Aufsatz

Julian Pawlak*

Der Schutz maritimer kritischer Infrastrukturen und das Konzept der Abschreckung

https://doi.org/10.1515/sirius-2023-2005

Kurzfassung: Deutschland und der Westen stehen vor der Herausforderung, auch ihre maritimen kritischen Infrastrukturen (KRITIS) gegen Angriffe zu schützen. Lösungsansätze für den Schutz maritimer KRITIS lassen sich identifizieren im Rahmen von notwendiger Resilienz, ausreichend Redundanzen und einer übergreifenden Zusammenarbeit verschiedener Stakeholder, etwa zur effektiven Überwachung und Präsenz. Um erfolgreich zu sein, sollten solche Kooperationen über Staaten und ihre Streitkräfte hinausgehen und privatwirtschaftliche Akteure einbeziehen. Aus strategischem Blickwinkel wird zusammenfassend deutlich, dass der Schutz maritimer kritischer Infrastrukturen als ein Teil effektiver Abschreckung anzusehen ist.

Schlüsselwörter: Maritime Sicherheit, kritische Infrastruktur, maritime Infrastruktur, Resilienz, Redundanz, Abschreckung

Abstract: Germany and the West face the challenge of protecting their maritime critical infrastructures against attacks. Possible solutions for the protection of maritime critical infrastructures can be identified within the framework of necessary resilience, sufficient redundancies, and an overarching cooperation of different stakeholders, for example for effective monitoring and presence. Of particular importance is that this cooperation must go beyond nation states and their armed forces, to also include the private sector in order to be successful. In summary, from a strategic perspective, it must be recognized that the protection of maritime critical infrastructure must also be seen as a part of effective deterrence.

Keywords: Maritime Security, critical Infrastructure, maritime Infrastructure, resilience, redundancy, deterrence

1 Einleitung

Die Sabotage der Nord-Stream-Pipelines im September 2022 hat den Schutz kritischer Infrastrukturen (KRITIS) im maritimen Raum auf die Tagesordnung der sicherheitspolitischen Debatte gebracht. Die Angriffe in der zuvor in Anbetracht der Beitrittsverhandlungen Schwedens und Finnlands voreilig als „NATO-Meer“ bezeichneten Ostsee[1] unterstreichen die Vulnerabilität extra-terrestrischer Infrastrukturen. Sie werfen zudem ein Licht auf eine ganze Reihe von Unwägbarkeiten unterhalb der Meeresoberfläche beziehungsweise auf dem Meeresboden. Diesen Sabotageakt begleiteten weitere Ereignisse, die maritime kritische Infrastrukturen betrafen. Dazu gehörten die unbefugten Drohnenüberflügen über norwegische Offshore-Anlagen[2], die Abtrennung von 4,2 km an Unterseedatenkabel vor Spitzbergen[3] sowie die ebenfalls absichtlichen Beschädigungen von Unterseekabeln vor der französischen Mittelmeerküste.[4] In der Bundesrepublik verstärkte die Sabotage am Zugfunksystem der Deutschen Bahn die Aufmerksamkeit für kritische Infrastrukturen.[5] Bei all diesen Vorfällen besteht der Verdacht des Vorsatzes. Daher liegt die breite Aufmerksamkeit für den Schutz maritimer kritischer Infrastrukturen nicht mehr bloß auf Sicherheitsmaßnahmen gegen unabsichtliche oder natürliche Schadensgeschehen (Unfälle, menschliches Versagen, Naturereignisse) bei der Abwägung von wirtschaftlichen Faktoren oder Umweltschutz. Heute gilt es, den Schutz maritimer KRITIS vor vor-

***Kontakt: Julian Pawlak**, Wissenschaftlicher Mitarbeiter an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg und Koordinator des dortigen interdisziplinären Forschungsschwerpunkts Maritime Sicherheit (iFMS); E-Mail: pawlakj@hsu-hh.de

1 Julian Pawlak: „No, Don’t Call the Baltic a ‚NATO Lake‘“, *RUSI Commentary*, 5.9.2022.

2 Fears Grow as More Drones Appear above Norway’s Offshore Facilities, *Euronews*, 23.10.2022.

3 Atle Staalesen: ‚Human Activity‘ behind Svalbard Cable Disruption. *The Independent Barents Observer*, 11.2.2022.

4 Chris King: Serious Incident Involving CUT Underwater Cables in South of France Affects Internet Worldwide. *Euro Weekly News*, 23.10.2022.

