# 3. Kapitel: Staatenverantwortlichkeit für informationstechnische Systeme

Die negativen Auswirkungen von informationstechnischen Vorgängen können staatliche Einstandspflichten, wie sie in Kapitel 2 definiert wurden, notwendig machen. Zunächst müssen die Charakteristika dieser Vorgänge näher beschrieben werden, um sie völkerrechtlich einordnen zu können (A.). Beispiele aus der Vergangenheit verdeutlichen die Dimension der völkerrechtlichen Problemstellung (B.) und belegen zugleich die Schwächen der existenten Regelungsansätze einer Staatenverantwortlichkeit für informationstechnische Systeme. Die Völkerrechtswidrigkeit von Verhalten innerhalb informationstechnischer Systeme ist zunächst anhand vertrauter völkerrechtlicher Bestimmungen zu beurteilen (C.). Da die Handlungen nur dann für das Recht der Staatenverantwortlichkeit relevant sind, wenn ein Staatenbezug hergestellt werden kann, wird sich zeigen, dass im Regelungsfeld informationstechnischer Systeme eine Zurechnung nicht ohne Weiteres möglich ist (D.) und dass zur Begründung von staatlichen Handlungspflichten die konstitutiven Elemente der Kenntnis sowie der realen Handlungsmöglichkeit hohe Hürden darstellen und die gebotene Sorgfalt nur bedingt zur Verhinderung von bzw. zum Schutz vor rechtsverletzenden Handlungen beitragen kann (E.). Die Frage nach einer Schadenskompensation bleibt durch das Recht der Staatenverantwortlichkeit unbeantwortet (F.), so dass das Konzept der Staatenhaftung für informationstechnische Systeme in den Fokus der völkerrechtlichen Reglementierung zu rücken ist.

## *A. Informationsoperationen*

Informationstechnische Systeme bilden eine abgeschlossene Funktionseinheit zur Informationsverarbeitung. Diese Systeme werden durch das universelle und frei zugängliche Internet auf Datenebene miteinander zu einer virtuellen Welt verbunden.[1] Diese Vernetzung bedingt eine globa-

1 Bundesministerium des Innern (Hg.), Cyber-Sicherheitsstrategie für Deutschland, 2016, abrufbar unter: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it

le Gefährdungslage durch sogenannte Informationsoperationen, die zum Ziel haben, fremde informationstechnische Systeme auszuforschen, zu stören, zu verfälschen oder gar zu zerstören, um sich Vorteile zu verschaffen.[2] Aufgrund eines divergierenden Problemverständnisses sowie technischer und juristischer Feinheiten fehlt es derzeit zwar an international gültigen Begrifflichkeiten und Definitionen für die unterschiedlichen Informationsoperationen,[3] ungeachtet dessen erlauben spezifische Merkmale von Vorgängen innerhalb informationstechnischer Systeme eine Kategorisierung in Informationsangriffe und Informationsausbeutung.[4]

## I. Informationsangriffe

Informationsangriffe sind vorsätzliche Handlungen, deren Ziel es ist, ein informationstechnisches System oder ein Netzwerk oder die darauf gespeicherten Daten zu verändern, zu stören, zu manipulieren, zu schwächen, zu beeinträchtigen oder zu zerstören.[5] Dabei sind im Wesentlichen zwei

---

-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html (geprüft am 15.05.2020), S. 46.

2 *D. B. Hollis*, Why States Need an International Law for Information Operations, LCLR 11 (2007), S. 1023 (1030 ff.); *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (1); *T. Theuerkauf*, Informationsoperationen, Europäische Sicherheit 2 (2000), S. 14 (14 ff.). In diesem Zusammenhang wird häufig auch von Cyberkrieg(sführung) und Informationskrieg(sführung) gesprochen. Siehe *S. Gaycken*, Cyberwar, 2011, S. 21 ff.; *W. Heintschel von Heinegg*, Informationskrieg und Völkerrecht, in: V. Epping/H. Fischer/ders. (Hg.), Brücken bauen und begehen, Festschrift für Knut Ipsen, 2000, S. 129 (129 ff.); *T. A. Morth*, Considering Our Position, Case Western Reserve JIL 30 (1998), S. 567 (567 ff.); *D. Ventre*, Cyberwar and Information Warfare, 2011, S. 1 ff. Diese Terminologien weisen aber – im Gegensatz zum Begriff der Informationsoperation – eine Nähe zum Kriegsbegriff auf, so dass ihnen die notwendige Offenheit fehlt, um als Oberbegriff für Handlungen im Rahmen informationstechnischer Systeme dienen zu können.

