtungen, vgl. *Deutsche Marine* (Fn. 95); *Brake*, Von globaler Verantwortung zum strategischen Tunnelblick, MarineForum 04-2023.

118 Vgl. *Bundeswehr,* Operation Aspides: Luftverteidigung im Roten Meer, https://www.bundeswehr.de/de/organisation/marine/aktuelles/operation-aspides-luftverteidigung-rotes-meer-5746740, abgerufen am 15.03.2024.

119 *Deutsche Marine* (Fn. 95), S. 7.

und Bedrohungsszenarien durch unbemannte Angriffssysteme effizient begegnen können.

Im Zusammenspiel mit zivilen Behörden kommt der Marine eine zentrale Rolle auch bei maritimen Ordnungsfunktionen zu – vor allem bei hybriden Bedrohungen und in globaler Perspektive. Aufgrund der militärischen Qualität hybrider Bedrohungen und des geografisch unbegrenzten, globalen Ausmaßes maritimer Interessen, kommt eine zeitgemäße Anpassung der maritimen Sicherheitsarchitektur Deutschlands nicht ohne eine enge Integration der Marine aus. Als wertvolles Instrument deutscher Außenpolitik in der Zeitenwende muss sie mit ihrer Ausstattung und hinsichtlich des Rechtsrahmens in der Lage sein, die gesamte Bandbreite an Marineaufgaben abzudecken: Unterstützung der Diplomatie, Ordnungsfunktionen und militärische Abschreckung, bzw. Verteidigung.[120]

Mit dem Krieg in der Ukraine entlarvte sich Russland als gewalttätiger Aggressor in der unmittelbaren Nachbarschaft, dennoch hört die Welt nicht auf, weitere Krisen aufzuwerfen und die deutsche Außenpolitik vor globale Herausforderungen zu stellen. Im Gegenteil, mit eskalierender systemischer Rivalität, hybriden Bedrohungen bis hin zum offenen Krieg in der europäischen Nachbarschaft steigen die Herausforderungen auch global. Eine der größten Sorgen, für die außenpolitische Antworten gefunden werden müssen, steht in direkter Wechselwirkung mit Russlands Expansionspolitik – und stellt sie in den möglichen Folgen in den Schatten: Der Aufstieg Chinas in Verbindung mit einer möglichen Eskalation der Taiwan-Frage. Um hier hochgefährliche Kosten-Nutzen-Abwägungen in die richtige Richtung zu beeinflussen, braucht es frühzeitig deutliche Signale von möglichst vielen internationalen Partnern. Die globale systemische Rivalität, mit der Deutschland umgehen muss, hat dabei eine ganz zentrale maritime Dimension.

Deutschlands außenpolitisches Gewicht, internationale Verantwortung und Interessen erfordern, dass maritime Sicherheit global gedacht wird. Selbst in der Rivalität des Westens mit Russland muss die Aufmerksamkeit

120 Militärisch flankierte Diplomatie wird als „Verteidigungsdiplomatie" in den aktuellen Verteidigungspolitischen Richtlinien des BMVg bezeichnet. Dabei kann es sich für die Marine u.A. um Hafenbesuche, Ausbildungskooperationen, gemeinsame Manöver, aber auch humanitäre Hilfeleistungen handeln. Grundsätzlich hat aber jede Präsenz von Kriegsschiffen – kooperativ, abwartend oder auch drohend – eine diplomatische Dimension. Zu Verteidigungsdiplomatie in den aktuellen VPR, *BMVg*, Verteidigungspolitische Richtlinien 2023, S. 18; für Deutschland und seine Marine, vgl. *Brake* (Fn. 8), S. 49-54.

auch weit jenseits der heimischen europäischen Gewässer liegen. Die in Verbindung mit China und Russland gebrachten Fälle von Handelsschiffen, die allem Anschein nach mindestens seit Oktober 2023 mutwillig Beschädigungen und Zerstörungen einer Pipeline, mehrerer Datenkabel und des Stromkabels EstLink2 in der Ostsee verursachten, zeigen, dass Europas systemische Rivalen nicht nur im Roten Meer mit hybriden Methoden Schwachstellen ausnutzen.[121] Die maritime Vernetztheit der globalisierten Weltwirtschaft ermöglicht es dabei, Deutschland und Europa auch sehr empfindlich an geografisch weit entfernten Orten zu treffen. Jenseits des Schutzes von marKRITIS und von Seewegen – der Gewährleistung der für die freie Weltwirtschaft unverzichtbaren guten Ordnung auf See – darf auch der Meeresschutz als weiteres Element von Deutschlands Verantwortung für maritime Sicherheit nicht vergessen werden.

121 Siehe Fn. 2.