4. Kapitel: Staatenhaftung für informationstechnische Systeme

Die Rechtsquellenanalyse hat bewiesen, dass eine völkerrechtliche Staatenhaftung, wie sie von der Völkerrechtskommission ursprünglich konzipiert wurde, keineswegs eine deplatzierte Schwerpunktsetzung im völkerrechtlichen Diskurs um staatliche Einstandspflichten darstellt, sondern eine Lösung für die Regulierung von transnationalen Gefährdungslagen bietet. Eine Gesamtschau der Rechtsquellen verdeutlicht allerdings, dass das Konzept der Staatenhaftung im Umweltvölkerrecht zu verorten ist. Daher ist zunächst die Möglichkeit einer analogen Anwendung der bestehenden umweltvölkerrechtlichen Staatenhaftung auf die virtuelle Welt zu untersuchen (A.), um sodann die konkrete Umsetzung der Staatenhaftung für informationstechnische Systeme beschreiben zu können (B.).

A. Anwendbarkeit von Umweltvölkerrecht in der virtuellen Welt

Die Analogie ist Ausdruck grundlegender Gerechtigkeitserwägungen, die ein elementarer Bestandteil der Völkerrechtsordnung sind.[1] Sie beruht auf dem Postulat, dass Gleichartiges rechtlich gleich zu behandeln ist.[2] In diesem Sinne ist die Analogie besonders geeignet, die Defizite bei

---

1 Ausführlich zur (umstrittenen) Zulässigkeit der Analogie im Völkerrecht *A. Bleckmann*, Analogie im Völkerrecht, AVR 17 (1977), S. 161 (161 ff.); *ders.*, Grundprobleme und Methoden des Völkerrechts, 1982, S. 198 ff., 227 ff.; *G. Dahm/J. Delbrück/R. Wolfrum*, Völkerrecht, Band I/1 Die Grundlagen. Die Völkerrechtssubjekte, 1989, S. 80 ff.; *U. Fastenrath*, Lücken im Völkerrecht, 1991, S. 136; *C. L. Riemer*, Staatengemeinschaftliche Solidarität in der Völkerrechtsordnung, 2003, S. 294 f.; *A. Verdross*, Die Verfassung der Völkerrechtsgemeinschaft, 1926, S. 71; *S. Vöneky*, Analogy in International Law, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 7 ff. Die Analogie wird unterdessen nicht nur als allgemeiner Rechtsgrundsatz, sondern auch als Rechtsquelle qualifiziert. So *A. Bleckmann*, Analogie im Völkerrecht, AVR 17 (1977), S. 161 (169); *ders*., Zur Feststellung und Auslegung von Völkergewohnheitsrecht, ZaöRV 37 (1977), S. 504 (516); *ders*., Die Aufgaben einer Methodenlehre des Völkerrechts, 1978, S. 43; *ders.*, Grundprobleme und Methoden des Völkerrechts, 1982, S. 250.

2 *U. Fastenrath*, Lücken im Völkerrecht, 1991, S. 134; *K. Larenz/C.-W. Canaris*, Methodenlehre der Rechtswissenschaft, 1995, S. 202.

der völkerrechtlichen Regulierung von völkerrechtlich nicht verbotenen Informationsoperationen auszugleichen. Analogiebasis, Analogiebedürfnis und eine ausreichende Vergleichbarkeit zwischen umweltspezifischer und informationstechnischer Problemlage zeigen, dass die Staatenhaftung die rechtliche Lücke in der virtuellen Welt im Wege der Analogie schließt.[3]

I. Analogiebasis

Das Völkerrecht kennt zwei Analogiearten, die sich nach der Breite der Analogiebasis unterscheiden. Bei der Einzelanalogie steht eine einzelne Bestimmung zur Verfügung, die als Ausdruck eines allgemeineren Prinzips angesehen wird und sich damit zur Übertragung auf einen bislang ungeregelten Sachverhalt eignet, während bei der Gesamtanalogie aus mehreren Bestimmungen ein übergreifender Rechtsgedanke gewonnen wird, der sich dann auf andere ungeregelte Fälle erstrecken kann.[4] Die Analogiebasis ergibt sich vorliegend aus den in Kapitel 1 (Staatenhaftung in der Systematik des Völkerrechts) beleuchteten umweltspezifischen Bestimmungen, die sich – wie in Kapitel 2 B. (Konstitutive Elemente der Staatenhaftung) gezeigt – zu einem Konzept der Staatenhaftung für erhebliche grenzüberschreitende Schäden durch völkerrechtlich nicht verbotene Aktivitäten zusammenfassen lassen. Da das Umweltvölkerrecht spezielle Problemlagen erfasst, ist nicht ohne Weiteres evident, dass diese Basis für eine Gesamtanalogie zur Lösung virtueller Konflikte geeignet ist.[5] Dies ergibt sich aber aus der Erwägung, dass das Umweltvölkerrecht eine ähnliche Entwicklung durchlief, wie sie das Völkerrecht der virtuellen Welt nun durchläuft.[6] Die ersten Umweltbelastungen verursachten internationale Problemlagen, ohne dass darauf zugeschnittene völkerrechtliche Regeln bereitstanden. Im Gegenteil war ein Rückgriff auf allgemeine Rechtsgrundsätze des Völker-

3 Zu den Voraussetzungen einer Analogie im Völkerrecht siehe *C. L. Riemer*, Staatengemeinschaftliche Solidarität in der Völkerrechtsordnung, 2003, S. 295 f.; *S. Vöneky*, Analogy in International Law, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 4 f., 12 ff.

4 *A. Bleckmann*, Analogie im Völkerrecht, AVR 17 (1977), S. 161 (176); *U. Fastenrath*, Lücken im Völkerrecht, 1991, S. 134.

5 Vgl. *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (480 f.).

6 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (130 f.).

rechts notwendig. Gleichzeitig erforderten und erfordern internationale Umweltprobleme Reaktionsmaßnahmen, die dem technologischen und gesellschaftlichen Wandel gerecht werden.[7] Dementsprechend besteht das Umweltvölkerrecht aus einem Konglomerat von völkervertraglichen und völkergewohnheitsrechtlichen Regeln sowie allgemeinen Rechtsgrundsätzen, das den Staaten durch ausreichende Rechtssicherheit ermöglicht, das nationale Regelungsumfeld so zu gestalten, dass Wirtschaft und Industrie funktionsfähig bleiben, und das gleichzeitig flexibel genug ist, um Schutz vor internationalen Umweltbelastungen zu bieten.[8] Die virtuelle Welt steht ebenso vor unwägbaren und sich stetig weiterentwickelnden Konfliktlagen, deren Reglementierung mit der rasanten technologischen Entwicklung mithalten und gleichzeitig genügend Rechtssicherheit für ihre ökonomische Nutzung bieten muss.[9] Folglich kann der Regelungsansatz des Umweltvölkerrechts perspektivisch eine passende Regulierung von informationstechnischen Systemen bieten.[10] An dieser Stelle dienen insbesondere die Umweltgrundsätze als Basis für eine mögliche Analogie, denn diese erweitern aufgrund ihres Prinzipiencharakters[11] das Regelungspotential des Völkerrechts.[12] Die Bedeutung der Umweltgrundsätze für eine Analogie wird zudem durch den Umstand gestützt, dass diese eine Art Renaissance erleben,[13] die mit einer schwindenden Bedeutung von völkervertraglichen Übereinkünften zur Reglementierung neuartiger Umwelt-

7 *Id.*, S. 129 (131); *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (481 f.).

8 *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (481 f.).

9 *Id.*, S. 465 (481).

10 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (134 f.); *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 210; *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (481). Auch die Experten des Tallinn Manual 2.0 bestimmen die Sorgfaltspflicht im virtuellen Raum explizit in Analogie zum Umweltrecht. Tallinn Manual 2.0, Kommentar zu Regel 6, S. 36 f., Rn. 25.

11 Siehe 1. Kapitel E. V.

12 Vgl. *U. Fastenrath*, Lücken im Völkerrecht, 1991, S. 125.

13 So *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (131).

probleme einhergeht.[14] Lösungen für neuartige informationstechnische Konfliktlagen sind ebenso auf der Grundlage von allgemeinen Grundsätzen zu eruieren, denn auch in der virtuellen Welt sind Bestrebungen, völkervertragliche Übereinkünfte zur Reglementierung von Informationsoperationen zu etablieren, aufgrund der divergierenden Interessen der Staaten wenig aussichtsreich.[15] In diesem Sinne nimmt auch die vom Europarat aufgestellte Arbeitsgruppe zu grenzüberschreitenden Fragen des Internet (Ad-hoc Advisory Group on Cross-border Internet) Bezug auf die Präventionsartikel der Völkerrechtskommission und auf das Schädigungsverbot im Umweltkontext, um staatliche Pflichten in der virtuellen Welt auszubuchstabieren.[16]

Es wird zwar zum Teil bemängelt, dass keine klare Linie zwischen Analogien und allgemeinen Rechtsgrundsätzen gezogen werden könne.[17] Dies ist aber jedenfalls bei der Frage nach der Übertragbarkeit von rechtlich anerkannten Regelungen auf ungeregelte Bereiche nicht hinderlich. Die beiden völkerrechtlichen Regelinstrumente können sich vielmehr bei der Übertragbarkeit von bestehenden Regeln auf ungeregelte Bereiche argumentativ stützen. Die besprochenen allgemeinen Rechtsgrundsätze untermauern wie gezeigt in ihrer umweltspezifischen Konkretisierung das Gesamtkonzept der Staatenhaftung und dienen hier als Basis für eine Übertragbarkeit des Konzepts auf die virtuelle Welt.[18]

---

14 *Ibid*.

15 Vgl. *S. Hobe*, Die Zukunft des Völkerrechts im Zeitalter der Globalisierung, AVR 37 (1999) S. 253 (267 f.); Ausführlich zu den Gründen, aus denen ein umfassendes Vertragswerk für die virtuelle Welt unwahrscheinlich ist siehe Jack Goldsmith, Cybersecurity Treaties, A Skeptical View, Hoover Institution Task Force on National Security and Law, Future Challenges Essay 9 March 2011, abrufbar unter: http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (geprüft am 15.05.2020). *R. Crootof* spricht nicht nur dem Völkervertragsrecht, sondern auch dem Völkergewohnheitsrecht die Möglichkeit zur umfassenden Regulierung von Aktivitäten in der virtuellen Welt ab. *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (640 ff.; 642 f.).

16 Council of Europe, Ad-hoc Advisory Group on Cross-border Internet, Interim Report to the Steering Committee on the Media and New Communication Services incorporating Analysis of Proposals for International and Multi-stakeholder Cooperation on Cross-border Internet, H/Inf (2010) 10, Rn. 60 ff.

17 *G. Beaucamp/L. Treder*, Methoden und Technik der Rechtsanwendung, 2015, S. 67, Rn. 248; *N. MacCormick*, Legal Reasoning and Legal Theory, 1978, S. 161, 186.

18 Vgl. auch die Ausführungen von *C. L. Riemer*, der in Bezug auf eine staatengemeinschaftliche Solidarität in der Völkerrechtsordnung in vergleichbarer Weise davon spricht, „daß sich die einzelnen solidartragenden Umweltregime in ihrer

II. Bedürfnis der Übertragbarkeit

Wie den Betrachtungen in Kapitel 3 (Staatenverantwortlichkeit für informationstechnische Systeme) zu entnehmen ist, bestehen eine regelungssystematische Lücke des Völkerrechts mit Blick auf informationstechnische Problemlagen und das Bedürfnis zu ihrer Schließung. Der in der völkerrechtlichen Literatur erfolgte Perspektivenwechsel von der Bedeutung des *ius ad bellum* und des *ius in bello* im virtuellen Raum hin zu einer möglichen Reglementierung von Informationsoperationen zu Friedenszeiten, verdeutlicht das Regelungsbedürfnis von Informationsoperationen, die unterhalb der Schwellenvoraussetzungen von Gewaltanwendung bzw. Intervention bleiben und mithin nicht ohne Weiteres als völkerrechtswidrig qualifiziert werden können. Im Schrifttum werden derartige Informationsoperationen als „‚below the threshold' cyber operations"[19], „malicious cyber-attacks"[20], „low-intensity cyber attacks"[21], oder als „international cybertorts"[22] bezeichnet und dabei mit unterschiedlichen Nuancen von „cyberwarefare and cybercrime" abgegrenzt.[23] Diese Arbeit subsumiert derartige Vorgänge unter die Kategorie der völkerrechtlich nicht verbotenen Informationsoperationen. Deren Regelungsbedürfnis ergibt sich, wie so oft im Völkerrecht, aus dem Entwicklungsrückstand der Rechtsordnung gegenüber den modernen Anforderungen einer globalen und vernetzten Welt.[24] Wie dargelegt, resultieren aus dem heimlichen und ubiquitären Charakter von Informationsoperationen Unsicherheiten mit Blick auf Verursacher und Ablauf von Informationsoperationen. Daher ist eine Rege-

---

Funktion und Geltung wie die Teilstücke eines Kuchens zu einer ganzen Solidaritäts-‚Torte' ergänzen" können und mithin grundsätzliche geeignet sind, „eine in Sachbereiche aufgegliederte multiple Basis für eine Analogie" zu bieten. *C. L. Riemer*, Staatengemeinschaftliche Solidarität in der Völkerrechtsordnung, 2003, S. 300.

19 *M. N. Schmitt*, "Below the Threshold" Cyber Operations, Va JIL 54 (2014), S. 697 (697 ff.).

20 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 32 f.

21 *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1460 ff.).

22 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (565 ff.).

23 *Id.*, S. 565 (592 ff.), mit dem Hinweis, es käme zu Überschneidungen der Kategorien (auf S. 593 f.).

24 Vgl. *J. Barboza*, The Environment, Risk and Liability in International Law, 2011, S. 153; *S. Hobe*, Die Zukunft des Völkerrechts im Zeitalter der Globalisierung, AVR 37 (1999) S. 253 (280).

lungskonzept vorzugswürdig, das nicht die Zurechnung einer konkreten Handlung erfordert, sondern auf einer Risikozuweisung basiert.[25] Eine staatliche Haftung ist somit grundsätzlich geeignet, den Herausforderungen für die Völkerrechtsordnung durch völkerrechtlich nicht verbotene Informationsoperationen zu begegnen.