3 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 8.

4 Vgl. die vom US-Militär entwickelte Terminologie, welche regelmäßig als Grundlage für wissenschaftliche Diskussionen über Informationsoperationen genutzt wird. Joint Chiefs of Staff, Cyberspace Operations, Joint Pub 3–12, 8 June 2018, abrufbar unter: https://fas.org/irp/doddir/dod/jp3_12.pdf (geprüft am 15.05.2020), Kapitel 2, S. 3, 6 f.; vgl. auch *W. A. Owens/K. W. Dam/H. S. Lin* (Hg.), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 2009, S. 1.

5 Joint Chiefs of Staff, Cyberspace Operations, Joint Pub 3–12, 8 June 2018, abrufbar unter: https://fas.org/irp/doddir/dod/jp3_12.pdf (geprüft am 15.05.2020), Glossary,

Angriffsmethoden zu unterscheiden, welche darauf gerichtet sind, die Sicherheit von informationstechnischen Systemen zu brechen.[6] Zum einen kann die Funktionsfähigkeit der Systeme von außen beeinträchtigt oder gänzlich unterbrochen werden und zum anderen können intrusive Angriffe den Abfluss und die Vernichtung von Informationen bewirken sowie Fehlfunktionen mit sekundärer Schadwirkung verursachen.[7]

In den meisten Staaten sind wesentliche Bereiche der Daseinsfürsorge und der staatlichen Infrastruktur an informationstechnische Systeme gebunden, die gegenüber Informationsoperationen äußerst verwundbar sind. So können Netzwerke instrumentalisiert werden, um kritische Infrastrukturen, wie etwa Kommunikations-, Verkehrs- und Energieversorgungssysteme, zu beeinträchtigen oder zu zerstören.[8] Neben staatlichen Netzwerken können auch private Unternehmen und internationale Institutionen betroffen sein. Informationstechnologien sind für das Funktionieren von Wirtschaft und Gesellschaft mittlerweile unentbehrlich. Dementsprechend kann deren Ausfall enorme Schäden verursachen.[9]

Ferner können virtuelle Sabotage und Manipulationen die politische Landschaft und Geschicke eines Staates beeinflussen.[10] So können beispielsweise Wahlergebnisse manipuliert, falsche Informationen verbreitet und das öffentliche Bewusstsein der Bevölkerung eines fremden Staates in eine bestimmte Richtung gelenkt werden. Dies kann zu Unruhen und bis hin zum Umsturz der Regierung eines Landes führen.[11]

---

S. 4; *W. A. Owens/K. W. Dam/H. S. Lin* (Hg.), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 2009, S. 1.

6 Zu den verschiedenen Angriffsmethoden siehe *S. Gaycken*, Cyberwar, 2011, S. 215 ff.

7 *A. Bendiek*, Umstrittene Partnerschaft, SWP-Studie 26/2013, S. 10, Fn. 25; *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (405 f.).

8 *A. Bendiek*, Kritische Infrastrukturen, Cybersicherheit, Datenschutz, SWP-Aktuell 35/2013, S. 2; *N. Melzer*, Cyberwarfare and International Law, 2011, S. 14 f.; *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 18.

9 *A. Bendiek*, Umstrittene Partnerschaft, SWP-Studie 26/2013, S. 10 f.; *J. A. Lewis/S. Baker*, The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, Report of 22 July 2013, abrufbar unter: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf (geprüft am 15.05.2020), S. 3 ff.

10 Vgl. *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (33 f.).

11 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 15.

## II. Informationsausbeutung

Informationsausbeutung zielt weniger auf Destruktion als vielmehr auf Informationsgewinnung ab.[12] Sie hat also das Ausspionieren informationstechnischer Systeme und die Informationsabschöpfung zum Gegenstand und kennt verschiedene Methoden, um die Vertraulichkeit dieser Systeme zu stören.[13] Im Rahmen der Informationsausbeutung kommen oftmals Informationsangriffe zur Informationsbeschaffung zum Einsatz und begründen damit eine zweifache Bedrohung.[14]

Im Kontext zwischenstaatlicher Spionage geht es in der Regel um die Beschaffung als geheim eingestufter oder anderweitig geschützter Informationen, etwa über den Stand und die Entwicklung der Volkswirtschaft eines fremden Staates oder über Militärgeheimnisse.[15] Im Interesse der nationalen Sicherheit werden überdies auch persönliche Informationen über ausländische Personen gesammelt und ausgewertet.[16] Unternehmen oder Einzelpersonen können Gegenstand fremdstaatlicher oder nicht-staatlicher Wirtschaftsspionage sein, die auf private Geschäfts- bzw. Betriebsgeheimnisse abzielt.[17]