5 Nach Sabotage – Bahnverkehr im Raum Norddeutschland normalisiert sich weiter. P*ressemitteilung der Deutschen Bahn*, 8.10.2022; https://www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/Nach-Sabotage-Bahnverkehr-im-Raum-Norddeutschland-normalisiert-sich-weiter-8960922.

sätzlicher Beschädigung, temporärem Ausfall oder dauerhafter Zerstörung durch staatliche Akteure sicherzustellen.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) definiert kritische Infrastrukturen als „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."[6] Zum Bereich maritimer KRITIS gehören insbesondere die beiden Sektoren Energie sowie Informations- und Kommunikationstechnologie (IKT).[7] Erhöhte Wachsamkeit ist angebracht beim weltweiten Netz an Unterseedatenkabeln[8], den Pipelines der Energieversorgung,[9] den *Offshore*-Energieinstallationen sowie den jeweiligen Transfer- und Transportrouten und den entsprechenden Anlande- und Verteilerstationen. Auf militärischer Seite hat man seit einigen Jahren auf die Risiken und Herausforderungen für maritime KRITIS, vor allem auch unterhalb der Wasseroberfläche, hingewiesen, ohne jedoch in der Politik Resonanz zu finden.[10] Häufig bezogen sich diese Warnungen auf entsprechende Fähigkeiten Russlands.[11] Speziell die Aktivitäten der russischen Seestreitkräfte[12] entlang bedeutender Unterseekabel beobachtete man skeptisch. Norwegische Medien konnten unter anderem anhand von AIS-Daten[13] *(Automatic Identification System)* unregelmäßige Bewegungen russischer Fischerboote im Bereich beschädigter Unterseekabel feststellen.[14]

In der strategisch und sicherheitspolitisch orientierten Wissenschaft werden die Risiken für maritime kritische Infrastrukturen häufig unter dem Oberbegriff „hybride Bedrohungen" subsumiert.[15] Mittlerweile hat man die maritimen Abhängigkeiten, von KRITIS bis zu Lieferketten und Energieversorgung, als *weaponized interdependence*[16] identifiziert, also als Verwendung von ökonomischen Abhängigkeiten als politische Waffe.[17] Eine kürzlich erschienene, für das Europäische Parlament erstellte Analyse gibt einen guten Überblick über die aktuellen Risiken für die Europäische Union.[18]

Es ist davon auszugehen, dass derzeit alle maritimen kritischen Infrastrukturen unzureichend gegen vorsätzliche Beschädigung geschützt sind. Dies gilt insbesondere mit Blick auf staatliche Akteure wie Russland, das derartige Fähigkeiten in den vergangenen 15 Jahren konsequent entwickelt hat. Der Schutz maritimer KRITIS findet auf zwei Ebenen statt: Erstens ist es der Schutz im Sinn von Resilienz und Redundanzen der KRITIS, der nach wie vor im Wesentlichen in der Verantwortung der privatwirtschaftlichen Betreiber liegt. Hier geht es darum, durch passiven Schutz und den Aufbau redundanter Strukturen die möglichen Konsequenzen einzelner Ausfälle so gering wie möglich zu halten. Zweitens ist es der Schutz durch Präsenz und Überwachung und gegebenenfalls durch aktives Eingreifen seitens staatlicher Stellen. Das bedeutet, dass kommerzielle und staatliche Akteuren kooperieren müssen. Denn wegen der geographischen Lage dieser Infrastrukturen, die sich zu weiten Teilen auf dem Meeresboden der Hohen See und damit außerhalb hoheitlicher Territorialgewässer befinden, stellt der Schutz dieser Strukturen eine besondere Herausforderung dar und verlangt komplexe internationale Absprachen. Dieser Artikel zeigt im Rahmen einer Bestandsaufnahme von Risiken und Gegenmaßnahmen auf, dass auch dieser Herausforderung strategisch und im internationalen Verbund mit dem Konzept der Abschreckung zu begegnen ist.

6 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (o. J.): Was sind Kritische Infrastrukturen und warum sind sie so wichtig?; https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html.

7 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (o. J.): Sektoren und Branchen KRITIS. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html.

8 Eine Übersicht über das globale Netz an Unterseekabeln bietet https://www.submarinecablemap.com/.

9 Hier insbesondere die Gasinfrastruktur inkl. Flüssiggas (LNG), einsehbar unter https://globalenergymonitor.org/projects/global-gas-infrastructure-tracker/tracker/.

10 Franz-Stefan Gady: Russian Submarine Activity at Highest Level Since Cold War. *The Diplomat*, 5.2.2016; siehe auch die thematische Aufsatzsammlung des *Center for International Maritime Security* (CIMSEC) zu „Seabed Warfare": https://cimsec.org/seabed-warfare-week/.

11 H. I. Sutton: Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables, *Naval News*, 19.8.2021.

12 Michael Birnbaum: Russian Submarines Are Prowling around Vital Undersea Cables. It's Making NATO Nervous, *Washington Post*, 22.12.2017.

13 Das *Automatic Identification System* (AIS) ist ein System zum Austausch von u. a. Navigationsdaten im Schiffsverkehr.

14 Benjamin Fredriksen/Beth Mørch Pettersen/Gyda Katrine Hesla/Inghild Eriksen/Håvard Gulldahl: Russiske trålere krysset begge kablene før forbindelsen forsvant, *Norsk rikskringkasting (NRK)*, 26.6.2022; https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-for-brudd-1.16007084.