Während die meisten Autoren völkerrechtliche Verbotskategorien ausweiten bzw. ergänzen oder umweltrechtliche Grundsätze auf die virtuelle Welt übertragen wollen, deren Verletzung zur Staatenverantwortlichkeit führt,[26] taucht die Idee der Staatenhaftung für Informationsoperationen nur vereinzelt im Schrifttum auf.[27] Die völkerrechtliche Bestandskraft der Staatenhaftung[28] bzw. deren Anwendbarkeit auf die virtuelle Welt[29] wird dabei vorausgesetzt. Alle erheblich schädigenden Informationsoperationen, die keine Verletzung des Gewaltverbotes oder Interventionsverbotes darstellen,[30] seien danach dem Anwendungsbereich der Staatenhaftung zu unterstellen.[31] Die Staatenhaftung sei zwar vornehmlich im Umweltvöl-

25 Vgl. *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (6) in Bezug auf das Vorsorgeprinzip.

26 Vgl. hierzu schon die Ausführungen im 3. Kapitel.

27 So etwa bei *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (565 ff.); *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 204 ff.; *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1460 ff.).

28 *J. D. Jolley* spricht von einer völkergewohnheitsrechtlich anerkannten Theorie der verschuldensunabhängigen Haftung für hochgefährliche Aktivitäten. *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 206.

29 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (588, 604); *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1499 ff.).

30 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 17; *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1466). Insbesondere bei den Ausführungen von *R. Crootof* verschwimmt aber die Grenze zwischen der staatlichen Einstandspflicht für rechtmäßige und unrechtmäßige Aktivitäten. Vgl. *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (593).

31 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (588 ff., 604); *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 212 ff.; *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1499).

kerrecht zu verorten,[32] allerdings bestärke insbesondere die *Korfu Kanal*-Entscheidung die Annahme, dass die Staatenhaftung grundsätzlich auch auf andere Bereiche des Völkerrechts anwendbar sei.[33] Diese Schlussfolgerung geht jedoch aufgrund der gebotenen Differenzierung zwischen Verhinderungs- und Schadensvermeidungspflichten fehl.[34] Vielmehr ist eine Übertragbarkeit des umweltvölkerrechtlichen Konzepts der Staatenhaftung auf die virtuelle Welt nur dann möglich, wenn sich die virtuelle Welt und die natürliche Umwelt ausreichend gleichen, entsprechende rechtliche Herausforderungen bedingen und vergleichbare Interessen bzw. Werte betreffen.[35]

III. Vergleichbarkeit

Die virtuelle Welt und die natürliche Umwelt gleichen sich dadurch, dass sich Cyber- bzw. Umweltschäden, die durch Handlungen in einem Staat begründet sind, in einem anderen Staat verwirklichen können.[36] Zugleich sind beide Welten internationale Räume ohne physische Staatsgrenzen.[37]

---

32 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 204 f.; *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1480); zustimmend *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (603).

33 *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1483 f.); zustimmend *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (603 f.); vgl. auch *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 212.

34 Siehe 1. Kapitel B.

35 *J. D. Jolley* diskutiert ebenfalls eine Vergleichbarkeit zwischen natürlicher Umwelt und virtueller Welt, um eine analoge Anwendung der verschuldensunabhängigen Haftung für hochgefährliche Aktivitäten auf „malicious cyber-attacks" zu begründen. *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 206 ff.

36 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 2015), S. 129 (131); *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 207; *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (21).

37 *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 299; *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in

Dementsprechend ist der Schutz von Gemeinschaftsgütern, für deren Erhalt Staaten eine gemeinsame, geteilte Verantwortung tragen, sowohl im Kontext der Umwelt, etwa mit Blick auf den Weltraum, die Hohe See, die Antarktis, als auch hinsichtlich der virtuellen Welt von Bedeutung.[38] Staaten haben nicht nur ein Interesse am Erhalt natürlicher Ressourcen, sondern ebenso an der Funktionalität des virtuellen Raums.[39] So ist das Internet als gemeinsame bzw. geteilte Ressource zu qualifizieren, die eine nachhaltige und gerechte Nutzung gebietet.[40] Ähnlich wie natürliche Ressourcen haben technische Ressourcen einen essenziellen Wert und Nutzen für die Menschheit. Kommunikationsinfrastrukturen sind notwendig für sozialwirtschaftliche Beziehungen und sonstige ökonomische Betätigungen.[41] Diese sind, wie im Umweltkontext etwa das Klima oder die Biodi-

---

International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 207.

38 *J. Bäumler* spricht von einer möglichen Analogie zu Gemeinschaftsgütern. *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 299; siehe auch *P. W. Franzese*, Sovereignty in Cyberspace, AF Law Review 64 (2009), S. 1 (14 ff.); *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 209 f.; *M. C. Kettemann*, Das Internet als internationales Schutzgut, ZaöRV 72 (2012), S. 469 (476 f.); *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (167). Es gibt zwar Stimmen, die sich gegen die Sinnhaftigkeit dieses Rechtsinstituts im Cyberkontext aussprechen. So *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 2015), S. 129 (133). Allerdings sollen an dieser Stelle zunächst die Parallelen zwischen der virtuellen und natürlichen Welt dargelegt werden, die sich anhand der diskutierten Lösungsansätze herauskristallisieren lassen.

39 Das Interesse am Bestehen der Funktionalitäten des Internets korrespondiere mit einer *erga omnes*-Pflicht des potenziellen Störer-Staates hinsichtlich der Stabilität, Integrität und Funktionalität des Internets. So *M. C. Kettemann*, Das Internet als internationales Schutzgut, ZaöRV 72 (2012), S. 469 (478) unter Hinweis auf Prinzip 3 und 5 der Erklärung des Ministerkomitees des Europarates über die Grundsätze der Internet Governance, angenommen bei der 1121. Sitzung der Stellvertreter der Minister am 21.09.2011.

40 *Id.*, S. 469 (467 f., 479 f.); *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (21 f.); *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (180).

41 So *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (467), siehe auch *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 207.

versität, zu schützen.[42] Die Vergleichbarkeit von virtueller und natürlicher Welt wird durch den Umstand bestärkt, dass sowohl das Internet als auch Umweltbestandteile wie die Luft allgegenwärtig und gleichzeitig nicht greifbar sind.[43]

Darüber hinaus sind Umweltverschmutzungen, so wie „Verschmutzungen" der virtuellen Welt auch, nicht ohne Weiteres zu identifizieren und zu stoppen und machen damit staatliche Kooperations- und Einstandspflichten unumgänglich.[44] Die grenzüberschreitenden Auswirkungen auf die Umwelt und auf die virtuelle Welt erfordern dabei gleichermaßen einen Ausgleichsmechanismus zwischen der Wahrung von Souveränitätsrechten einerseits und der Sicherstellung zwischenstaatlicher Verpflichtungen andererseits.[45]

Ferner entstehen sowohl informationstechnische als auch umweltbezogene Problemlagen primär durch nicht-staatliche und weniger durch staatliche Akteure,[46] so dass eine völkerrechtliche Verbindung zwischen staatlichen Pflichten und nicht-staatlichen Aktivitäten notwendig ist. Eine solche Verbindung kann weder durch wissenschaftliche noch durch technische Zurechnung erreicht werden; in der vielschichtigen natürlichen bzw. vir-

42 *O. Gross*, Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (495). Die Verletzung der staatlichen Schutzpflicht hinsichtlich der Funktionalität, Stabilität und Integrität des Internets könne zur Staatenverantwortlichkeit führen. So *M. C. Kettemann*, Das Internet als internationales Schutzgut, ZaöRV 72 (2012), S. 469 (480).

43 So *J. Bäumler* spricht von einer möglichen Analogie zu Gemeinschaftsgütern. *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 299.

44 *J. Healey/H. Pitts*, International Environmental Legal Norms to Cyber Statecraft, I/S: A Journal of Law and Policy for the Information Society 8 (2012), S. 356 (384 f.); vgl. auch *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 299 bezüglich der Anwendung des Schädigungsverbotes auf schädigende Handlungen im Internet.

45 *J. Healey/H. Pitts*, International Environmental Legal Norms to Cyber Statecraft, I/S: A Journal of Law and Policy for the Information Society 8 (2012), S. 356 (384).

46 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 2015), S. 129 (131); *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 219; *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (482).

tuellen Welt kann nur ein regulatorischer Ansatz in Form von Risikozuteilung zielführend sein.[47]

Im Ergebnis können die wissenschaftlichen und technischen Unsicherheiten und die potenziell schädigenden Auswirkungen, die sich in beiden Welten zeigen, nur durch normativ festgelegte Regulierungskriterien bewältigt werden.[48]

IV. Ergebnis

Trotz der aufgezeigten Parallelen zur Umwelt gibt es durchaus Aspekte in der virtuellen Welt, die spezifische Regulierungen erfordern. Zu Bedenken sind etwa die vornehmlich nicht greifbaren Auswirkungen von Informationstechnik, die durch die technischen Möglichkeiten bedingte Zeit-Raum-Kompression sowie der anonyme und ubiquitäre Charakter der virtuellen Welt. Nichtsdestoweniger hält das konsolidierte Umweltvölkerrecht Mechanismen bereit, die auch im Kontext informationstechnischer Systeme funktionieren.[49]

B. Umsetzung der Staatenhaftung für informationstechnische Systeme

Die folgende Darstellung einer Staatenhaftung für informationstechnische Systeme wird zeigen, dass die informationstechnischen Hürden für das Völkerrecht durch existente normative Instrumente überwindbar und erhebliche grenzüberschreitende Schäden durch Informationsoperationen nicht etwa „lost in translation" sind.[50]

47 Vgl. *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (482).

48 *Ibid*.

49 *Id.*, S. 465 (483 f.) mit dem Hinweis, dass beim Rekurs auf das Umweltvölkerrecht die fehlende Territorialität in der virtuellen Welt Berücksichtigung finden muss.

50 *J. E. Messerschmidt*, Hackback, Col. JTL 52 (2013), S. 275 (296).

I. Anwendungsbereich

Eine Staatenhaftung für informationstechnische Systeme kommt nur dann in Betracht, wenn diesen das Risiko eines erheblichen grenzüberschreitenden Schadens immanent ist.

1. Schaden

Der herkömmliche Schadensbegriff setzt zunächst physische Auswirkungen auf Mensch, Eigentum oder Umwelt voraus.[51] Allerdings führen Informationsoperationen wie gezeigt nicht nur zur Zerstörung von physischen Komponenten der virtuellen Welt, beispielsweise von Computern, sondern zu neuartigen digitalen, immateriellen und wirtschaftlichen Schäden, wie Zerstörung von Datensystemen, Datenverlust, Veröffentlichung privater und vertraulicher Informationen, Umsatz- und Imageverluste von Unternehmen oder Kosten für die Abwehr und Beseitigung von Informationsoperationen.[52] Die Beschränkung der Staatenhaftung auf die physische Qualität einer Aktivität und deren Schadensfolgen ist indes nicht mehr zeitgemäß,[53] denn in vielen Bereichen potenzieren sich die Möglichkeiten zwischenstaatlicher Beeinträchtigungen durch die fortschreitende Technisierung, aufgrund der zunehmenden wirtschaftlichen Interdependenzen und der Globalisierung im Allgemeinen.[54] Passt man das Konzept der Staatenhaftung dem Zeitalter des Internets an, müssen demnach auch digitale Schäden in den Anwendungsbereich fallen.[55] Denn erst eine Neudefinition des Schadensbegriffs ermöglicht es, neuartigen Gefährdungslagen zu begegnen.[56] Der Begriff des Schadens ist hierfür auch entwick-

51 *X. Hanqin*, Transboundary Damage in International Law, 2003, S. 5.

52 Siehe 3. Kapitel A. und B.

53 *S. Townley*, The Rise and Risk in International Law, Chi. JIL 18 (2018), S. 594 (627, 631).

54 *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 5, 276.

55 So *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 137; vgl. auch *S. Townley*, The Rise and Risk in International Law, Chi. JIL 18 (2018), S. 594 (631 f.).

56 *R. M. Bratspies/R. A. Miller*, Introduction, in: dies. (Hg.), Transboundary Harm in International Law, 2006, S. 1 (8); *S. Townley*, The Rise and Risk in International Law, Chi. JIL 18 (2018), S. 594 (627). Nach *B. A. Walton* bestünde hingegen kein Bedürfnis für eine Neudefinition, da es schon gar nicht auf die physische Qualität ankomme, wenn eine gewisse Erheblichkeit der nicht-physischen Auswirkungen

lungsoffen, dies zeigt die Haftungsstudie der Völkerrechtskommission. Auch wenn der Schutz der Umwelt im Vordergrund stand, beabsichtigte sie keine Begrenzung auf Fragen ökologischer Natur oder Kategorien physischer Gebietsnutzung.[57] Zudem greifen Mechanismen der Staatenhaftung bereits im Wirtschaftsvölkerrecht, mithin für Beeinträchtigungen wirtschaftlicher Interessen.[58] Bemerkenswert ist, dass schon in den *Trail Smelter*-Entscheidungen wirtschaftliche Erwägungen Gegenstand der Schadensbestimmung waren. So bezog sich die Staatenhaftung im *Trail Smelter*-Fall nicht nur auf physische Schäden an der Umwelt, sondern auch auf finanzielle Verluste in der Landwirtschaft aufgrund ausgebliebener Erträge sowie sonstiger Wertverluste der Grundstücke und auch die Kosten für die Beseitigung von Schäden spielten eine Rolle.[59] Im Ergebnis sind im Sinne eines dynamischen Schadensbegriffs auch digitale, immaterielle und wirtschaftliche Posten bei der Schadensbestimmung zu berücksichtigen.

Außerdem muss der Schaden durch die fragliche Informationsoperation grenzüberschreitend sein, das heißt auf fremdstaatlichem Territorium oder in anderen Gebieten unter der Hoheitsgewalt eines fremden Staates eintreten.[60] Wie bereits dargelegt, wird die virtuelle Welt, wie auch Bereiche der Umwelt, als Gemeinschaftsgut qualifiziert, welches sich außerhalb einzelstaatlicher Hoheitsgewalt befinde. Dies steht der Anwendbarkeit der Staatenhaftung nicht entgegen, da sich jedenfalls die physischen Kompo-

---

gegeben sei. In diesem Sinne seien bereits nicht-physische Schäden durch Strahlenbelastungen als Folge von Atomtests Gegenstand von völkerrechtlichen Streitfällen zu Kompensationsansprüchen. *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1505) unter Bezugnahme auf ILC Secretariat, Survey of liability regimes relevant to the topic of international liability for injurious consequences arising out of acts not prohibited by international law (international liability in case of loss from transboundary harm arising out of hazardous activities), YBILC 2004-II/1, UN Doc. A/CN.4/543, S. 79, und IGH, Nuclear Tests (Australia v. France), Interim Protection, Order of 22 June 1973, ICJ Reports 1973, S. 99 (99 ff.). Nach *J. D. Jolley* seien die Schäden durch Informationsoperationen zwar digital, besäßen aber zugleich aufgrund der monetären Verluste physische Qualität. *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 138.