Die Informationsausbeutung hat weitreichende negative Auswirkungen. In den Bereichen Forschung und Entwicklung führt sie zu erheblichen volkswirtschaftlichen Schäden. Unternehmen erleiden enorme wirtschaftliche Einbußen in Form von entgangenen Geschäften, wertlosen Ausgaben

12 US Joint Chiefs of Staff, Cyberspace Operations, Joint Pub 3–12, 8 June 2018, abrufbar unter: https://fas.org/irp/doddir/dod/jp3_12.pdf (geprüft am 15.05.2020), Glossary, S. 4; *W. A. Owens/K. W. Dam/H. S. Lin* (Hg.), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 2009, S. 2.

13 *A. Bendiek*, Umstrittene Partnerschaft, SWP-Studie 26/2013, S. 10, Fn. 25; *A. Tsolkas/F. Wimmer*, Wirtschaftsspionage und Intelligence Gathering, 2012, S. 101 ff.

14 Vgl. *A. Bendiek*, Umstrittene Partnerschaft, SWP-Studie 26/2013, S. 12.

15 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (597); *O. A. Hathaway/R. Crootof/P. Levitz/H. Nix/A. Nowlan/W. Perdue/J. Spiegel*, The Law of Cyber-Attack, Cal. LR 100 (2012), S. 817 (829); *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 11.

16 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 13 f.

17 *Id.*, S. 11; *H. W. Többens*, Wirtschaftsspionage und Konkurrenzausspähung in Deutschland, NStZ 10 (2000), S. 505 (505).

für Innovationen sowie Reputationsschäden.[18] Das Ausspionieren von Individuen geht regelmäßig mit Eingriffen in die Privatheit einher.[19]

## B. Informationsoperationen in der internationalen Praxis

Informationstechnische Systeme sind aufgrund der wachsenden globalen Vernetzung und der erhöhten Abhängigkeit von komplexen Technologien besonders anfällig für Informationsoperationen, die vermehrt zu internationalen Konflikten führen.[20] Dabei handelt es sich nicht um ein neuartiges Phänomen. Bereits im Jahr 1982 kam es im Kontext des Kalten Krieges zu einer schadensverursachenden Informationsoperation. Agenten des sowjetischen Geheimdienstes entwendeten eine kanadische Software zur Kontrolle von Gaspipelines. Der US-Geheimdienst wusste von diesem Vorhaben der Sowjetunion und manipulierte in Zusammenarbeit mit dem kanadischen Softwareunternehmen die Software mittels einer Logikbombe, welche schließlich nach ihrem Einsatz in einer sibirischen Pipeline zu einer massiven Gasexplosion führte.[21]

Die unterschiedlichen Erscheinungsformen von Informationsoperationen werden im Folgenden anhand ausgewählter Beispiele illustriert. Dabei sind insbesondere staatliche und staatlich motivierten Informationsoperationen von Interesse, die eine negative grenzüberschreitende Wirkung haben. Informationsoperationen, die auf nicht-staatliche Akteure zurück-

---

18 Siehe *J. Lewis*, The Economic Impact of Cybercrime – No Slowing Down, Center for Strategic and International Studies, Report of 21 February 2018, abrufbar unter: https://www.csis.org/analysis/economic-impact-cybercrime (geprüft am 15.05.2020).

19 Der Begriff der Privatheit wird in diesem Zusammenhang „als Inbegriff der auf der Achtung der Menschenwürde und damit freien (informationellen) Selbstbestimmung des Individuums beruhenden Persönlichkeitsrechte, Schutz von Daten und Privatsphäre des Individuums verstanden". *I. Pernice*, Vom Völkerrecht des Netzes zur Verfassung des Internets, HIIG Discussion Paper Series, Discussion Paper No. 2017–02, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959257 (geprüft am 15.05.2020), S. 1 (6 Fn. 23).

20 Vgl. Bundesministerium des Innern (Hg.), Cyber-Sicherheitsstrategie für Deutschland, 2016, abrufbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (geprüft am 15.05.2020), S. 4 ff.; *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (594 ff.).