15 Murphy/Hoffmann/Schaub 2016.

16 Farrell/Newman 2019.

17 Siehe dazu die Konferenz des interdisziplinären Forschungsschwerpunkts Maritime Sicherheit (iFMS) an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg zum Thema „Maritime Sicherheit zwischen Weaponized Interdependence und Geo-Economics" unter https://www.hsu-hh.de/ifms/konferenzen/.

18 Bueger/Liebetrau/Franken 2022.

2 Resilienz und Redundanzen

Die in der Auseinandersetzung mit hybriden Bedrohungen häufig verwendeten *buzzwords* „Resilienz“ und „Redundanzen“ haben auch im Rahmen des Schutzes maritimer kritischer Infrastruktur ihre Gültigkeit. Konkret bedeutet der Ruf nach mehr Resilienz und Redundanzen maritime kritische Infrastrukturen zu härten, stärker gegen physische wie auch digitale Gefahren zu sichern sowie durch erhöhte Diversifizierung parallele Strukturen zu errichten. Vergleichbares gilt für die Energieerzeugung, bei der besonders Transferrouten oder Verteiler und Knotenpunkte betroffen wären. Ziel muss es sein, die Auswirkungen einer einzelnen Störung beziehungsweise eines einzelnen Schadensvorfalls – sei es ein Naturereignis, menschliches Versagen oder mutwillige Beschädigung beziehungsweise Zerstörung – auf die KRITIS zu minimieren.

Offshore Windkraftanlage Anholt vor der dänischen Küste

Das gilt vor allem für maritime kritische Infrastrukturen des Energiesektors. Nach Plänen der Bundesregierung sollen, um bis 2045 das Ausbauziel für Windenergie auf See zu erreichen, mindestens 70 Gigawatt durch Offshore-Windkraftanlagen erzeugt werden.[19] Die Energie muss von den Standorten in den deutschen Küstenregionen über See- und Landkabel und entsprechende Trassen sowie Konverter-Stationen zum Festland übertragen werden. Hier sollte man erwägen, solche Unterseekabel diversifizierter zu verlegen als bisher. Denn nur so ließe sich verhindern, dass einzelne Schadensereignisse gebündelte Kabeltrassen außer Betrieb setzen. Ähnliche Aufmerksamkeit ist angebracht bei Konverter-Stationen und Anlandepunkten von Datenkabeln, die aufgrund ihrer Position am Festland ein einfaches Ziel für potenzielle Angreifer darstellen könnten. Wie es Häfen für Seewege sind, so sind auch Anlandestationen für See- und Datenkabel die vulnerablen, neuralgischen Punkte, an denen unterschiedliche Routen von See und Festland zusammenlaufen. Diese gilt es zu schützen und durch eine Lastenverteilung zu diversifizieren.[20] Welche Herausforderungen der redundante Ausbau maritimer KRITIS mit sich bringt, zeigt die Entscheidung der Bundesregierung, die fünf LNG-Terminals an vier unterschiedlichen Standorten[21] errichten zu lassen. Dadurch entstehen vermeintliche „Überkapazitäten,“ die Resilienz bewirken.[22]

2.1 Digitale Sicherheit

Neben physischer Resilienz ist der Schutz der IT-Sicherheit im Auge zu behalten. Das Beispiel des Cyber- beziehungsweise Ransomware-Angriffs auf die *Deutsche Windtechnik* im April 2022 lässt erkennen, wie solchen Bedrohungen effektiv begegnet werden kann. Obwohl der Angriff dafür sorgte, dass die Kommunikation zu 2.000 Windrädern in der Nordsee für zwei Tage abgeschaltet werden musste, hat er keine nennenswerten Schäden verursacht.[23] Denn zum einen ist das IT-System des Betreuungsunternehmens so dezentral organisiert, dass dieser Angriff nahezu isoliert bearbeitet werden konnte. Zum anderen erlaubte die Einstellung der Windkraftanlagen auch bei Kommunikationsverlust einen autonomen Weiterbetrieb, sodass weiterhin Energie eingespeist werden konnte.[24] Der Fall zeigt, dass bereits *by design* resilient sowie redundant aufgebaute Systemstrukturen helfen können, Auswirkungen von Angriffen zu minimieren, die darauf abzielen, diese Strukturen temporär oder langfristig auszuschalten.

19 Siehe Bundesregierung: Mehr Windenergie auf See. https://www.bundesregierung.de/breg-de/themen/klimaschutz/windenergie-auf-see-gesetz-2022968.

20 Eine Diversifizierung von Datenkabel- durch Ausweichen auf Satellitenkommunikation ist hier aufgrund der vergleichsweise geringen Bandbreite der Datenübertragung höchstens für einzelne, spezifische Anwendungsfälle, wie etwa bei Streitkräften, eine Option.