57 Sonderberichterstatter *R. Q. Quentin-Baxter*, Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law, YBILC 1983-II/1, UN.Doc. A/CN.4/373, S. 205 f., Rn. 17.

58 Siehe 1. Kapitel D. I. 4.

59 Trail Smelter Arbitration (United States v. Canada), Award of 16 April 1938 and 11 March 1941, 3 UNRIAA (1941), S. 1905 (1925 f.).

60 Vgl. *X. Hanqin*, Transboundary Damage in International Law, 2003, S. 8.

nenten informationstechnischer Systeme und auch die Verursacher bzw. Opfer von Informationsoperationen auf Gebieten befinden, die der Souveränität von Staaten unterliegen.[61] Ferner bezieht sich die Staatenhaftung für informationstechnische Systeme mit Blick auf ihre praktische Umsetzbarkeit nicht auf diffuse allgemeine grenzübergreifende Schäden, die etwa durch die Überbeanspruchung der globalen Ressource Internet (*information pollution*) entstehen und das Gemeinschaftsgut „virtueller Raum" gefährden, sondern auf Informationsoperationen, die zu konkreten nachteiligen Auswirkungen auf andere Staaten führen. So qualifiziert auch die vom Europarat aufgestellte Arbeitsgruppe zu grenzüberschreitenden Fragen des Internet (Ad-hoc Advisory Group on Cross-border Internet) das Internet einerseits als Gemeinschaftsgut,[62] stellt aber andererseits zur Begründung staatlicher Pflichten im virtuellen Raum auf nachteilige Auswirkungen auf andere Staaten ab, und nicht auf Schäden am virtuellen Raum im Allgemeinen.[63] Im Rahmen der folgenden rechtlichen Erwägungen sind also kollektive Rechte und Pflichten von Staaten hinsichtlich der Stabilität, Integrität und Funktionalität der globalen Ressourcen der virtuellen Welt von untergeordneter Bedeutung.[64] Der Grundsatz angemessener Nutzung geteilter Ressourcen hingegen liefert auch in der virtuellen Welt Anknüpfungspunkte für eine Staatenhaftung für informationstechnische Systeme, da er Ressourcen betrifft, die der Hoheitsgewalt von Staaten unterliegen und gleichzeitig grenzüberschreitender Natur sind.[65]

Letztlich müssen Parameter gefunden werden, die einen Schaden durch eine Informationsoperation als erheblich qualifizieren.[66] Zur Abgrenzung von einer hinzunehmenden Beeinträchtigung wird ein Vergleich mit der territorialen Integrität von Staaten vorgeschlagen. Sind die betroffenen Interessen von ähnlicher Bedeutung wie die territoriale Integrität eines Staa-

61 Siehe hierzu 1. Kapitel E. I.

62 Council of Europe, Ad-hoc Advisory Group on Cross-border Internet, Interim Report to the Steering Committee on the Media and New Communication Services incorporating Analysis of Proposals for International and Multi-stakeholder Cooperation on Cross-border Internet, H/Inf (2010) 10, Rn. 14.

63 *Id.*, Rn. 69.

64 Siehe hierzu *M. C. Kettemann*, Das Internet als internationales Schutzgut, ZaöRV 72 (2012), S. 469 (469 ff.).

65 Vgl. *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (154 f.); *M. Herdegen*, Possible Legal Framework and Regulatory Models for Cyberspace, GYIL 85 (2015), S. 169 (179).

66 Vgl. *X. Hanqin*, Transboundary Damage in International Law, 2003, S. 7 f. mit dem Hinweis, dass die Erheblichkeitsschwelle ziel- und kontextabhängig zu bestimmen ist.

tes, dann ist eine Erheblichkeit anzunehmen.[67] Informationsinfrastrukturen erfassen alle Bereiche des gesellschaftlichen Lebens und sind für die Staaten von essenzieller Bedeutung. Gleichzeitig bedingen sie durch die Allgegenwärtigkeit der Vernetzung eine besondere Verwundbarkeit.[68] Die Beeinträchtigung von Informationsinfrastrukturen ist demnach mit Auswirkungen auf die territoriale Integrität vergleichbar.[69] Schwierig gestaltet sich die Erheblichkeitsbeurteilung bei immateriellen Schäden, etwa als Konsequenz von Wahleinmischung oder Ausspähung Privater durch Informationsoperationen, da derartige Beeinträchtigungen schwer zu beziffern sind. In diesem Zusammenhang findet sich der Vorschlag, dass für die Frage nach der Erheblichkeit entscheidend sei, inwiefern die Opferstaaten selbst zur Vermeidung von vergleichbaren schädigenden Aktivitäten beitragen würden.[70] Die Erheblichkeit von Schäden durch Aktivitäten, die auf internationaler Ebene regelmäßig praktiziert und geduldet würden, sei zu verneinen. Dementsprechend falle Spionage mangels Erheblichkeit der daraus resultierenden Schäden aus dem Anwendungsbereich der Staatenhaftung.[71] Allerdings unterliegt herkömmliche Spionage in der physischen Welt aufgrund möglicher strafrechtlicher Verfolgung der Spione durch den Opferstaat gewissen Begrenzungen. Die virtuelle Welt hingegen bietet nicht nur eine größere Angriffsfläche für Spionage, sondern dämmt zugleich das Risiko des Entdecktwerdens sowie der Strafverfolgung für Spione ein, die von ihrem Heimatstaat aus die Informationsausspähung und Informationsausbeutung durchführen können.[72] Die entsprechenden Beispiele aus der internationalen Praxis verdeutlichen, dass die Spionage in der virtuellen Welt Dimensionen erreicht, die nicht mehr hinnehmbar sind und zunehmend zu zwischenstaatlichen Spannungen führen. Die Staatenhaftung bietet mit Blick auf die erheblichen Auswirkungen von Informationsspionage in der virtuellen Welt eine geeignete Reaktionsmög-

67 *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 276.

68 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 5; vgl. auch *S. P. Kanuk*, Information Warfare, Harv. ILJ 37 (1996), S. 272 (285).

69 *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (21).

70 *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1506) unter Bezugnahme auf Präventionsartikel 10 lit. d und lit. f; vgl. auch *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 187.

71 *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1506).

72 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (607).

lichkeit durch Opferstaaten, ohne dabei einen Teufelskreis von Retorsionen in Gang zu setzen. Hilfreich für die Erheblichkeitsbeurteilung sind auch Überlegungen, die effektive Souveränitätsausübung eines Staates als schützenswertes Rechtsgut zu kategorisieren.[73] Demnach haftet ein Staat, wenn er die Souveränitätsausübung eines anderen Staates in einer Weise behindert, dass letzterem die Abwehr bzw. Beseitigung dieser Beeinträchtigung unmöglich oder nur unter erheblichen eigenen Verlusten möglich ist.[74] Ein Vergleich zu nationalem Deliktsrecht zeigt schließlich, dass eine Entschädigung für immaterielle Schäden durchaus möglich ist und im Grunde die Anspruchssteller selbst entscheiden, wann ein Schaden erheblich genug ist, um seine Kompensation gerichtlich einzufordern, und wann Sachverständige zur Beurteilung der Erheblichkeit herangezogen werden.[75] So wird sich die Erheblichkeitsschwelle auf internationaler Ebene durch die Anwendung auf konkrete Fälle konkretisieren.[76]

2. (Hoch-)Gefährliche Aktivität

Das Konzept der Staatenhaftung bezieht sich auf (hoch-)gefährliche Aktivitäten. Die Kriterien zur Beurteilung der Gefährlichkeit einer Aktivität sind nicht statisch und müssen – sowie der Schadensbegriff auch – dem Wandel der Zeit entsprechend angepasst werden.[77] Demnach können auch informationstechnische Aktivitäten dem Anwendungsbereich der Staatenhaftung unterfallen. Auch für andere neuartige Gefährdungslagen, beispielsweise im Zusammenhang mit dem Einsatz von autonomen Waffensystemen, werden entsprechende Ansätze diskutiert.[78] Dabei darf der Anwendungsbereich der Staatenhaftung aber nicht zu weit gefasst werden, um ihren Sinn und Zweck nicht zu unterlaufen. Das Konzept der Staa-

---

73 *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 276 unter Bezugnahme auf *M. Ronzoni*, The Global Order, Philosophy & Public Affairs 37 (2009), S. 229 (248 f.).

74 Vgl. *id.*, S. 277.

75 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (608 f.).

76 *Id.*, S. 565 (608) zum Vorschlag zur Etablierung eines Expertengremiums, das entsprechende Ansprüche evaluiert (S. 367 ff.).

77 Vgl. *J. Barboza*, The Environment, Risk and Liability in International Law, 2011, S. 9; *S. Townley*, The Rise and Risk in International Law, Chi. JIL 18 (2018), S. 594 (627 ff.).

78 *N. Bhuta/S.-E. Pantazopoulous*, Autonomy and uncertainty, in: N. Bhuta/S. Beck/R. Geiß/H.-Y. Liu/C. Kreß (Hg.), Autonomous Weapons Systems, 2016, S. 284 (291).

tenhaftung zielt, wie gezeigt, auf eine *ex ante* Regulierung von Gefahrenlagen, um daraus resultierenden Unsicherheiten zu begegnen und einen gerechten Interessenausgleich der betroffenen Staaten schon im Vorhinein zu gewährleisten. Schließlich erfasst der Anwendungsbereich der Staatenhaftung keine schädigenden Einzelakte, sondern gemeinnützige und/oder wirtschaftlich vorteilhafte Aktivitäten, bei denen der Schadenseintritt allenfalls eine ungewollte Nebenwirkung darstellt.[79]

Vor diesem Hintergrund können einzelne Informationsoperationen nicht als Anknüpfungspunkt für die Staatenhaftung in der virtuellen Welt dienen. Informationsoperationen sind so vielgestaltig, dass eine Kategorisierung in gefährlich bzw. hochgefährlich nicht ohne Weiteres möglich ist. So besteht zwar bei Informationsausbeutung regelmäßig die hohe Wahrscheinlichkeit erheblicher finanzieller bzw. wirtschaftlicher Schäden oder erheblicher Beeinträchtigungen des Rechts auf Privatheit, während bei Informationsangriffen grundsätzlich die Möglichkeit katastrophaler Schäden, etwa durch die Störung kritischer Infrastrukturen, gegeben ist.[80] Allerdings ist eine *ex post facto* Analyse unabdingbar, um die Schadenswahrscheinlichkeit und den Schadensumfang einer bestimmten Informationsoperation beurteilen zu können.[81] Das Risiko jeder einzelnen Informationsoperation kann nicht *ex ante* im Sinne eines gerechten Interessenausgleichs reguliert werden. Informationsoperationen stellen im Übrigen auch keine vorrangig gemeinnützige oder wirtschaftlich vorteilhafte Aktivität dar; Informationsoperationen sind vielmehr Einzelakte, die einen Schaden intendieren.

Zur Beurteilung der Gefährlichkeit ist daher auf informationstechnische Systeme im Allgemeinen abzustellen. Der Betrieb dieser Systeme ist der Gesellschaft und auch der Staatengemeinschaft primär von Nutzen. Durch die Erlaubnis zum Betrieb informationstechnischer Systeme – und nicht durch die Erlaubnis zu jeder einzelnen Informationsoperation – schaffen Staaten erst das Risiko, welches sie regulieren und für dessen Realisierung – in Gestalt einer Informationsoperation – sie am Ende einstehen müssen.[82] Vergleichbar mit dem Betrieb (hoch-)gefährlicher Anlagen ist auch

79 Siehe 1. Kapitel A. II. 1. a) und 2. Kapitel B. I. 2.

80 Siehe 3. Kapitel A. und B.

81 Vgl. *G. Handl*, State Liability for Accidental Transnational Environmental Damage by Private Persons, AJIL 74 (1980), S. 525 (555).

82 *H. Krieger* stellt vergleichbar hinsichtlich staatlicher Sorgfalts-, Informations- und Warnpflichten fest: „Nach dem Gedanken des Vorsorgeprinzips muss der Blick weg vom Verursacher auf den Betreiber gerichtet werden, d.h. auf alle Staaten, die die Gefährdungslage für die internationale Sicherheit schaffen, weil sie das In-

hier das Risiko im Vorhinein bestimmbar und eine *ex ante* Regulierung der Gefährdung auf Grundlage eines gerechten Interessenausgleichs möglich. Der Betrieb informationstechnischer Systeme ist grundsätzlich jeder Art von Informationsoperation zugänglich und ist im Ergebnis als hochgefährlich zu kategorisieren, da die auch noch so geringe Wahrscheinlichkeit katastrophaler Schäden durch diese Systeme begründet wird.[83]

3. Kausalität

Der Betrieb informationstechnischer Systeme auf staatlichem Territorium bzw. unter staatlicher Hoheitsgewalt muss ursächlich für den Schaden sein, damit die Staatenhaftung greifen kann. Im Umweltkontext ist Kausalität in der Regel durch eine physische Verbindung zwischen einer Aktivität und ihren Folgen gekennzeichnet.[84] Bei einer direkten Beziehung zwischen den informationstechnischen Systemen und den schädigenden Auswirkungen kann nichts anderes gelten.[85] Informationstechnische Systeme können nämlich ohne Weiteres Schäden verursachen, wenn sich das ihnen immanente Risiko – in Gestalt einer Informationsoperation – realisiert.

Während für die Zurechnung völkerrechtswidriger Informationsoperationen eine klare und überzeugende Beweislage gefordert wird,[86] reicht für den Kausalitätsnachweis bei Schäden durch völkerrechtlich nicht verbotene Informationsoperationen im Sinne des Vorsorgegrundsatzes schon die Möglichkeit der Schadensverursachung aus.[87] Diese unterschiedlichen Beweisanforderungen spiegeln sich auch in der Rechtsprechung des IGH, wonach eindeutigere Nachweise gefordert werden, je einschneidender der

---

ternet ohne hinreichende technische Sicherung nutzen." *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (16); vgl. auch *S. Erichsen*, Das Liability-Projekt der ILC, ZaöRV 51 (1991), S. 94 (109 f.).

83 Vgl. *O. Gross*, Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (482 f.).

84 *X. Hanqin*, Transboundary Damage in International Law, 2003, S. 4.

85 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 137 f.; vgl. auch *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1465 Fn. 25).

86 Siehe 3. Kapitel D. I.

87 Vgl. 2. Kapitel B. I. 3.

Eingriff ist.[88] In der Regel ist die geografische Herkunft von Informationsoperationen anhand der Internetadressen ermittelbar und mithin auf die jeweiligen informationstechnischen Systeme des Ursprungsstaates zurückführbar.[89] Dementsprechend wird der geforderte Kausalitätsnachweis in diesen Fällen gelingen.

