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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

> 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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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 "BreNOS" (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).

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

(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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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 Backup-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)

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -

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.

https://doi.org/10.5771/9783748953494-105 https://www.inlibra.com/de/agb - Open Access -