21 Zwei Terminals in Wilhelmshaven, jeweils eines in Brunsbüttel, Stade und Lubmin.

22 Catiana Krapp: Flüssiggas: Bei LNG drohen Überkapazitäten – baut Deutschland zu viele Terminals? *Handelsblatt*, 4.1.2023.

23 Deutsche Windtechnik: Cyber-Angriff auf Deutsche Windtechnik. *Pressemeldung Deutsche Windtechnik AG,* 22.4.2022; https://www.deutsche-windtechnik.com/news/aktuelles/detail/cyber-angriff-auf-deutsche-windtechnik/.

24 Dirk Knop: Cyber-Angriff – Fernüberwachung von Windkraftanlagen lahmgelegt. *Heise online*, 27.4.2022; https://www.heise.de/news/Cyber-Angriff-legte-offenbar-Windturbinen-lahm-7066606.html.

Eine andere Dimension der Sicherheit ist die Frage, ob und wieweit sich bei Ausschreibungen für Aufbau und Unterhaltung maritimer kritischer Infrastrukturen bedenkliche Firmen berücksichtigen lassen. In der deutschen Debatte um die digitale Sicherheit kritischer Infrastrukturen sorgte kürzlich der 5G-Netzausbau durch den chinesischen Anbieter *Huawei* für Aufregung. Diese Sorge ist auch bei maritimer kritischer Infrastruktur angebracht, denn *Huawei* ist heute gemeinsam mit weiteren chinesischen Unternehmen ein bedeutender Anbieter von Unterseekabeln, die auch als Teil einer „digitalen Seidenstraße" bezeichnet werden.[25] Infolge des Ausschlusses *Huaweis* von verschiedenen europäischen Infrastrukturprojekten[26] und vor dem Hintergrund der weiter wachsenden globalen Bedeutung[27] von Unterseekabeln änderte *Huawei Marine Networks* bereits im Jahr 2020 seinen Namen in *HMN Technologies*.[28] Der neue Name ändert jedoch nichts an dem Problem: Risiken für maritime kritische Infrastruktur liegen nicht nur in der Gefahr der Beschädigung oder Zerstörung, sondern auch in der Kontrolle wichtiger Technologien durch ausländische Konzerne, die eng mit der chinesischen Regierung kooperieren. Ebenfalls gilt zu beachten, wer durch den Ausbau von KRITIS oder die technologische Beteiligung möglicherweise erleichterten Zugang zu Daten erhalten kann. Das umfasst das eventuelle Anzapfen von Datenströmen in Unterseekabeln, das sogenannte *tapping*.[29]

2.2 Resilienz durch Reparaturfähigkeiten

Letztlich wird Resilienz auch durch Reparaturfähigkeit untermauert. Bei Unterseedatenkabeln ist die Verfügbarkeit von Schiffen mit Befähigung zur Reparatur eine kritische Größe. Global gesehen ist die Flotte an *Cableships* derzeit im Verhältnis zur Menge und Länge vorhandener Datenkabel klein.[30] Die Reparatur von Seekabeln bildet mittlerweile einen separaten Industriezweig. Gemeinsam mit den Betreibern und Eigentümern von Unterseekabeln werden vertragliche Regelungen für etwaige Störungen getroffen.[31] Die räumliche Verantwortungszuweisung findet durch eine global verteilte Organisation statt: für den atlantischen Raum etwa durch das *Atlantic Cable Maintenance & Repair Agreement* (ACMA) von 1965, das über drei *Cableships* verfügt, von denen zwei in Europa und eines auf den niederländischen Antillen stationiert sind.[32] Gemeinsam mit den beiden Schiffen unter dem *Mediterranean Cable Maintenance Agreement* (MECMA) sind in Europa vier *Cableships* stationiert.[33]

Das 1983 in Dienst gestellte Kabelschiff USNS Zeus

Es ist zu Recht bemängelt worden, dass vier Schiffe bei weitem nicht genügen und es nicht unproblematisch ist, dass sie sich in privatwirtschaftlicher Hand befinden. In Großbritannien und den USA hat man bereits erste Maßnahmen eingeleitet, um dies zu verbessern. So wird derzeit in Liverpool das erste *Multi-Role Ocean Surveillance Ship* (MROSS) für die *Royal Fleet Auxiliary*, die Unterstützungskräfte der *Royal Navy*, umgerüstet. Außerdem wird in Großbritannien ein zweites MROSS völlig neu konstruiert und gebaut.[34] Da der aktuelle britische Premierminister Rishi Sunak erst 2017 als *Member of Parliament* eine Studie zum Schutz von Unterseekabeln veröffentlichte,[35] kommt die Entscheidung für ein zweites MROSS anstatt einer neuen *Royal Yacht* wenig überraschend.[36] Die US Navy verfügt

25 Siehe Bueger/Liebetrau 2021, 404, mit Verweis auf Shen 2018.

26 Kauranen/Mukherjee: UPDATE 1-Finland Approves Law to Ban Telecoms Gear on Security Grounds, *Reuters News*, 7.12.2020.