Bei technischen Rückverfolgungsproblemen, etwa im Fall von *Onion Routing*, hilft die erleichterte Beweisführung, die auch für den Nachweis der Kenntnis des Ursprungsstaates von völkerrechtswidrigen Informationsoperationen gilt.[90] Danach ist der Kontext der Informationsoperation maßgeblich. Als Indizien für die Herkunft einer Informationsoperation können beispielsweise der Nutzen einer Informationsoperation für einen

88 IGH, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ Reports 1949, S. 4 (17); IGH, Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, ICJ Reports 2003, Separate Opinion of Judge Higgins, S. 225 (234 Rn. 33); IGH, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, ICJ Reports 2007, S. 43 (119 Rn. 181, 129 Rn. 208 f., 130 Rn. 210); IGH, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia), Judgment of 3 February 2015, ICJ Reports 2015, S. 3 (74 Rn. 178).

89 *J. Healey/H. Pitts*, Applying International Environmental Legal Norms to Cyber Statecraft, I/S: A Journal of Law and Policy for the Information Society, 8 (2012), S. 356 (379).

90 Siehe 3. Kapitel E. III. Die Bezugnahme auf die erleichtere Beweisführung im Zusammenhang mit völkerrechtswidrigen Informationsoperationen ändert aber nichts daran, dass der Nachweis für die Kenntnis von völkerrechtswidrigen Informationsoperationen keine begründeten Zweifel lassen darf, während für den Kausalitätsnachweis im Kontext von völkerrechtlich nicht verbotenen Informationsoperationen die Möglichkeit der Schadensverursachung ausreicht.

bestimmten Staat[91] oder die mangelnde Kooperationsbereitschaft eines Staates bei der Aufklärung der Sachlage[92] herangezogen werden.[93]

Ähnlich wie im Rahmen der staatlichen Pflichten zur Verhinderung von bzw. zum Schutz vor Informationsoperationen stellt sich aber bei der Kausalitätsprüfung die Problematik von Bots oder Datenpaketen, die erst im Zielstaat erhebliche Schäden verursachen. Wie beschrieben, ist im Rahmen der staatlichen Verhinderungs- bzw. Schutzpflicht eine Verantwortlichkeit des Ursprungsstaates nur zu bejahen, wenn die Bots bzw. Datenpakete auf staatlichem Hoheitsgebiet bzw. unter staatlicher Hoheitsgewalt für sich allein die notwendige Intensität erreichen, um als völkerrechtswidriges Verhalten qualifiziert werden zu können. Ist eine völkerrechtswidrige Informationsoperation nur durch das gesamte Botnet bzw. Datenwerk begründet, entsteht keine Verhinderungs- bzw. Schutzpflicht hinsichtlich der einzelnen Bots bzw. Datenpakete.[94] Denn Staaten werden den Vorwurf völkerrechtswidrigen Verhaltens von sich weisen und nicht gewillt sein, eine Verantwortlichkeit für gesamte Botnets bzw. Datenwerke zu akzeptieren, wenn sich ihr eigener kausaler Beitrag lediglich auf einzelne Bots bzw. Datenpakete beschränkt, welche für sich genommen keine völkerrechtswidrige Informationsoperation darstellen. Eine andere Betrachtungsweise

---

91 *F. Hare*, The Significance of Attribution to Cyberspace Coercion, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 125 (136 ff.).

92 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 201 ff. unter Bezugnahme auf IGH, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ Reports 1949, S. 4 (18 f.); vgl. *R. K. Knake*, Untangling Attribution: Moving to Accountability in Cyberspace, Statement Before the Subcommittee on Technology and Innovation, Committee on Science and Technology, United States House of Representatives 2nd Session, 111th Congress, 2010, abrufbar unter: https://www.cfr.org/sites/default/files/pdf/2010/07/Knake%20-Testimony%20071510.pdf (geprüft am 15.05.2020), S. 8.

93 *M. C. Libicki* lehnt dagegen diese Anknüpfungspunkte für eine Zurechnung ab, da diese missbraucht und mithin irreführend sein könnten. Aussagekräftiger seien Methode und Ausführung der Informationsoperation sowie das darin zum Ausdruck kommende Wissen über die Zielsysteme. *M. C. Libicki*, Cyberdeterrence and Cyberwar, 2009, S. 44 ff., 47 f. Die kontextbezogene Zurechnung mag für das Regime der Staatenverantwortlichkeit ungenügend sein, ist aber im Bereich der Staatenhaftung zulässig, da hier allgemein weniger strenge Anforderungen gelten. Vgl. in Bezug auf politische Zurechnung *K. Ziolkowski*, Confidence Building Measures for Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 553 (556).

94 Siehe 3. Kapitel E. I.

ist aber bei der Staatenhaftung gerechtfertigt, da Staaten hier kein Fehlverhalten ihrerseits eingestehen müssen, sondern lediglich für den eigenen kausalen Beitrag zur Verursachung eines Schadens durch völkerrechtskonformes Verhalten Entschädigung leisten müssen.[95] Wie gezeigt, kommt hier der Verursachergrundsatz zum Tragen, nach dem schon einzelne Verursachungsbeiträge die Kausalitätsanforderungen erfüllen.[96] In Haftungsübereinkommen finden sich bereits entsprechende Regeln für eine gesamtschuldnerische Haftung der beteiligten Staaten, wenn beispielsweise zwei Weltraumgegenstände zur Schädigung eines Drittstaates beitragen (Art. IV Weltraumhaftungsübereinkommen). Zwar besteht für den in Anspruch genommenen Staat die Möglichkeit zur Schadloshaltung bei den anderen mitverursachenden Staaten, so dass auch eine Gesamthaftung in Betracht käme. Allerdings dürfte dieser Ansatz außerhalb völkervertraglicher Übereinkünfte auf Ablehnung der Staaten stoßen,[97] weil sie möglicherweise Hindernisse bei der Regressnahme befürchten. Daher ist in dieser Konstellation eine anteilige Haftung der jeweiligen Ursprungsstaaten interessengerecht und vorzugswürdig.[98]

II. Schadensvermeidung und Schadenskompensation

Die völkerrechtliche Diskussion über die Verantwortung von Staaten für Informationsoperationen entfernt sich sinnvollerweise von dem Erfordernis völkerrechtlicher Verbotstatbestände hin zum Erfordernis allgemei-

95 *M. B. Akehurst*, International liability for injurious consequences arising out of acts not prohibited by international law, NYIL 16 (1985), S. 3 (15) unter Bezugnahme auf Sonderberichterstatter *R. Q. Quentin-Baxter*, Preliminary report on international liability for injurious consequences of acts not prohibited by international law, YBILC 1980-II/1, UN Doc. A/CN.4/334 and Add.l and 2, S. 263, Rn. 56; siehe auch *J. E. Noyes/B. D. Smith*, State Responsibility and the Principle of Joint and Several Liability, YIL 13 (1988), S. 225 (264). Selbst wenn man die notwendige Kausalität nur dann bejahen wollte, wenn Bots auf dem Hoheitsgebiet oder unter der Hoheitsgewalt eines Staates für sich genommen einen erheblichen Schaden verursachen, ist jedenfalls – im Gegensatz zur Schwelle der Völkerrechtswidrigkeit – die Schwelle zur Erheblichkeit schneller erreicht, so dass die Staatenhaftung auch hier greifen kann.

96 2. Kapitel B. I. 3.

97 Vgl. *J. Bäumler*, Das Schädigungsverbot im Völkerrecht, 2017, S. 282.

98 *Ibid*.

ner Schadensvermeidungspflichten für die virtuelle Welt.[99] Themen wie Kriegsführung und Gegenmaßnahmen in der virtuellen Welt rücken derweil in den Hintergrund. Die vom Europarat aufgestellte Arbeitsgruppe zu grenzüberschreitenden Fragen des Internet (Ad-hoc Advisory Group on Cross-border Internet) betonte überdies, dass sich die staatliche Pflicht zur Verhinderung und Regulierung grenzüberschreitender Störungen des Internets grundsätzlich von der Frage der Staatenverantwortlichkeit für völkerrechtswidriges Verhalten unterscheidet und legte den Fokus ihrer Untersuchungen auf verfahrensbezogene Schadensvermeidungspflichten und Sorgfaltsstandards in der virtuellen Welt.[100] Die diskutierten Regelungsansätze bilden die Grundlage für die Konkretisierung von Schadensvermeidungspflichten in der virtuellen Welt und liefern mithin Anknüpfungspunkte für einen gerechten Schadensausgleich für Schäden durch völkerrechtlich nicht verbotene Informationsoperationen.

1. Schadensprävention

Die Staaten müssen alle möglichen und zumutbaren Maßnahmen ergreifen, um erheblichen grenzüberschreitenden Schäden durch die Nutzung von informationstechnischen Systemen zuvorzukommen oder zumindest deren konkretes Risiko zu minimieren.[101]

Die effektive Umsetzung von konkreten Präventionspflichten in der virtuellen Welt ist wiederum von der schädigenden Informationsoperation im Einzelfall abhängig.

Prävention in der virtuellen Welt ist offenkundig bei staatseigenen oder staatlich befürworteten Informationsoperationen möglich. Da es aber gerade das Ziel von Informationsoperationen ist, grenzüberschreitende

---

99 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (132 f.) m.w.N.

100 Council of Europe, Ad-hoc Advisory Group on Cross-border Internet, Interim Report to the Steering Committee on the Media and New Communication Services incorporating Analysis of Proposals for International and Multi-stakeholder Cooperation on Cross-border Internet, H/Inf(2010)10, Rn. 85.

101 Vgl. 2. Kapitel B. II.; Council of Europe, Ad-hoc Advisory Group on Cross-border Internet, Interim Report to the Steering Committee on the Media and New Communication Services incorporating Analysis of Proposals for International and Multi-stakeholder Cooperation on Cross-border Internet, H/Inf(2010)10, Rn. 72, 74; *R. Kolb*, Reflections on Due Diligence Duties and Cyberspace, GYIL 58 (2015), S. 113 (123).

Schäden zu verursachen, werden Ursprungsstaaten keine Maßnahmen zur Schadensprävention oder Risikominimierung ergreifen. Staaten könnten allenfalls Anlass zur Risikoanalyse, Regulierung und Kontrolle der (hoch-)gefährlichen Informationsoperation haben, um möglichen Kollateralschäden an Drittstaaten (*Spillover*-Effekte) zuvorzukommen oder deren Risiko zu begrenzen. Kooperationspflichten wird der Ursprungsstaat in aller Regel aufgrund von Geheimhaltungsinteressen weder mit Zielstaaten noch mit potenziell betroffenen Drittstaaten umsetzen.

Bei nicht-staatlichen Informationsoperationen besteht zwar kein staatliches Geheimhaltungsinteresse, so dass eine Kooperation mit betroffenen Staaten durch Benachrichtigung, Information, Warnung und Konsultation möglich ist.[102] Maßnahmen zur Schadensprävention können allerdings aufgrund der Zeit-Raum-Kompression in der virtuellen Welt einerseits und des heimlichen Charakters von Informationsoperationen andererseits in aller Regel nicht ergriffen werden, bevor eine nicht-staatliche Informationsoperation durchgeführt wird und mithin grenzüberschreitende Schäden eingetreten sind oder ein konkretes Risiko gegeben ist.[103] Neben den technischen Hürden bei der Entdeckung von nicht-staatlichen Informationsoperationen ist überdies zu beachten, dass die in Betracht kommenden Maßnahmen der Schadensprävention, namentlich Überwachungs- und Kontrollmechanismen, erheblichen menschenrechtlichen Bedenken begegnen.[104] Denn anders als im Kontext umweltbelastender Aktivitäten können in der virtuellen Welt Präventionspflichten nicht nach Größe und Ausmaß der gefährlichen Aktivitäten begrenzt werden. Smartphones,

---

102 Eine Mitteilungs- und Warnpflicht bei Computerviren wird teilweise in Analogie zu den Vorgaben der Weltgesundheitsorganisation in Fällen von Infektionskrankheiten vorgeschlagen. So *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, Juristenzeitung 14 (2015), S. 685 (689); siehe auch *R. Geiß/H. Lahmann*, Freedom and Security in Cyberspace, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 621 (656).

103 Die Experten des Tallinn Manual 2.0 gehen noch weiter und stellen nicht nur die effektive Umsetzbarkeit von Präventionspflichten in der virtuellen Welt in Frage, sondern verneinen schon das Bestehen von Präventionspflichten und schließen allgemeine Vorsorgemaßnahmen kategorisch aus. Tallinn Manual 2.0, Kommentar zu Regel 7, S. 44 f., Rn. 7 ff. Dies liegt daran, dass die Experten zum einen Kenntnis des Ursprungsstaates von der Informationsoperation voraussetzen (Kommentar zu Regel 7, S. 45, Rn. 9), und zum anderen daran, dass sie keine klare Trennung zwischen Verhinderungs- und Schadensvermeidungspflichten vornehmen (Kommentar zu Regel 7, S. 44 f., Rn. 7).

104 Vgl. Tallinn Manual 2.0, Kommentar zu Regel 7, S. 45, Rn. 8; *O. Dörr*, Obligations of the State of Origin of a Cyber Security Incident, GYIL 58 (2015), S. 87 (95).

Computer und sonstige Geräte sind gleichermaßen geeignet, erhebliche grenzüberschreitende Schäden durch Informationsoperationen zu verursachen.[105] Eine breit angelegte Überwachung aller informationstechnischen Aktivitäten auf staatlichem Territorium bzw. unter staatlicher Hoheitsgewalt wäre mit menschenrechtlichen Verpflichtungen zum Schutz der Privatheit unvereinbar.[106] Folglich führen die spezifischen Charakteristika von Informationsoperationen nur zu beschränkten Möglichkeiten der Schadensprävention in der virtuellen Welt.

2. Schadensvorsorge

Während staatliche Präventionspflichten von der konkreten Gefahr durch spezifische Informationsoperationen abhängig sind, werden durch den Vorsorgegrundsatz die staatlichen Pflichten weit ins Vorfeld einer Gefahr verlagert. Der Vorsorgegrundsatz gelangt zur Anwendung, wenn Ursachenzusammenhänge und Auswirkungen von zu regulierenden Vorgängen ungewiss sind. Vorsorgemaßnahmen sind schon zu ergreifen, bevor ein konkretes Schadensrisiko entsteht.[107] Dies ist insbesondere in der virtuellen Welt, die durch wissenschaftliche und technische Unsicherheiten bei der Regulierung informationstechnischer Aktivitäten gekennzeichnet ist, sinnvoll.[108] Staaten müssen von vornherein strategische, politische, organisatorische, administrative und legislative Vorkehrungen für den Betrieb informationstechnischer Systeme treffen.[109] Anleihen für konkrete Vorsorgemaßnahmen lassen sich dabei dem Umweltkontext entnehmen.