21 *S. J. Shackelford/R. B. Andres*, State Responsibility for Cyber Attacks, Geo. JIL 42 (2010–2011), S. 971 (972).

gehen und vornehmlich durch nationales Recht zu sanktionieren sind, werden im Rahmen dieser Arbeit nur am Rande zu erörtern sein.[22]

## I. Informationsangriffe auf Estland und Georgien

Die Gefahr, welche die Ausweitung staatlicher Informationsinfrastrukturen mit sich bringt, zeigt sich am Beispiel der internetgestützten Angriffe auf informationstechnische Systeme in Estland im Jahr 2007 und in Georgien im Jahr 2008. Bei den Angriffen wurden informationstechnische Systeme der Länder mit einer großen Anzahl von Befehlen durch mit einer Schadsoftware infiltrierte Computer überlastet.[23] Infiltrierte Computer (*Bots*) sind von außen fernsteuerbar und können mit anderen Bots weltweit zusammen zum Einsatz kommen (*Botnet*), um eine Überbeanspruchung der Rechenleistung und Netzwerkbandbreite von informationstechnischen Systemen zu bewirken.[24] Derartige sogenannte *Denial of Service*-Angriffe führten auch in Estland und in Georgien zum Absturz wichtiger informationstechnischer Systeme.[25] Daneben manipulierten Hacker durch sogenanntes *Defacement* Webseiten und verbreiteten Inhalte, die den Interessen der estnischen bzw. georgischen Regierung zuwiderliefen.[26]

---

22 Insoweit erfasst das nationale und internationale Strafrecht private Handlungsformen in der virtuellen Welt, wie etwa Identitätsdiebstahl, Phishing, Spams und Computerviren. Der Umgang mit derartigen Straftaten ist auch Gegenstand des Europäischen Übereinkommens über Computerkriminalität vom 23. November 2001 (BGBl. 2008 II. S. 1242, 1243; 2010 II S. 218).

23 *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (401 f.); *S. J. Shackelford*, From Nuclear War to Net War, BJIL 27 (2009), S. 192 (207).

24 *C. Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, US Congressional Research Report of 29 January 2008, No RL32114, abrufbar unter: https://fas.org/sgp/crs/terror/RL32114.pdf (geprüft am 15.05.2020), S. 5.

25 *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (401 f.); *S. J. Shackelford*, From Nuclear War to Net War, BJIL 27 (2009), S. 192 (207). Sofern mehrere Systeme betroffen sind, spricht man von Distributed Denial of Service-Angriff. Siehe *S. Gaycken*, Cyberwar, 2011, S. 233.

26 In Estland wurden auf diese Weise pro-russische Parolen verbreitet und in Georgien ersetzten Hacker auf Regierungswebseiten Bilder des Staatspräsidenten Mikheil Saakashvili durch Bilder von Adolf Hitler. *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (401 f.).

In Estland wurden im Jahr 2007 informationstechnische Systeme von Regierungs- und Verwaltungsstellen, der größten estnischen Bank sowie von wichtigen Nachrichtenportalen außer Dienst gestellt. Außerdem kam es zu negativen Auswirkungen auf Krankenhäuser, Energieversorgungssysteme und Notrufnummern. Um weitere Schäden zu vermeiden, sahen sich zahlreiche Serverbetreiber gezwungen, die Verbindung zu externen Netzwerken zu unterbrechen, so dass Estland von der Außenwelt abgeschottet war. In Anbetracht der Tatsache, dass Estland bereits 2007 zu den höchst technisierten Ländern weltweit zählte und alle wesentlichen Verwaltungsangelegenheiten und Vorgänge des öffentlichen Lebens über die gut ausgebaute elektronische Verwaltung des Landes liefen, waren die Auswirkungen der Angriffe umso einschneidender.[27] Die Angriffe starteten einen Tag nach Verlegung der Statue eines Soldaten der Roten Armee von einem zentralen Platz in der Hauptstadt Tallinn auf den Militärfriedhof am Stadtrand. Die Entscheidung der estnischen Regierung über die Verlegung erzeugte Unmut bei der russischen Minderheit in Estland sowie bei außerhalb Estlands lebenden Russen, weil die Statue den Sieg der Sowjetunion im Zweiten Weltkrieg symbolisiert und ihrer gefallenen Opfer gedenkt. Dies verstärkte die Spannungen zwischen Estland und Russland, die schließlich als Anlass für die Angriffe gewertet werden.[28] Während die estnische Regierung Russland für die Störung der estnischen Informationsinfrastrukturen öffentlich anprangerte, bestritt die russische Regierung aber jegliche Beteiligung an den Angriffen und verortete die Angriffsquelle bei patriotischen Hackern.[29]

Während die Angriffe auf Estland vornehmlich für das gesellschaftliche Leben notwendige Infrastrukturen betrafen, ging es bei den Angriffen auf informationstechnische Systeme in Georgien im Jahr 2008 vor allem darum, die nationalen und internationalen Kommunikations- sowie Infor-

---

27 *S. Herzog*, Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 49 (50 ff.); *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (402); *J. Shackelford*, From Nuclear War to Net War, BJIL 27 (2009), S. 192 (202 f. Fn. 57, 207); *E. Tikk/K. Kadri/L. Vihul*, International Cyber Incidents, 2010, S. 18 ff.