27 Grand View Research 2022.

28 HMN Technologies: Huawei Marine Networks Rebrands as HMN Technologies, Pressemeldung vom 3.11.2020; https://www.hmntechnologies.com/enPressReleases/37764.jhtml.

29 Caleb Larson: How a US Navy Submarine Secretly Tapped Russia's Undersea Cables. *The National Interest*, 26.7.2021.

30 Eine Übersicht von *Cableships* ohne Anspruch auf Vollständigkeit bietet das International Cable Protection Committee: https://www.iscpc.org/information/cableships-of-the-world/. Zur Verfügbarkeit von Reparaturschiffen siehe auch Dan Swinhoe: The cable ship capacity crunch. DatacentreDynamics, 6.12.2022; https://www.datacenterdynamics.com/en/analysis/the-cable-ship-capacity-crunch/.

31 Bueger/Liebetrau/Franken 2022, 28.

32 https://www.acma2017.com.

33 https://www.mecmamc.org/public/#.

34 Schutz maritimer Infrastruktur: erstes Schiff bei Royal Navy eingetroffen, *MarineForum*, 23.1.2023; https://marineforum.online/royal-navy-erstes-schiff-zum-schutz-kritischer-infrastruktur-eingetroffen/.

35 Sunak 2017.

36 Aubrey Allegretti: Sunak Sinks New Royal Yacht Plan in Favour of Ocean Surveillance Ship, *The Guardian*, 7.11.2022.

zurzeit über lediglich ein aktives *Cableship*, die *USNS Zeus* des *Military Sealift Command*. Man hat bereits gefordert, die Reparaturfähigkeit von Unterseekabeln als *wartime necessity* anzuerkennen.[37] Und tatsächlich gingen die USA Anfang 2022 einen Vertrag zur *Cable Security Fleet*[38] ein, der zwei zivile, aber mit US-Flagge und -Besatzung ausgestattete Schiffe privatwirtschaftlicher Betreiber verpflichtet, im Kriegs- oder Notstandsfall binnen 24 Stunden zur Verfügung zu stehen. Für eine vertraglich zugesicherte Gebühr von jeweils 5 Millionen US-Dollar jährlich umgehen die USA somit mögliche Konflikte mit kommerziellen Betreibern, die womöglich wegen nationaler Vorbehalte, versicherungstechnischer Gründe oder ihrer aktuellen Auftragslage nicht schnell genug akute Probleme von Unterseekabeln beheben könnten.[39]

3 Präsenz und Überwachung

Jegliche Härtung von kritischen Infrastrukturen macht wenig Sinn, wenn unbefugter Zugang uneingeschränkt möglich ist. Aus diesem Grund ist die aktive Überwachung von Seegebieten als Teil einer *Maritime Domain Awareness* und maritimer kritischer Infrastrukturen im Besonderen notwendig. Allerdings deckte die Sabotage von *Nord Stream* auf, dass weder die Deutsche Marine noch die europäischen beziehungsweise NATO-Seestreitkräfte in der Lage sind, das globale Netz an Unterseekabeln und Pipelines rund um die Uhr zu überwachen oder gar zu schützen. Doch auch die kommerziellen Betreiber und Eigentümer maritimer kritischer Infrastrukturen sind nicht imstande, außer auf die bereits bestehenden kriminellen und terroristischen Risiken nun eigenständig auch noch auf Bedrohungen durch Fähigkeiten staatlicher oder staatlich beauftragter Akteure zu reagieren. Das macht eine intensivere Zusammenarbeit von staatlichen Behörden und Streitkräften mit der Privatwirtschaft beziehungsweise den Eigentümern und Betreibern maritimer kritischer Infrastrukturen unerlässlich. Letztere haben den Zugriff auf die Infrastrukturen und können zusätzliche Monitoringmaßnahmen vornehmen. Diese reichen von optischer Überwachung wie zusätzlicher Videoüberwachung an *Offshore*-Energieanlagen bis hin zu hochentwickelter, fest installierter Sensorik unterhalb der Meeresoberfläche, über die Daten etwa mit der Deutschen Marine oder einer übergeordneten Stelle auf NATO- oder EU-Ebene geteilt werden könnten. Seestreitkräfte wie die Deutsche Marine könnten über die Amtshilfe in den nationalen Territorialgewässern hinaus auch auf Hoher See und in Ausschließlichen Wirtschaftszonen (AWZ) ihren Beitrag leisten. Durch ihre besondere Position repräsentieren sie souveräne staatliche Präsenz und verfügen über einzigartige Fähigkeiten, wie etwa die Aufklärung durch U-Boote. Ergänzen ließe sich dies durch den Einsatz unbemannter Systeme wie *Unmanned underwater vehicles* (UUVs) und *Unmanned aerial vehicles* (UAVs) über, auf und unter der Wasseroberfläche, die an Offshore-Anlagen oder Pipelines patrouillieren und Unstimmigkeiten frühzeitig identifizieren.[40]