---

105 So *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, Juristenzeitung 14 (2015), S. 685 (688).

106 *J. Healey/H. Pitts*, Applying International Environmental Legal Norms to Cyber Statecraft, I/S: A Journal of Law and Policy for the Information Society 8 (2012), S. 356 (365 f.); *A. Reinisch/M. Beham*, Mitigating Risks, GYIL 58 (2015), S. 101 (112); *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, Juristenzeitung 14 (2015), S. 685 (688).

107 Siehe 1. Kapitel E. II. 3.

108 *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (5 f.); *T. Marauhn*, Customary Rules of International Environmental Law, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 465 (475); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 215.

109 *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (169).

a) Kooperation

Wie im Umweltkontext bilden Kooperationspflichten auch in der virtuellen Welt einen zentralen Anknüpfungspunkt zur Schadensvorsorge. Effektive Sicherheitsvorkehrungen sind nur durch Information, Warnung, Benachrichtigung und Konsultationen möglich.[110] Der Zugang zu sicherheitsrelevanten Informationen kann durch Meldepflichten über feindliche Aktivitäten und durch das Einrichten von Frühwarnverfahren gewährleistet werden.[111] Die Effektivität solcher Maßnahmen zeigt sich am Beispiel der Informationsausspähungen, die oftmals für zukünftige Manipulations- und Sabotageakte genutzt werden.[112] Aufgrund einer entsprechenden Information kann eine vorsorgliche Abschaltung oder Neukonfiguration kompromittierter Systeme erfolgen, um weiteren nachteiligen Auswirkungen zuvorkommen.[113] Aber auch Informationsaustauch über den Umgang mit Präzedenzfällen kann zur Reifung von erprobten Reaktionsmaßnahmen auf Informationsoperationen beitragen.[114] Schließlich ist die multinationale und organisationsübergreifende Koordination zur Bewältigung virtueller Bedrohungslagen zu verbessern und Dialoge mit Stakeholdern aus dem Bereich der Cybersicherheit sind zu fördern.[115] Diese konkreten Pflichten sind für informationstechnische Systeme noch nicht etabliert, können aber als politisch verbindliche Richtlinien langfristig zu Gewohnheitsrecht erstarken.[116] Entsprechende Forderungen finden sich bereits im internationalen Diskurs zur Cybersicherheit.[117]

---

110 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (144 ff., 149); *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (20).

111 *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (18 f.).

112 *Id.*, S. 1 (19).

113 *S. Gaycken*, Die vielen Plagen des Cyberwar, in: R. Schmidt-Radefeldt/C. Meissler (Hg.), Automatisierung und Digitalisierung des Krieges, 2012, S. 89 (110).

114 Vgl. *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, Juristenzeitung 14 (2015), S. 685 (689).

115 Ausführlich zu den Regulierungsansätzen internationaler und regionaler Organisationen im Bereich Cybersicherheit und den derzeitigen Schwächen *L. Areng*, International Cyber Crisis Management and Conflict Resolution Mechanisms, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 565 (565 ff.).

116 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 6; *K. Ziolkowski,* Confidence Building Measures for Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 553 (560 f.).

117 Ausführlich hierzu siehe *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 170 ff., 199 f., 219.

b) Risikoanalyse

Eine Risikoanalyse von möglicherweise schädigenden Aktivitäten ist nicht nur im Umweltkontext sinnvoll, sondern auch in der virtuellen Welt denkbar. Eine Art Cyberumweltverträglichkeitsprüfung kann die möglichen Auswirkungen des Betriebs informationstechnischer Systeme bewerten und unter Umständen als Vorsorgemaßnahme eine Nutzungsbeschränkung oder gar ein Verbot gebieten.[118] In diese Richtung gehen auch Überlegungen, die einen Vergleich zu Massenvernichtungswaffen und Atomwaffen vornehmen.[119] Entsprechende Diskussionen zu einer Vorsorgeverpflichtung von Staaten, die Entwicklung, Herstellung und Anwendung von Schadprogrammen und -befehlen (sogenannte Informationswaffen) zu untersagen, wurden schon 1998 im Rahmen der Vereinten Nationen geführt.[120] Im Ergebnis ist dieser Ansatz aber nicht umsetzbar, da Informationsoperationen eben mittels alltäglicher Informationstechnik erfolgen, ihren Ausgangspunkt überall haben und über unterschiedliche Pfade laufen können.[121] Ein Betriebsverbot informationstechnischer Systeme ist im Ergebnis unrealistisch und auch eine Nutzungsbeschränkung ist in der virtuellen Welt kaum zu kontrollieren.[122]

c) Beste Schutzpraktiken

Eine Umsetzung des Vorsorgegrundsatzes in Gestalt von besten Schutzpraktiken ist in der virtuellen Welt von besonderem Interesse, da hier – wie auch im Umweltkontext – eine Kombination von Einsatzmitteln,

118 Nach *C. Walter* sprechen Gründe des Freiheitsschutzes gegen eine „Cyberverträglichkeitsprüfung". *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, Juristenzeitung 14 (2015), S. 685 (688 f.).

119 Siehe hierzu *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (7 f.); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 216 ff.

120 VN-Generalversammlung, First Committee, Fifty-third session, 30. September 1998, Role of science and technology in the context of international security, disarmament and other related fields, Appendix Developments in the field of information and telecommunications in the context of international security Russian Federation: draft resolution, UN Doc. A/C.1/53/3, S. 3 f., Abs. 7, Rn. 3, lit. c.

121 *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (8); zustimmend *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 217.

122 Vgl. *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 217 f.

wie Kontrollmaßnahmen und weitergehende Strategieentwicklung, zielführend ist.[123] Wenngleich der Betrieb informationstechnischer Systeme im Allgemeinen aufgrund von menschenrechtlichen Bedenken keiner umfassenden Kontrolle unterstellt werden kann, ist dies für besonders schützenswerte informationstechnische Systeme denkbar. Demnach ist zunächst eine Unterscheidung zwischen kritischen Infrastrukturen, wie etwa von Krankenhäusern, Atomkraftwerken oder militärischen und staatlichen Einrichtungen, und sonstigen Informationsinfrastrukturen vorzunehmen.[124] Erstere erfordern besondere Vorsorge vor Gefahren durch Informationsoperationen, da zum einen verheerende Folgen durch Angriffe drohen und zum anderen aufgrund der globalen Vernetzung Angriffe auf kritische Infrastrukturen in einem Staat zu empfindlichen Auswirkungen auf interdependente Systeme und Netzwerke in anderen Staaten führen können.[125] Die Begrenzung auf militärische und kritische zivile Infrastrukturen rechtfertigt eine staatliche Überwachung und ist durch eine entsprechende Entnetzung auch technisch möglich.[126] Die Entkopplung von zivilen Netzwerken und ausschließliche Nutzung von stark kontrollierten internen Netzen ist in Anbetracht der besonderen Gefährdungslage auch trotz der hohen Umstellungskosten nicht unverhältnismäßig,[127] zumal die Neuorientierung schrittweise erfolgen kann.

Schließlich erfordern die besten Schutzpraktiken aber zusätzlich, den Selbstschutz informationstechnischer Systeme im Allgemeinen zu erhöhen

123 Vgl. mit Blick auf Kapazitätenaufbau im Bereich Cybersicherheit *H. Tiirmaa-Klaar*, Cyber Diplomacy, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 509 (523 ff.).

124 Vgl. *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (17 f.). Zum Begriff der kritischen Infrastrukturen *S. Gaycken/M. Karger*, Entnetzung statt Vernetzung, Paradigmenwechsel bei der IT-Sicherheit, Multimedia und Recht 1 (2011), S. 3 (5); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 19 ff.

125 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 219.

126 *S. Gaycken/M. Karger*, Entnetzung statt Vernetzung, Multimedia und Recht 1 (2011), S. 3 (8); *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (17 f.); *S. Schmahl*, Cybersecurity, in: N. Dethloff/G. Nolte/A. Reinisch (Hg.), Freiheit und Regulierung in der Cyberwelt, 2016, S. 159 (182) m.w.N.; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 203 f.

127 *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (17 f.).

und fortwährend dem Stand der Technik anzupassen[128] sowie Notfallpläne für informationstechnische Vorfälle aufzustellen.[129]

3. Schadensminderung

Auch wenn aufgrund der wissenschaftlichen und technischen Unsicherheiten selten Maßnahmen zur Schadensprävention vor Beginn einer (nichtstaatlichen) Informationsoperation ergriffen werden können, sind jedenfalls nach Eintritt eines Vorfalls und bei andauernden Geschehnissen sowohl vom Ursprungs- als auch vom Opferstaat Maßnahmen zur Schadensminderung zu ergreifen. Die Schadensminderungspflicht stellt eine Verlängerung der Schadenspräventionspflicht in die Phase der andauernden bzw. beendeten Informationsoperation dar. In dieser Phase ist eine konkrete Gefährdungslage durch eine Informationsoperation gegeben und die Auswirkungen sind in aller Regel bestimmbar.[130] Darüber hinaus kann der Ursprung der Informationsoperation auf spezifische informationstechnische Systeme nun eingegrenzt oder gar zurückgeführt werden, so dass entsprechende Maßnahmen zur Beseitigung oder Begrenzung negativer Auswirkungen durchführbar sind.[131]

Zuvorderst sind aber auch hier menschenrechtliche Schutzgewährleistungen und staatliche Bestrebungen zur Beendigung schadhafter Informationsoperationen – durch Abwägung zwischen Eingriff und Legitimität im Einzelfall – in Einklang zu bringen.[132] Wenn Staaten die eigene Infrastruktur sichern und abschalten, sind etwaige Auswirkungen auf die In-

---

128 *S. Gaycken/M. Karger*, Entnetzung statt Vernetzung, Multimedia und Recht 1 (2011), S. 3 (5); *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (19); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 204.

129 *S. Gaycken/M. Karger*, Entnetzung statt Vernetzung, Multimedia und Recht 1 (2011), S. 3 (5); *O. Gross*, Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (501 f.).

130 Vgl. *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, Juristenzeitung 14 (2015), S. 685 (689 f.) unter Hinweis auf Präventionsartikel, Kommentar zu Art. 12, S. 165, Abs. 12.

131 In diese Richtung zielt auch die Sorgfaltsregel des Tallinn Manual 2.0, wonach alle möglichen Maßnahmen zu ergreifen sind, um eine Informationsoperation zu beenden (Regel 7 Tallinn Manual 2.0).

132 Die Meinungsäußerungsfreiheit im Internet kann beispielsweise nur aufgrund des aus Menschenrechtskodifikationen bekannten dreiteiligen Tests eingeschränkt werden. VN Human Rights Council, Sonderberichterstatter *Frank La Rue*, Report on the Promotion and Protection of the Right to Freedom of Opin-

formations- und Kommunikationsinfrastruktur des eigenen Staates sowie von Drittstaaten so gering wie möglich zu halten.[133] Denn jeder Mensch hat „das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten".[134] Zudem hat ein vernünftiger Interessenausgleich mit Blick auf Natur, Ausmaß und Reichweite des (potenziellen) Schadens beim Ursprungsstaat einerseits und beim betroffenen Staat andererseits zu erfolgen.[135] Schließlich dürfen Selbsthilfemaßnahmen, wie sogenannte *Hackbacks*, welche darauf gerichtet sind die Systeme des Angriffsursprungs außer Dienst zu stellen oder zu zerstören, zumeist aufgrund rechtlicher Hürden nicht ergriffen werden. Derartige Informationsoperationen verletzen nämlich unter Umständen Schutzgewährleistungen des humanitären Völkerrechts und/oder nationale Vorschriften.[136] Diese Defizite können zum Teil durch verfahrensbezogene Pflichten aufgefangen werden.[137] Damit wird deutlich, dass in dieser Phase zwischenstaatliche Kooperationspflichten wie Informationsaustauch, Mitteilung und Warnung sowie Absprachen zu Abhilfemaßnahmen, essenziell für eine Schadensbegrenzung sind.[138]

---

ion and Expression, UN Doc. A/HRC/17/27, 16.05.2011, S. 19, Rn. 69, S. 20, Rn. 72.

133 Tallinn Manual 2.0, Kommentar zu Regel 7, S. 49 f., Rn. 25.

134 Art. 19 Allgemeine Erklärung der Menschenrechte; siehe auch Art. 19 Internationaler Pakt über Bürgerliche und Politische Rechte; Art. 10 Europäische Menschenrechtskonvention; Art. 13 Amerikanische Menschenrechtskonvention; Art. 9 Afrikanische Menschenrechtskonvention.

135 Tallinn Manual 2.0, Kommentar zu Regel 7, S. 49 f., Rn. 25.

136 *O. Gross*, Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (501) m.w.N.

137 Vgl. *O. Dörr*, Obligations of the State of Origin of a Cyber Security Incident, GYIL 58 (2015), S. 87 (96).

138 *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (186). Es wird indes vorgeschlagen, dass sich diese Kooperationspflicht auch auf die Ermittlung und Verfolgung von Urhebern schadhafter Informationsoperationen erstreckt. *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (145) unter Bezugnahme auf *M. J. Sklerov*, Solving the Dilemma of State Responses to Cyberattacks, Military Law Review 201 (2009), S. 1 (62) und *W. Heintschel von Heinegg*, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies 89 (2013), S. 123 (135). Allerdings geht es im Rahmen der Staatenhaftung um Schadensvermeidungs- und Kompensationspflichten und nicht um Verhinderungs- bzw. Schutzpflichten mit Blick auf kriminelle Aktivitäten, die eine strafrechtliche Verfolgung

4. Schadenskompensation

Angesichts der dargelegten Schwierigkeiten bei der Schadensvermeidung in der virtuellen Welt kann es regelmäßig dennoch zu einem erheblichen grenzüberschreitenden Schaden durch völkerrechtlich nicht verbotene Informationsoperationen kommen. Daher ist der Staat, auf dessen Territorium bzw. unter dessen Hoheitsgewalt eine Informationsoperation stattfindet, die einen erheblichen Schaden in einem anderen Staat verursacht, zur Kompensation der entstandenen Schäden verpflichtet. Bei der Bemessung der Kompensationspflicht werden die ergriffenen Maßnahmen zur Schadensvermeidung, das heißt Schadensprävention, Schadensvorsorge und Schadensminderung, Berücksichtigung finden. Der Opferstaat darf nicht auf den Kosten sitzen bleiben, gleichzeitig hat ein gerechter Interessenausgleich zwischen den betroffenen Staaten zu erfolgen.[139] So ist bei der Bemessung der Kompensationspflicht auch der Grad der Beteiligung des Opferstaates an der Konfliktlage in die Abwägung miteinzubeziehen. Die staatliche Einstandspflicht für reaktive völkerrechtmäßige *Hackbacks*[140] auf feindliche Informationsoperationen ist beispielsweise im Umfang zu begrenzen, wenn deren Auswirkungen nicht außer Verhältnis stehen.