Ein gutes Lagebild der maritimen Domäne gelingt nur in enger Zusammenarbeit. Aufgrund der begrenzten nationalen Quantitäten, aber auch aufgrund der zum Teil unklaren oder sich überschneidenden Zuständigkeiten außerhalb eigener Hoheitsgewässer muss diese Kooperation international strukturiert sein. Informationskanäle müssen nationale Behörden und Regierungen, internationale Organisationen (NATO, EU) sowie die Privatwirtschaft miteinander verbinden. Dabei geht es nicht nur um den Datenaustausch, sondern auch bei der Datenauswertung ist die Zusammenarbeit auszuweiten und zu optimieren. Ziel muss es sein, Kooperation und Monitoring mithilfe von Streitkräften und Industriepartnern, Polizeikräften und Küstenwachen, aber auch ergänzt durch externe Akteure und Satellitenbilder, so auszubauen, dass Vorfälle wie die kürzlich gesichteten Drohnenüberflüge über maritime kritische Infrastruktur unmittelbar gesichtet, geortet und anschließend identifiziert werden können. Die Tatsache, dass selbst für ein vergleichsweise kleines Seegebiet wie die Ostsee keine vollständige *Maritime Domain Awareness* existiert, demonstriert, wie komplex und ambitioniert, aber auch, wie notwendig diese Zielsetzung vor dem Hintergrund der aufgezeigten Herausforderungen ist.

4 Abschreckung und Attribution

Die beschriebenen Anforderungen für den Schutz maritimer kritischer Infrastrukturen lassen sich in ihrer Zielsetzung in das Konzept der Abschreckung einbetten.[41] Wenn maritime KRITIS gehärtet, resilienter und dezentraler konzipiert sowie durch Reparatur- und Überwachungsmaßnah-

37 Burnett 2022.

38 Burnett 2021, 1679–80.

39 Burnett 2022.

40 Daponte/Paladi 2023.

41 Eine übersichtliche Erläuterung zum Verständnis von Abschreckung bietet Mazarr 2021, siehe auch Mazarr/Cheravitch/Hornung/Pezard 2021 sowie Bergeron 2018, De Wijk 2018, Thomson 2018 sowie Rühle 2020.

men ergänzt werden, werden sich Störungen oder direkte Angriffe weniger leicht erfolgreich und unentdeckt durchführen lassen. Dadurch tragen solche Maßnahmen zu einer Abschreckung durch Versagung eines Erfolgs – *deterrence by denial* – bei. Allerdings kann es auch bei maritimen kritischen Infrastrukturen keine hundertprozentige Sicherheit im Sinn von Schutz vor Störungen oder Angriffen geben. Deswegen sollte man auch Maßnahmen der Abschreckung durch Bestrafung beziehungsweise durch Reaktionen – *deterrence by punishment* – in Betracht ziehen. Es ist sehr ratsam, über eine ausgeglichene Abschreckungsbalance zwischen *denial* und *punishment* zu verfügen.[42] Nur so kann man das Kosten-Nutzen-Kalkül potenzieller Angreifer besser beeinflussen, wenn man seine maritimen kritischen Infrastrukturen schützen will. Die NATO formulierte zwar bereits im Rahmen des Gipfels von Warschau 2016, dass die Abwehr von hybriden Bedrohungen den Mitgliedsstaaten obliegt.[43] Sie unterstrich im Communiqué von Brüssel im Jahr 2021 jedoch, dass auch bei hybriden Angriffen ähnlich wie bei einem bewaffneten Angriff der Artikel 5 Anwendung finden könnte.[44] Die Reaktion muss nicht kinetischer Natur sein, denn rechtlich werden die Voraussetzungen für einen potenziellen Gegenschlag im Sinn der Selbstverteidigung ähnlich eines bewaffneten Angriffs bewertet und anhand ihrer Angemessenheit und Notwendigkeit gemessen.[45] In Bezug auf die Abschreckungstheorie gilt es in der wissenschaftlichen Debatte als gesichert, dass die Drohung des *punishment* in jedem Fall glaubhaft und mit entsprechenden Fähigkeiten hinterlegt sein muss.