III. Gebotene Sorgfalt

Die gebotene Sorgfalt zur Schadensvermeidung richtet sich auch in der virtuellen Welt nach der konkreten Gefährdungslage und dem anzulegenden Sorgfaltsmaßstab. Grundsätzlich gilt, dass gefährliche Aktivitäten, denen das Risiko erheblicher Schäden immanent ist, einen flexibleren Sorgfaltsstandard erfordern als hochgefährliche Aktivitäten, die zu katastrophalen Schäden führen können.[141] Informationsangriffe gebieten demnach die Beachtung eines strikten Sorgfaltsstandards, während bei Informationsausbeutungen flexible Sorgfalt gilt.

Dies entbehrt aber nicht, den Kontext, Sinn und Zweck der gebotenen Sorgfalt zur Schadensvermeidung sowie die Umstände des konkreten Einzelfalls bei der Bestimmung des Sorgfaltsstandards zu berücksichtigen. So

---

und Bestrafung von Tätern erfordern. Vgl. in Bezug auf die Sorgfaltspflicht des Tallinn Manual 2.0, Kommentar zu Regel 7, S. 48, Rn. 21.

139 Siehe 2. Kapitel B. II.

140 Siehe hierzu *J. E. Messerschmidt*, Hackback, Col. JTL 52 (2013), S. 275 (275 ff.).

141 Siehe 2. Kapitel B. III.

sind aufgrund des absichtlichen Charakters von Informationsoperationen unterschiedliche Sorgfaltsmaßstäbe bei staatlichen und staatlich befürworteten Informationsoperationen einerseits und nicht-staatlichen Informationsoperationen andererseits anzulegen.[142]

Bei staatlichen oder staatlich befürworteten Informationsoperationen ist angesichts der intendierten Schäden eine Missachtung der gebotenen Sorgfalt – unabhängig vom anzulegenden Maßstab – indiziert, so dass den Staat diesbezüglich in jedem Fall eine vollumfängliche Einstandspflicht trifft. Nichts anderes gilt für Kollateralschäden. Bedingt durch die internationale Vernetzung und den ubiquitären Charakter des Internets können selbst strategisch und technisch durchdachte Informationsoperationen zu nicht in unmittelbarem Zusammenhang mit dem Ziel der Operation stehenden, aber dennoch billigend in Kauf genommen Begleitschäden führen.[143] Folglich erübrigt sich hier eine Differenzierung der Sorgfaltsanforderungen nach gefährlichen und hochgefährlichen Informationsoperationen.

Bei nicht-staatlichen Informationsoperationen ist nicht die Absicht oder Fahrlässigkeit der nicht-staatlichen Akteure entscheidend, sondern die Missachtung der gebotenen Sorgfalt bei der Schadensvermeidung durch den Staat, auf dessen Hoheitsgebiet bzw. unter dessen Hoheitsgewalt informationstechnische Systeme für die Informationsoperation genutzt werden. Allerdings ist eine *ex ante* Bestimmung der Gefährdungslage nach Art und Ausmaß der nicht-staatlichen Informationsoperation nicht möglich und eine *ex post* Bewertung zur Festlegung des Sorgfaltsstandards wäre der Rechtssicherheit abträglich.[144] Dementsprechend ist für die Bestimmung der Sorgfaltsanforderungen auf das Risiko, das informationstechnischen Systemen im Allgemeinen immanent ist, abzustellen. Die Staaten müssen bei deren Nutzung durch nicht-staatliche Akteure die gebotene Sorgfalt zur Schadensvermeidung walten lassen.[145] Bei der nicht-staatlichen Nutzung informationstechnischer Systeme besteht die Wahrscheinlichkeit katastrophaler Schadensfolgen, da diese Systeme sowohl gefährlichen In-

142 Zwar spielt die Absicht bei der Staatenhaftung selbst keine Rolle, sie ist aber durchaus bei der Bewertung der gebotenen Sorgfalt von Interesse. *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1503 f., 1499).

143 *A. McKay/J. Neutze/P. Nicholas/K. Sullivan*, International Cyber Security Norms, Reducing Conflict in an Internet- Dependent World, Microsoft Whitepaper 2014, abrufbar unter: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA (geprüft am 15.05.2020), S. 4.

144 Vgl. 2. Kapitel B. III.

145 Für unfallbedingte Schäden durch die Nutzung informationstechnischer Systeme kann nichts anderes gelten.

formationsausbeutungen als auch hochgefährlichen Informationsangriffen zugänglich sind.[146] Damit scheint ein strikter Sorgfaltsstandard für informationstechnische Systeme im Allgemeinen angezeigt.

Doch ein solcher Sorgfaltsstandard würde Staaten zu einer Kontrolle dieser Systeme und Beschränkung des freien Zugangs und der freien Nutzung motivieren, was aus menschenrechtlichen Gesichtspunkten bedenklich ist.[147] Ein strikter Sorgfaltsstandard könnte gar ein Nutzungsverbot von informationstechnischen Systemen aufgrund der nicht auszuschließenden Möglichkeit katastrophaler Schadensfolgen erfordern. Dies ließe aber den erheblichen sozialen, ökonomischen und technischen Nutzen von informationstechnischen Systemen außer Acht. Ein Ausgleich dieser Belange kann nur mit einem nachgiebigen, das heißt flexibleren Sorgfaltsstandard erreicht werden.[148]

Ferner ist die gebotene Sorgfalt in der von technischen und wissenschaftlichen Unsicherheiten geprägten virtuellen Welt in hohem Maße von den zumutbaren und zur Verfügung stehenden Möglichkeiten zur Schadensvermeidung abhängig. Geeignete und angemessene Schadensvermeidungsmaßnahmen sind nicht immer verfügbar.[149] So kann unter Verhältnismäßigkeitsgesichtspunkten nicht erwartet werden, dass ein Staat etwa seine gesamte Kommunikationsinfrastruktur abstellt, um negative Auswirkungen auf andere Staaten zu vermeiden.[150]

Schließlich müssen die Sorgfaltsanforderungen entsprechend den unterschiedlichen technischen Kapazitäten und Fähigkeiten von Staaten variabel bleiben.[151] Ein subjektiver Sorgfaltsstandard, der sich am (sicherheits-)technischen Entwicklungsstand eines Staates orientiert, ist zwar problematisch, weil angesichts der globalen Vernetzung Sicherheitslücken in einem weniger entwickelten Staat genutzt werden könnten, um in verbun-

146 Siehe 3. Kapitel A und B.

147 Vgl. Tallinn Manual 2.0, Kommentar zu Regel 6, S. 31 f., Rn. 5 f., Kommentar zu Regel 7, S. 45, Rn. 8; *O. Dörr*, Obligations of the State of Origin of a Cyber Security Incident, GYIL 58 (2015), S. 87 (95).

148 Vgl. *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1492 ff.).

149 Tallinn Manual 2.0, Kommentar zu Regel 7, S. 47, Rn. 16 f., S. 49, Rn. 24; *R. Kolb*, Reflections on Due Diligence Duties and Cyberspace, GYIL 58 (2015), S. 113 (126 f.).

150 Tallinn Manual 2.0, Kommentar zu Regel 7, S. 49 f., Rn. 25.

151 *R. Kolb*, Reflections on Due Diligence Duties and Cyberspace, GYIL 58 (2015), S. 113 (123); *A. Reinisch/M. Beham*, Mitigating Risks, GYIL 58 (2015), S. 101 (105 f.).

denen Systemen weltweit Schäden anzurichten.[152] Ein objektiver Standard kommt allerdings nicht in Betracht, da einem Staat keine ihm aufgrund seines Leistungsvermögens unmögliche Pflicht auferlegt werden kann.[153] Ein subjektiver Maßstab führt zu dem interessengerechten Ergebnis, dass die Anforderungen an technisch entwickelte Staaten aufgrund des ihnen zugänglichen Wissens und der technischen Möglichkeiten höher sind.[154] Zudem werden die weiter entwickelten Staaten, die im Grunde nicht gewillt sind, ihre grundsätzlich als vertraulich eingestuften Möglichkeiten zur Aufdeckung und Bekämpfung von Informationsangriffen Preis zu geben,[155] zur Zusammenarbeit und zum Kapazitätenaufbau sowie Technologietransfer veranlasst. Schließlich haben sie ein ureigenes Interesse am Schließen von Sicherheitslücken, die zu grenzüberschreitenden Schäden führen können.[156]

IV. Haftungsart und -standard

Für die Umsetzung einer Haftung für informationstechnische Systeme sind schließlich die Haftungsart und der Haftungsstandard festzulegen.

1. Haftungsart

Wie sich aus der Rechtsquellenanalyse im 1. Kapitel ergibt, kennt das Völkerrecht die primäre Staatenhaftung, die subsidiäre Staatenhaftung und die ergänzende Staatenhaftung. Im Folgenden wird dargetan, dass bei der Umsetzung eines Haftungssystems für informationstechnische Systeme alle drei Haftungsarten zum Tragen kommen. Ein Rückgriff auf die Ausführungen zu den Haftungsübereinkommen[157] sowie zum Verursa-

152 *O. Gross*, Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents, Cornell ILJ 48 (2015), S. 481 (498); *R. Kolb*, Reflections on Due Diligence Duties and Cyberspace, GYIL 58 (2015), S. 113 (127).

153 *R. Kolb*, Reflections on Due Diligence Duties and Cyberspace, GYIL 58 (2015), S. 113 (123).

154 Siehe 2. Kapitel B. III.

155 *M. N. Schmitt*, The Law of Cyber Warfare, SLPR 25 (2014), S. 269 (278).

156 *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 221 m.w.N.

157 Siehe 1. Kapitel D.

chergrundsatz[158] zeigt besonders deutlich, dass dem Haftungssystem für die virtuelle Welt dieselben Erwägungen wie den Haftungskonzeptionen im Umweltvölkerrecht zugrunde liegen: Zunächst dürfen die Schäden durch gefährliche Aktivitäten in der virtuellen Welt ebenso wenig auf das Opfer abgewälzt werden. Folgerichtig müssen die direkten Schadensverursacher primär haften (a). Des Weiteren ist auch hier die Garantenstellung der Staaten im internationalen Gefüge von Bedeutung.[159] Sofern der Schadensausgleich durch den Verursacher im engeren Sinne nicht oder nur begrenzt erfolgt, ist eine subsidiäre bzw. ergänzende Haftung des Ursprungsstaates angezeigt. Vergleichbar mit der Schlüsselfunktion des Ursprungsstaates aufgrund der Erlaubnis zum Betrieb umweltgefährdender Anlagen setzt der Staat durch die Erlaubnis zum Betrieb informationstechnischer Systeme auf seinem Hoheitsgebiet indirekt die Schadensursache und ist damit in der virtuellen Welt ebenfalls als Verursacher im weiteren Sinne zu qualifizieren (b). Der Umfang der ergänzenden und der subsidiären Staatenhaftung ist schließlich – wie im Umweltvölkerrecht auch – entsprechend der staatlichen Bemühungen zur Schadensvermeidung zu begrenzen.[160] Daher ist auf dritter Ebene ein Entschädigungsfonds durch die Staatengemeinschaft einzurichten, der darüber hinausgehende Schäden auffängt. Der Fonds soll aber nicht nur ergänzend, sondern insbesondere auch subsidiär greifen, wenn der Ursprungsstaat der Informationsoperation schon nicht festgestellt werden kann. Durch den Entschädigungsfonds wird so eine Kollektivierung des Schadensausgleiches möglich. Auch diese Idee stammt aus dem Umweltvölkerrecht, wo Entschädigungsfonds als Ausdruck des Interesses der Staatengemeinschaft am Ausgleich katastrophaler (Umwelt-)Schäden und am Erhalt von Gemeinschaftsgütern fungieren (c).

a) Primäre Staatenhaftung für staatliche und staatlich befürwortete Informationsoperationen

Nach dem Verursachergrundsatz trifft die Kompensationspflicht den Urheber der grenzüberschreitenden Schädigung. Demnach muss der Staat Entschädigung leisten, wenn staatseigene Informationsoperationen grenzüberschreitende Schäden verursachen. Im Umweltkontext sind ferner Be-

158 Siehe 1. Kapitel E. III.
159 Vgl. 1. Kapitel C. II. 6.
160 Vgl. 1. Kapitel A. II. 1. c) und 1. Kapitel D. IV. 2.

treiber (hoch-)gefährlicher Aktivitäten bzw. Eigentümer von Anlagen bzw. Schiffen, die für (hoch-)gefährliche Aktivitäten genutzt werden, als Verursacher zu qualifizieren und mithin zur Schadenskompensation verpflichtet. Übertragen auf die virtuelle Welt sind Staaten als Betreiber bzw. Eigentümer regierungseigener Informationsinfrastrukturen zu betrachten und daher für grenzüberschreitende Schäden durch die Nutzung dieser Systeme einstandspflichtig.[161]

Dies bedeutet jedoch nicht, dass Staaten ohne Urheber- oder Betreiber- bzw. Eigentümereigenschaft *per se* von der Haftung freigestellt sind. Dies gilt namentlich bei staatlich befürworteten Informationsoperationen. Hier müssen unter Gerechtigkeitserwägungen die Vorteile, welche dem Staat durch derartige Informationsoperationen entstehen, Berücksichtigung finden. Denn Informationsoperationen durch patriotische Hacker und staatliche Stellvertreter bedeuten durchaus wirtschaftliche Vorteile und politisch-strategischen Machtgewinn auf internationaler Ebene für Staaten.[162] Bei derartigen Informationsoperationen liegt es nahe, dass die profitierenden Staaten diese ignorieren bzw. dulden. Damit verschmelzen staatliche und nicht-staatliche Akteure zu Verursachern von pseudostaatlichen Informationsoperationen.[163] Hier entgehen Staaten zwar einer zurechnungsbasierten Staatenverantwortlichkeit für staatlich befürwortete Informationsoperationen, jedoch muss der Staat als Kehrseite der erlangten Vorteile auch für Schäden einstehen.