In diesem Zusammenhang werden allerdings die Herausforderungen deutlich, die mit einer Abschreckungsstrategie verbunden sind: Zunächst ist der Umgang mit extra-terrestrischer beziehungsweise extra-territorialer maritimer kritischer Infrastruktur auch international zwischen den Partnerstaaten eindeutig zu definieren. Das gilt für Verantwortungsbereiche und Zuständigkeiten im übergreifenden europäischen und NATO-Rahmen. Darüber hinaus muss das benötigte Fundament der Abschreckung durch Erfolgsversagung, also die *Denial*-Fähigkeit in Form von Resilienz, Redundanzen, *Monitoring* und *Awareness* so glaubhaft ausgereift sein, dass die Identifikation etwaiger Angreifer nachweislich möglich ist, um die *Punishment*-Fähigkeit ebenfalls glaubhaft nach außen kommunizieren zu können.[46] Diese Problematik erinnert sehr an das Attributionsproblem, das Angriffe im Cyberraum mit sich bringen.[47] Die Autoren einer Studie des *International Center for Defence and Security (ICDS)* empfehlen dafür ein entsprechendes Update der *Counter-hybrid*-Strategie der NATO. Wichtig sei es, sich bereits im Vorfeld auf eindeutige Reaktionen auf spezifische, selbst schwierig zuzuschreibende hybride Aktivitäten festzulegen.[48] Das würde potenziellen staatlichen Akteuren offen mögliche Konsequenzen ihres Handelns aufzeigen und der Allianz zusätzliche Optionen bieten, auch unterhalb der Schwelle zum Artikel 5-Verteidigungsfall gezielt und methodisch abgestimmt reagieren zu können.

5 Ausblick

Der Schutz kritischer Infrastrukturen, maritim oder terrestrisch, ist in der sicherheitspolitischen Debatte sowie auf der politischen Tagesordnung angekommen. Die Bedeutung und Anzahl kritischer Infrastruktur sowohl im Bereich der *Offshore*-Energieerzeugung als auch im Bereich der Unterseedatenkabel wird perspektivisch weiter steigen. Aufgrund der *weaponizable interdependence* sind Wirtschaft und Politik in der Pflicht, neben ökonomischen und anderen Faktoren wie dem Naturschutz gleichermaßen Sicherheitsbedrohungen in ihre Kalkulationen für den Auf- und Ausbau von KRITIS einzubeziehen. Die politischen Rahmenbedingungen müssen übergeordnet von europäischer Ebene über staatliche Stellen an KRITIS-Betreiber weitergegeben werden. Die für 2024 geplante Verabschiedung einer europäischen Richtlinie über die Resilienz kritischer Einrichtungen (EU RCE) ist derzeit in Arbeit und die Bundesregierung bereitet das erforderliche KRITIS-Dachgesetz bereits vor. Nur so ist eine Umsetzung zusätzlicher Schutzmaßnahmen durch die privatwirtschaftlichen Betreiber zu garantieren. Mit Blick auf die beschriebene zweite Ebene des Schutzes maritimer Infrastrukturen – Präsenz, Überwachung, Abschreckung – ist eine rasche Einigung

42 Shala/Jackson/Hui/Sprague 2022, 2 und 6.

43 NATO: Warsaw Summit Communiqué Issued by NATO Heads of State and Government. 9.7.2016; https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

44 NATO: Brussels Summit Communiqué Issued by NATO Heads of State and Government, 14.6.2021; https://www.nato.int/cps/en/natohq/news_185000.htm.

45 Danae Azaria/Geir Ulfstein: Are Sabotage of Submarine Pipelines an ‚Armed Attack' Triggering a Right to Self-Defence? *EJIL: Talk! (blog),* 18.10.2022; https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/.

46 Dies orientiert sich auch an dem Ansatz der *deterrence by detection*: er basiert auf der Prämisse, dass Gegner von etwaigen Aggressionen abgeschreckt werden, wenn ihnen vor Augen geführt wird, dass sie, beispielsweise in bestimmten Operationsgebieten, durchgängig beobachtet und ihre Aktivitäten somit ausführlich dokumentiert und veröffentlicht werden können. Siehe dazu: Mahnken/Sharp/Kim 2020, 6.

47 Bendiek/Schulze 2021.

48 Shala/Jackson/Hui/Sprague 2022, 8–12.

hinsichtlich der Arbeitsteilung notwendig. Dies gilt einerseits auf der nationalen Ebene für die Koordination der sektorenübergreifenden Zusammenarbeit zwischen Akteuren wie der Deutschen Marine, der Bundespolizei und den Landespolizeistellen bis hin zu den übergeordneten Einrichtungen, darunter Bundesministerium der Verteidigung, Bundesministerium des Innern und für Heimat, BBK und weitere involvierte Behörden und Stellen. Angesichts des unvermindert wachsenden Aufgabenspektrums bei limitierter Verfügbarkeit von seegehenden Einheiten der Deutschen Marine ist die internationale Koordination von besonderer Bedeutung. Auf bilateraler Ebene bietet der deutsch-dänische Aktionsplan vom August 2022 Handlungsoptionen für eine engere Zusammenarbeit auch beim Schutz maritimer kritischer Infrastruktur.[49] Des Weiteren eröffnen Institutionen wie die Europäische Union und die NATO zusätzliche Möglichkeiten, eine Arbeitsteilung zu realisieren. Eine zielführende sowie vergleichsweise zügig umzusetzende Lösung wäre zum Beispiel eine *EU Cable Security Fleet* nach US-amerikanischem Vorbild. Die NATO bietet durch die bereits bestehende militärische Verflechtung mit ihren Bündnismitgliedern eine Möglichkeit, um Informationen der Allianzmitglieder und ihrer Partner zu bündeln und zu koordinieren. Eine wichtige Rolle spielt der im Februar 2023 vorgestellte Plan, eine Koordinationszelle im NATO-Hauptquartier zu errichten, um besser Verwundbarkeiten identifizieren und den Kontakt mit privatwirtschaftlichen Betreibern intensivieren zu können. Auf europäischer Ebene sollen im Rahmen der EU RCE Kooperation und Informationsaustausch nicht nur gefördert, sondern unter bestimmten Voraussetzungen auch vorgeschrieben werden. Und der im Januar 2023 gestarteten EU-NATO Task Force für die Resilienz kritischer Infrastrukturen wird es hoffentlich gelingen, die bereits existierenden Maßnahmen institutionenübergreifend zusammenzuführen und perspektivisch den Schutz vor und insbesondere die Abschreckung von Angriffen auf maritime KRITIS zu optimieren.

Literatur

Bendiek, Annegret/Schulze, Matthias (2021): *Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW*. Berlin: Stiftung Wissenschaft und Politik (SWP Research Paper)

Bergeron, James Henry (2018): Die Dynamik der Abschreckung, *Sirius – Zeitschrift für Strategische Analysen*, 2 (1), 21–31

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

Bueger, Christian/Liebetrau, Tobias/Franken, Jonas (2022): *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*. European Parliament In-Depth Analysis. Brüssel: Europaparlament; https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Burnett, Douglas R. (2021): Submarine Cable Security and International Law, *International Law Studies* 97, 1659–1682

Burnett, Douglas R. (2022): Repairing Submarine Cables Is a Wartime Necessity. *Proceedings* of the US Naval Institute, 148 (10). 1436 f.

Daponte, Pasquale/Paladi, Florentin (2023): *Monitoring and Protection of Critical Infrastructure by Unmanned Systems*. Washington, D.C.: IOS Press, (NATO Science for Peace and Security Series – D: Information and Communication Security)

De Wijk, Rob (2018): Die Rolle von Abschreckung im neuen strategischen Umfeld Europas, *Sirius – Zeitschrift für Strategische Analysen,* 2 (1), 3–20

Farrell, Henry/Newman, Abraham L (2019): Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security,* 44 (1), 42–79

Grand View Research (2022): *Submarine Cable Market Size Report, 2022–2030*. San Francisco, Cal.: Grand View Research; https://www.grandviewresearch.com/industry-analysis/submarine-cables-market

Hong, Shen (2019): Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative, *International Journal of Communication,* 12, 2683–2701

Mahnken, Thomas G./Sharp, Travis/Kim, Grace B. (2020): *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition.* Washington, D.C.: Center for Strategic and Budgetary Assessments (CSBA)

Mazarr, Michael J. (2021): *Understanding Deterrence*. In: Osinga, Frans/Sweijs, Tim (Hrsg.): NL ARMS Netherlands Annual Review of Military Studies 2020. Den Haag: T.M.C. Asser Press, 13–28

Mazarr, Michael J./Cheravitch, Joe/Hornung, Jeffrey W./Pezard, Stephanie (2021): *What Deters and Why? Applying a Framework to Assess Deterrence of Gray Zone Aggression.* Santa Monica, Cal.: The RAND Corporation

Murphy, Martin/Hoffman, Frank G./Schaub, Gary Jr. (2016): *Hybrid Maritime Warfare and the Baltic Sea Region.* Kopenhagen: Centre for Military Studies, University of Copenhagen; https://cms.polsci.ku.dk/publikationer/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf

Rühle, Michael (2020): Die (unvollkommene) Rückkehr der Abschreckung, *Sirius – Zeitschrift für Strategische Analysen*, 4 (4), 387–398

Shala, Arelena/Jackson, Bradley/Hui, Johannes/Sprague, Dave (2022): *A Better Balance. Imposing Costs on Hybrid Aggressors in the Baltic States*. Tallinn: ICDS (Policy Paper)

Sunak, Rishi (2017): *Undersea Cables. Indispensable, insecure*. London: Policy Exchange. https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

Swistek, Göran/Paul, Michael (2023): *Geopolitik im Ostseeraum. Die „Zeitenwende" im Kontext von kritischer maritimer Infrastruktur, Eskalationsgefahren und deutschem Führungswillen*. Berlin: Stiftung Wissenschaft du Politik (SWP-Aktuell)

Thomson, James A. (2018): Abschreckung einst und heute, *Sirius – Zeitschrift für Strategische Analysen*, 2 (1), 32–41

49 Swistek/Paul 2023.