In diesem Zusammenhang sind erneut die Beweisschwierigkeiten mit Blick auf den staatlichen Ursprung bzw. die staatliche Befürwortung einer Informationsoperation zu berücksichtigen. Während Indizienbeweise für die Zurechnung einer völkerrechtswidrigen Aktivität nicht ausreichen,[164] ist im Rahmen der Staatenhaftung aber eine erleichterte Beweisführung gestattet.[165] In Konstellationen, in denen die Beweise der ausschließlichen

---

161 Vgl. *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (209 f.).

162 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 5, 30.

163 *Id.*, S. 30 f., 84; *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1515).

164 *J. D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 36. In diesem Zusammenhang sei erneut darauf hingewiesen, dass Indizien nur für den Nachweis von Kenntnis und damit zur Begründung positiver Handlungspflichten ausreichen können.

165 Vgl. *C. Walter*, der für den Nachweis eines völkerrechtswidrigen bewaffneten Angriffs „full proof" fordert (bezugnehmend auf IGH, Oil Platforms (Islamic

Kontrolle der beklagten Seite unterliegen, ist ein Rückgriff auf Indizien zur Begründung staatlicher Einstandspflichten für völkerrechtmäßige Aktivitäten zulässig, sofern die Indizien nicht der verfügbaren direkten Beweis- und Faktenlage widersprechen.[166] Informationen über die staatliche Beziehung zu einer bestimmten Informationsoperation unterliegen in der Regel dem Ursprungsstaat, der aus Gründen der nationalen Sicherheit nicht bereit sein wird, diese Informationen zu teilen und auch nicht dazu verpflichtet ist.[167] Demnach müssen kontextbezogene Vermutungen ausreichen, so dass eben die Vorteile von pseudostaatlichen Informationsoperationen für einen Staat, die staatliche Befürwortung der Informationsoperationen indizieren,[168] mithin zur Begründung einer staatlichen Einstandspflicht beitragen.

b) Subsidiäre und ergänzende Haftung des Ursprungsstaates für nichtstaatliche Informationsoperationen

Im Rahmen nicht-staatlicher Informationsoperationen sind Aspekte der Risikozuweisung wegweisend, um die Art der staatlichen Haftung festzulegen. Der nicht-staatliche Urheber der Informationsoperation kann aufgrund der Hürden bei der Beweisführung in der virtuellen Welt nur selten zur Rechenschaft gezogen werden, während die privaten Betreiber bzw. Eigentümer informationstechnischer Systeme in Anbetracht der besonders unsicheren Gefährdungslage und den potenziell katastrophalen Auswir-

---

Republic of Iran v. United States of America), Judgment of 6 November 2013, ICJ Reports 2003, S. 161 (161 Rn. 57 ff.)) und in Bezug auf Aufklärungs- und Informationspflichten feststellt, dass „the standard of proof is lower" (bezugnehmend auf IGH, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ Reports 1949, S. 4 (18)). *C. Walter*, Obligations of States Before, During, and After a Cyber Security Incident, GYIL 58 (2015), S. 67 (82).

166 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (638 f. Fn. 324) bezugnehmend auf die Rechtsprechung des IGH.

167 *Id.*, S. 565 (638).

168 Vgl. *D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 30 ff.; *P. Pernik*, A Playbook for Hybrid War in Cyberspace?, International Center for Defence and Security, 29 August 2014, abrufbar unter: https://icds.ee/a-playbook-for-hybrid-war-in-cyberspace/ (geprüft am 15.05.2020).

kungen von Informationsoperationen kaum in der Lage sein werden, die Schadenslast zu antizipieren und zu tragen.

Die Möglichkeit von grenzüberschreitenden Schäden durch die Nutzung informationstechnischer Systeme ist vergleichbar mit möglichen Schäden durch den Betrieb von Kernkraftwerken, bei dem eine subsidiäre sowie eine ergänzende staatliche Einstandspflicht des Anlagenstaates greifen.[169] Derartige Einstandspflichten sind auch für informationstechnische Systeme sinnvoll. Mit der Erlaubnis zur Nutzung informationstechnischer Systeme ohne ausreichende Sicherung vor Informationsoperationen schaffen Staaten eine Gefährdungslage und müssen daher eine adäquate und unverzügliche Entschädigung für eine schadensbegründende Nutzung dieser Systeme gewährleisten.[170] Der Staat ist Verursacher im weiteren Sinne.

Die staatliche Regulierungsmacht bei der Nutzung informationstechnischer Systeme weist dem Staat eine zentrale Rolle im Bereich der Haftung für diese Systeme zu.[171] Wenn also Urheber der Informationsoperation oder Betreiber bzw. Eigentümer der informationstechnischen Systeme nicht identifizierbar sind, trifft den Staat eine Ausfallhaftung. Selbst wenn die Verursacher im engeren Sinne feststehen, dürfte der Staat als solventeste Partei mit der besten Möglichkeit zur Stärkung der Sicherheit informationstechnischer Systeme nicht aus seiner Einstandspflicht entlassen werden.[172] Im Gegenteil müssen die Ursprungsstaaten auch dann subsidiär bzw. ergänzend haften, wenn die Verursacher im engeren Sinne die (volle) Schadensumme nicht begleichen können bzw. müssen. Der Staat muss bekannte Urheber oder Betreiber bzw. Eigentümer allerdings soweit möglich in Regress nehmen.[173]

Schließlich sprechen auch Erwägungen der wirtschaftlichen Gerechtigkeit für diesen Ansatz, denn den Staaten erwächst aus der Nutzung informationstechnischer Systeme durch sie selbst aber auch durch ihre

169 Vgl. auch *D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://these s.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 214.

170 Vgl. *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (16).

171 Vgl. *F. O. Vicuña*, der in Bezug auf die Umwelthaftung feststellt: „Given the complexity of many environmental regimes States cannot realistically expect that the whole burden of liability might fall upon private operators or other entities." *F. O. Vicuña*, Responsibility and Liability for Environmental Damage under International Law, GIELR 10 (1998), S. 279 (287).

172 *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1515).

173 *C. Foster*, The ILC Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities, RECIEL 14 (2005), S. 265 (277); *N. de Sadeleer*, Environmental Principles, 2002, S. 24 f.

Staatsangehörigen ein nicht unerheblicher wirtschaftlicher Vorteil.[174] Die Schaffung von Risiken durch die Genehmigung gefährlicher Aktivitäten und daraus resultierende grenzüberschreitende Schäden gehen dann auf internationaler Ebene mit der Enteignung von Gleichheit und Souveränität einher. Daher lässt sich die staatliche Einstandspflicht auch mit dem Grundsatz der ungerechtfertigten Bereicherung erklären.[175]

c) Errichtung eines Entschädigungsfonds für eine subsidiäre Haftung bei nicht feststellbarem Ursprung der Informationsoperation und für eine ergänzende Haftung bei begrenzter Einstandspflicht des Ursprungsstaates

Die Hauptprobleme bei Einstandspflichten für Schäden durch (hoch-)gefährliche Aktivitäten werden im Haftungsrecht durch die Errichtung von Fonds gelöst. Entschädigungsfonds sind in erster Linie dazu gedacht, denjenigen, die Schäden durch Unfälle oder durch bestimmte nicht verbotene Aktivitäten erlitten haben, unverzügliche und angemessene Abhilfe zu gewähren.[176] Fonds ermöglichen dabei eine bessere Ausreichung größerer Entschädigungssummen und bieten Lösungen für Aufklärungsschwierigkeiten.[177] Die kollektiv organisierten Finanzmittel können zum einen eine individuelle Entschädigungspflicht ergänzen und auf diese Weise Risiken absichern, die nicht mehr vom Haftungsadressaten getragen werden können oder müssen. Zum anderen können kollektive Entschädigungsmechanismen vollständig individuelle Entschädigungssysteme ersetzen und

174 *D. Jolley*, Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law, 2017, abrufbar unter: http://theses.gla.ac.uk/id/eprint/8452 (geprüft am 15.05.2020), S. 214.

175 So kommt *L. F. E. Goldie* anhand der Analyse von Haftungskonzepten zu dem Ergebnis, dass „the creation of risk involves an expropriation of equal rights of amenities and, in the international arena, of equality and sovereign autonomy. This international law thesis of expropriation, moreover, is measured in terms of the application, in international relations, of the equitable doctrine of unjust enrichment." *L. F. E. Goldie*, Concepts of Strict and Absolute Liability and the Ranking of Liability in terms of Relative Exposure to Risk, NYIL 16 (1985), S. 175 (248).

176 *A. Douhan*, Liability for Environmental Damage, in: R. Wolfrum (Hg.), MPEPIL 2013, http://www.mpepil.com, Rn. 34; *C. Kojima*, Compensation Fund, in: R. Wolfrum (Hg.), MPEPIL 2009, http://www.mpepil.com, Rn. 1.

177 *C. Kojima*, Compensation Fund, in: R. Wolfrum (Hg.), MPEPIL 2009, http://www.mpepil.com, Rn. 3.

damit insbesondere bei unsicheren Verursachungszusammenhängen zum Einsatz kommen.[178] So übernehmen Fonds die finanzielle Entschädigung im Fall von Nachweisproblemen, etwa bei Unmöglichkeit der Identifizierung des konkreten Verursachers, bei einer Vielzahl potenzieller Verursacher, bei Synergieschäden oder bei unbestimmter Schadensursache.[179]

Während auf dem Gebiet der Kernenergie Schadensausmaße, die nicht mehr vom Betreiber des Kernkraftwerkes oder dem Anlagenstaat zu tragen sind, durch kollektive Finanzierungssysteme nach dem BZÜ und ÜEE kompensiert werden,[180] kommt der Internationale Entschädigungsfonds für Ölverschmutzungsschäden auch dann zum Einsatz, wenn der Verursacher nicht identifiziert werden kann und begründet mithin eine kollektive Ausfallhaftung.[181] Ebenso sehen das HNS-Übereinkommen 2010[182] und Anlage VI des Antarktisumweltschutzprotokolls über die Haftung bei umweltgefährdenden Notfällen[183] Entschädigungsfonds vor, die auch greifen sollen, wenn die Identität des Verursachers unklar ist. Bemerkenswert sind auch die entsprechenden Bestrebungen auf Ebene der EU zur Errichtung eines Entschädigungsfonds für Umweltschäden durch industrielle Unfälle, der bei Insolvenzrisiko und Versagen der Märkte für Deckungsvorsorge sowie bei Unbekanntheit des verantwortlichen Betreibers greifen soll.[184] Schließlich ist der Vorschlag der Kammer für Meeresbodenstreitigkeiten, die Einrichtung eines Treuhandfonds zur Schadensdeckung in Betracht zu ziehen, um den aufgezeigten Haftungslücken zu begegnen, nicht außer Acht zu lassen.[185]

Wie gezeigt, bestehen insbesondere bei Informationsoperationen aufgrund der komplexen technischen Verursachungsstrukturen und des nur selten hinreichend bestimmbaren Ursprungs der Operationen Nachweisprobleme. Zudem ist die Kompensationspflicht von bestimmbaren Ursprungsstaaten für nicht-staatliche Informationsoperationen dahingehend begrenzt, dass sich deren Ausmaß nach der Beachtung der gebotenen

178 Siehe 1. Kapitel D.
179 Art. 12 IDI-Resolution; *C. Kojima*, Compensation Fund, in: R. Wolfrum (Hg.), MPEPIL 2009, http://www.mpepil.com, Rn. 3; *U. Ranke*, Klima und Umweltpolitik, 2019, S. 102.
180 Siehe Ausführungen im 1. Kapitel D. II. 2.
181 Siehe Ausführungen im 1. Kapitel D. IV. 3. c).
182 Siehe Ausführungen im 1. Kapitel D. IV. 3. c).
183 Siehe Ausführungen im 1. Kapitel D. III. 2.
184 Siehe Ausführungen im 1. Kapitel D. IV. 3. c).
185 Siehe Ausführungen im 1. Kapitel B. I. 3. a).

Sorgfalt bei der Schadensvermeidung bemisst.[186] Darüber hinausgehende Schäden dürfen aber nicht auf das Opfer abgewälzt werden. Folglich ist für informationstechnische Systeme ebenso ein Entschädigungsfonds einzurichten, der bei Schäden greift, deren Ursprung nicht nachweisbar ist oder die ein Ausmaß erreichen, das von einzelnen Staaten nicht aufgefangen werden kann bzw. muss.[187]

Neben dem Aspekt des Opferschutzes spielen Erwägungen der (wirtschaftlichen) Gerechtigkeit und der Risikozuweisung eine wesentliche Rolle.[188] Alle Staaten können nicht nur Opfer von Informationsoperationen werden, sondern profitieren ebenso von vernetzten informationstechnischen Systemen. So besteht ein grundsätzliches Eigeninteresse aller Staaten am Zugriff auf (vernetzte) Informationstechnologie, etwa für die nationale Sicherheit. Nicht ohne Grund werden Anbieter derartiger Technologien von Staaten aufgefordert, ihre Verschlüsselungsmethoden entsprechend abzuschwächen,[189] was im Umkehrschluss zu einer gesteigerten Gefährdung für die internationale Sicherheit führt. In Anbetracht der Tatsache, dass die Technisierung und Vernetzung informationstechnischer Systeme immer weiter voranschreitet und damit die Abhängigkeit von informationstechnisch-gestützten Strukturen weltweit steigt, müssen auch entsprechend stärkere negative Auswirkungen aufgefangen werden, und zwar von der Staatengemeinschaft, die von diesen global verbundenen Systemen profitiert. Der Gerechtigkeitsgedanke gebietet mithin, dass Staaten für die informationstechnische Gefährdungslage einen Entschädigungsfonds zur Ausreichung von Entschädigungssummen einrichten.[190]

---

186 Vgl. 1. Kapitel A. II. 1. c) und 1. Kapitel D. IV. 2.

187 Vgl. *J. Kulesza*, Due Diligence in Cyberspace, in: I. M. Portela/F. Almeida (Hg.), Cyberspace, Organizational, Legal, and Technological Dimensions of Information System Administration, 2014, S. 76 (84 f.).

188 Vgl. 1. Kapitel E. III.

189 In einem gemeinsamen Statement „ermutigen" die USA, Großbritannien, Kanada, Australien und Neuseeland die Anbieter von Informations- und Kommunikationstechnologie, „freiwillig rechtmäßige Zugangswege zu ihren Produkten und Diensten einzurichten". Five Country Ministerial and Quintet Meeting of Attorneys General, Statement of Principles on Access to Evidence and Encryption, Australia 2018, abrufbar unter: https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf (geprüft am 15.05.2020).

190 Vgl. *S. Sucharitkul*, Responsibility and Liability for Environmental Damage Under International Law, Golden Gate University Law Digital Commons 664 (1996), abrufbar unter: https://digitalcommons.law.ggu.edu/pubs/664 (geprüft am 15.05.2020), S. 12.

Darüber hinaus ist der eigene Risikobeitrag, den die Staaten durch die Erlaubniserteilung zum Betrieb der informationstechnischen Systeme oder zu deren Nutzung selbst leisten, zu berücksichtigen. Damit besteht nämlich eine Verantwortungsnähe zu Schäden durch die Risikorealisierung in Gestalt von Informationsoperationen. Wie im Umweltvölkerrecht auch, ist der Verursachergrundsatz aufgrund dieser besonderen Nähe im Sinne einer Gruppenverantwortlichkeit zu verstehen.[191] Die logische Konsequenz ist die Errichtung eines Fonds, um der Haftung für die weltweit vernetzten informationstechnischen Systeme gerecht zu werden.[192] Es geht dabei allerdings nicht um Freiwilligkeit, sondern um eine Pflicht der Staatengemeinschaft – als Verursachergruppe.

Anreize zur Errichtung eines Entschädigungsfonds werden durch die dem internationalen Umweltschutz inhärenten Kooperations- und Solidaritätsgedanken geboten, die im Bereich informationstechnischer Systeme entsprechende Wirkung entfalten können.[193] Wie gezeigt, ist Kooperation für die Grundsätze der Schadensvorsorge, Schadensprävention und Schadensminderung essenziell.[194] Sie fordert von Staaten, finanzielle Mittel bereitzustellen, um Technologien, Warnsysteme und sonstige Kapazitäten zur Schadensvermeidung aufzubauen und zu teilen, aber auch Schäden aufzufangen.[195] Diese Maßnahmen zur Schadensvermeidung und Schadensabhilfe können effektiv durch Fonds verwirklicht werden.[196] Entschädigungsfonds bestehen zumeist aus solidarischen Beiträgen bestimmter Verursachergruppen.[197] Wenngleich die Solidarität keine völkerrechtlich festgelegte Rechtspflicht darstellt, prägt sie das Verhalten der Staatenge-

191 Vgl. *W. Kahl*, Umweltprinzip und Gemeinschaftsrecht, 1993, S. 24 f.; *M. Schröder*, Umweltschutz als Gemeinschaftsziel und Grundsätze des Umweltschutzes, in: H.-W. Rengeling (Hg.), Handbuch zum europäischen und deutschen Umweltrecht, Band I, 2003, § 9, Rn. 42.

192 Vgl. *C. Calliess,* Art. 191 AEUV (ex-Art. 174 EGV), in: ders./M. Ruffert (Hg.), EUV/AEUV, Kommentar, 2016, Rn. 38 (39).

193 Vgl. *O. Kimminich*, Völkerrechtliche Haftung für das Handeln Privater im Bereich des internationalen Umweltschutzes, AVR 22 (1984), S. 241 (266); *W. Rudolf*, Haftung für rechtmäßiges Verhalten im Völkerrecht, in: J. Damrau (Hg.), Festschrift für Otto Mühl, 1981, S. 535 (549 f.).

194 Siehe insbesondere 1. Kapitel E. II. und 2. Kapitel B. II.

195 Vgl. *I. Bantekas*, Trust Funds, in: R. Wolfrum (Hg.), MPEPIL 2010, http://www.mpepil.com Rn. 6; *O. Gross,* Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (495 f.); *U. Ranke*, Klima und Umweltpolitik, 2019, S. 102.

196 *C. Kojima*, Compensation Fund, in: R. Wolfrum (Hg.), MPEPIL 2009, http://www.mpepil.com, Rn. 23.

197 *M. Bothe/L. Gündling/R. Hofmann/C. Rumpf*, Neuere Tendenzen des Umweltrechts im internationalen Vergleich, in: Umweltbundesamt (Hg.), Umweltfor-

meinschaft.[198] So motiviert der Solidaritätsgedanke Staaten sehr anschaulich im Bereich der Naturkatastrophen zur Abhilfe in Schadensfällen.[199] Bei genauer Betrachtung handelt es sich dabei jedoch nicht um eine altruistische oder gar intrinsische Motivation. Ähnlich wie Naturkatastrophen sind Sicherheitslücken in informationstechnischen Systemen derzeit – und wohl auch zukünftig – unvermeidbar und können gleichzeitig mehrere Schadensopfer betreffen.[200] Alle Staaten sind von Informationsoperationen bedroht und haben ein Interesse an ausreichenden und verfügbaren Finanzmitteln für den Schadensfall.[201] Bedingt durch die globale Vernetzung von informationstechnischen Systemen entsteht eine diffuse und ubiquitäre Gefährdungslage, von der Staaten weltweit betroffen sind.[202] Diese Gefährdungslage wird dadurch potenziert, dass die Sicherheit informationstechnischer Systeme nur so stark wie das schwächste Glied in den weltweit vernetzten Systemen ist. Sicherheitslücken informationstechnischer Systeme in einem Staat können zu erheblichen negativen Auswirkungen in anderen Staaten führen (*Spillover*-Effekte).[203] Die Digitalisierung aller Gesellschaftsbereiche und die Allgegenwärtigkeit der Vernetzung informationstechnischer Systeme bilden demnach einen sicherheitspolitischen Raum, der nicht nur enorme Vorteile bietet, sondern auch eine globale Gefährdung bedeutet, da nationale Sicherheitsprobleme in der virtuellen Welt schnell zu internationalen Problemen werden können. Entsprechend haben schon 121 Staaten Sicherheitsstrategien für den virtuellen Raum aufgestellt[204] und auch supranationale bzw. zwischenstaatliche Institutionen wie EU und NATO haben entsprechende Vereinbarungen

---

schungsplan des Bundesministers für Umwelt, Naturschutz und Reaktorsicherheit, Berichte des Umweltbundesamtes, Band 2/90, 1990, S. 1 (274).

198 Siehe zur Geltung des Solidaritätsprinzips im Völkerrecht *D. Campanelli*, Principle of Solidarity, in: R. Wolfrum (Hg.), MPEPIL 2011, http://www.mpepil.com; *C. L. Riemer*, Staatengemeinschaftliche Solidarität in der Völkerrechtsordnung, 2003, insbesondere S. 308.

199 *O. Gross*, Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (491, 509 f.).

200 *Id.*, S. 481 (499 f.).

201 *Id.*, S. 481 (497).

202 *M. Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2011, S. 117 f.

203 *O. Gross*, Cyber Responsibility to Protect, Cornell ILJ 48 (2015), S. 481 (493).

204 International Telecommunications Union, National Cybersecurity Strategies Repository, abrufbar unter: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx (geprüft am 15.05.2020).

getroffen.[205] Demnach besteht ein ureigenes Interesse aller Staaten an internationaler Kooperation zum Schutz des sicherheitspolitischen Raums. Eine Entschädigungslösung durch einen Fonds verdeutlicht dabei, in vergleichbarer Weise wie im Bereich der Meere und der Antarktis, die Bedeutung der virtuellen Welt als Gemeinschaftsgut.[206]

Schließlich dürften ökonomische Gesichtspunkte den größten Anreiz für Staaten zur Errichtung eines Fonds bieten. Wie aufgezeigt, droht in zunehmendem Maße die einzelstaatliche Einstandspflicht für Schäden durch informationstechnische Systeme. Zum einen erfordern die möglichen katastrophalen Auswirkungen eine Ausreichung größerer Schadenssummen im Sinne einer Deckungsvorsorge. Zum anderen verändern sich die informationstechnischen Risiken und Schadenszenarien schnell und fortwährend und stehen damit einer umfassenden Versicherbarkeit der Gefährdung entgegen.[207] Dementsprechend werden alle Staaten an einer Kollektivierung des Schadensausgleichs interessiert sein.[208]

Die finanzielle Ausstattung von Entschädigungsfonds erfolgt in der Regel durch Beitragszahlungen von Regierungen oder privaten Industriegruppen, die das Risiko der Schadensverursachung schaffen. Die Beitragsleistungen variieren dabei nach der Höhe des Risikos, welches durch die jeweilige Partei verursacht wird.[209] Bei Anwendung dieses Modells auf einen Fonds für Schäden durch informationstechnische Systeme müsste für eine zwingende staatliche Beitragsleistung ein Zusammenhang zwischen den einzelnen Staaten und der Erhöhung des Risikos durch diese feststellbar sein. Weniger (sicherheits-)technisch entwickelte Staaten schaf-

---

205 NATO, Cyber Defence Pledge, 8 July 2016, abrufbar unter: http://www.nato.int/cps/en/natohq/official_texts_133177.htm (geprüft am 15.05.2020) und European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013, abrufbar unter: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (geprüft am 15.05.2020).

206 Vgl. *C. Kojima*, Compensation Fund, in: R. Wolfrum (Hg.), MPEPIL 2009, http://www.mpepil.com, Rn. 2, 23.

207 Vgl. *C. Wilson/T. Gaidosch/F. Adelmann/A. Morozova*, Cybersecurity Risk Supervision, International Monetary Fund, Monetary and Capital Markets Departmental Paper Series No.19/15, 2019, Annex I.

208 Vgl. *G. Brüggemeier*, Umwelthaftungsrecht, Kritische Justiz 22 (1989), S. 209 (222).

209 *S. Förster*, Internationale Haftungsregeln für schädliche Folgewirkungen gentechnisch veränderter Organismen, 2007, S. 366 f., 370. Siehe auch Ausführungen im 1. Kapitel D. IV. 3. b).

fen durch entsprechende Sicherheitslücken ein erhöhtes Risiko und könnten daher einer größeren Beitragspflicht unterliegen; allerdings profitieren gerade technisierte Staaten von informationstechnischen Systemen, von denen sie zugleich in größerem Umfang abhängig und damit in besonderem Maße für Informationsangriffe anfällig sind. Der spezifische Risikobeitrag eines Staates ist mithin nur schwer zu quantifizieren. Bei Entschädigungsfonds kommt es aber auch auf Gesichtspunkte der Praktikabilität an.[210] Vor diesem Hintergrund kann für einen Entschädigungsfonds für informationstechnische Schadensfälle nur das Bruttosozialprodukt der jeweiligen Staaten maßgeblich für die Beitragshöhe sein.[211]

2. Haftungsstandard

Wie bereits dargelegt, trifft den Staat im Rahmen verschuldensabhängiger Haftungssysteme nur dann eine Kompensationspflicht, wenn dieser die gebotene Sorgfalt außer Acht gelassen hat, während verschuldensunabhängige Haftungssysteme eine Einstandspflicht unabhängig von einem etwaigen Fehlverhalten des haftenden Staates begründen und lediglich das Ausmaß der Kompensationspflicht entsprechend der angewandten Sorgfalt bemessen. Eine verschuldensabhängige Haftung ist sinnvoll, wenn der Ursprungsstaat und der Opferstaat gleichermaßen zur Gefährdungslage beitragen. Staaten erlauben zwar die Nutzung informationstechnischer Systeme und schaffen damit eine Gefahrenquelle. Allerdings ist die konkrete Nutzung in Gestalt einer bestimmten Informationsoperation, die zu grenzüberschreitenden Schäden führt, nicht in gleicher Weise vom Ursprungsstaat und Opferstaat verursacht.[212] In diesem Zusammenhang

---

210 *M. Bothe/L. Gündling/R. Hofmann/C. Rumpf*, Neuere Tendenzen des Umweltrechts im internationalen Vergleich, in: Umweltbundesamt (Hg.), Umweltforschungsplan des Bundesministers für Umwelt, Naturschutz und Reaktorsicherheit, Berichte des Umweltbundesamtes, Band 2/90, 1990, S. 1 (274).

211 Vgl. Art. 12 BZÜ, wonach sich die Beitragshöhe je Vertragsstaat für nukleare Schäden zur Hälfte nach dem Bruttosozialprodukt der jeweiligen Staaten richtet. Alternativ könnten freiwillige Beitragsleistungen zur finanziellen Ausstattung des Fonds in Betracht gezogen werden. Der antarktische Haftungsfonds etwa soll gemäß Art. 12 Abs. 4 Anlage VI durch freiwillige Beiträge von Staaten oder Personen finanziert werden. Vgl. auch Art. 14 Abs. 1 Fondsübereinkommen 1992 und Art. 23 Abs. 1 HNS-Übereinkommen 2010, wonach Staaten die private Beitragspflicht freiwillig übernehmen können.

212 Eine Differenzierung zwischen verschuldensabhängiger Haftung bei nicht-staatlichen Informationsangriffen und verschuldensunabhängiger Haftung bei staat-

spielt außerdem die Verflechtung von Haftungsstandard und Sorgfaltsstandard eine entscheidende Rolle: Zum einen fehlt es insbesondere bei komplexen Vorgängen im Zusammenhang mit modernen risikobehafteten Technologien an festgelegten internationalen Sorgfaltsstandards zur Schadensvermeidung, was nicht zulasten des Staates gehen darf, der weder in ein konkretes Risiko eingewilligt hat oder Kontrolle über die betreffende Aktivität ausüben kann, noch von dieser in irgendeiner Form profitiert. Dies spricht für eine verschuldensunabhängige Haftung.[213] Zum anderen ist der Betrieb informationstechnischer Systeme ohnehin als hochgefährlich zu qualifizieren. Da sich der Sorgfaltsstandard bei hochgefährlichen Aktivitäten grundsätzlich zu einer verschuldensunabhängigen Haftung verdichtet,[214] ist im Ergebnis in jedem Fall ein verschuldensunabhängiges Haftungssystem für informationstechnische Systeme angezeigt, so dass die Beachtung bzw. Missachtung der gebotenen Sorgfalt das Ausmaß der Kompensationspflicht bestimmt.[215]

---

lichen und staatlich geförderten Informationsangriffen – wie sie *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1499 ff.) vornimmt – findet sich nicht in den beleuchteten Völkerrechtsquellen. Diesen zufolge spielt eine Differenzierung nach staatlich und nicht-staatlich vielmehr für die Unterscheidung zwischen originärer, ergänzender und subsidiärer staatlicher Haftung eine Rolle spielt.

213 *A. E. Boyle*, Globalising Environmental Liability, J. Envtl. L. 17 (2005), S. 3 (7).

214 *G. Handl*, State Liability for Accidental Transnational Environmental Damage by Private Persons, AJIL 74 (1980), S. 525 (550).

215 Bei der Staatenhaftung geht es im Gegensatz zur Staatenverantwortlichkeit nicht um die Wiederherstellung des *status quo ante*, sondern um einen gerechten Interessenausgleich, so dass sich die staatliche Kompensationspflicht bei Beachtung der gebotenen Sorgfalt zur Schadensvermeidung gar auf eine Minimalentschädigung reduziert. Nichtsdestotrotz soll das Opfer nicht die Schäden tragen. Als Lösung bieten sich, wie gezeigt, Entschädigungsfonds an, die diese Schadensposten auffangen.