28 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 27 f. Auf russischsprachigen Webseiten fanden sich zudem Aufrufe und Anleitungen, um sich an den Inforationsangriffen gegen Estland zu beteiligen. *E. Tikk/K. Kadri/L. Vihul*, International Cyber Incidents, 2010, S. 18.

29 *S. Herzog*, Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 49 (50 ff.); *J. Shackelford*, From Nuclear War to Net War, BJIL 27 (2009), S. 192 (204 f.); *E. Tikk/K. Kadri/L. Vihul*, International Cyber Incidents, 2010, S. 15 f.

mationskanäle des Landes zu unterbrechen.[30] Diese Beeinträchtigungen waren besonders gewichtig, weil sie zu einem Zeitpunkt eintraten, an dem Georgien in besonderem Maße von diesen Kanälen abhängig war. Die Angriffe standen nämlich im Zusammenhang mit dem politisch-militärischen Konflikt zwischen Russland und Georgien bezüglich des formal zu Georgien gehörenden, aber abtrünnigen Gebiets Südossetien.[31] Die Angriffe auf georgische Informationsinfrastrukturen starteten vor einer diesbezüglichen Militärintervention Russlands gegen Georgien und nahmen während deren Verlauf immer weitreichendere und komplexere Ausmaße an.[32] Georgien wurde mithin die Möglichkeit genommen, die eigene Bevölkerung über den Konflikt zu informieren und international hierzu Stellung zu beziehen.[33] Die Urheber der gut koordinierten Angriffe konnten nicht zweifelsfrei bestimmt und lokalisiert werden.[34] Auch hier bestritt die russische Regierung jegliche Beteiligung unter dem Hinweis auf patriotische Hacker. Dieses Argumentationsmuster wird in Anbetracht des zeitlichen Verlaufs, der Komplexität und der Koordinierung der Angriffe auf die staatlichen und zivilen Informationsinfrastrukturen allerdings als fragwürdig bewertet.[35]

---

30 *E. Tikk/K. Kaska/K. Rünnimeri/M. Kert/A.-M. Talihärm/L. Vihul*, Cyber Attacks Against Georgia, 2008, S. 15 f.

31 *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (402 mit Fn. 15); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 28; *E. Tikk/K. Kaska/K. Rünnimeri/M. Kert/A.-M. Talihärm/L. Vihul*, Cyber Attacks Against Georgia, 2008, S. 4.

32 *E. Tikk/K. Kaska/K. Rünnimeri/M. Kert/A.-M. Talihärm/L. Vihul*, Cyber Attacks Against Georgia, 2008, S. 4.

33 *W. C. Ashmore*, Impact of Alleged Russian Cyber Attacks, BSDR 11 (2009), S. 4 (10); *D. Hollis*, Cyberwar Case Study: Georgia 2008, Small Wars Journal (2011), abrufbar unter: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (geprüft am 15.05.2020), S. 1 (6); *E. Tikk/K. Kaska/K. Rünnimeri/M. Kert/A.-M. Talihärm/L. Vihul*, Cyber Attacks Against Georgia, 2008, S. 16.

34 Ähnlich wie bei den Angriffen gegen Estland wurden auf russischsprachigen Webseiten Aufrufe und Anleitungen zur Beteiligung an den Inforationsangriffen gegen Georgien verbreitet. *W. C. Ashmore*, Impact of Alleged Russian Cyber Attacks, BSDR 11 (2009), S. 4 (26); *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (402 f.).

35 *E. Tikk/K. Kaska/K. Rünnimeri/M. Kert/A.-M. Talihärm/L. Vihul*, Cyber Attacks Against Georgia, 2008, S. 12 ff.

## II. Informationsangriff durch Schadprogramm „Stuxnet“

Das Risiko, das informationstechnischen Systemen immanent ist, wurde in besonderem Maße durch das Schadprogramm *Stuxnet* deutlich, welches im Jahr 2009 über verseuchte USB-Speichersticks in Steuerungssysteme iranischer Atomanlagen eindrang und diese umprogrammierte. *Stuxnet* nutzte bis zu diesem Zeitpunkt unbekannte Sicherheitslücken des Betriebssystems der Anlagen, um die Rotationsfrequenz der Nuklearzentrifugen zu verändern und gleichzeitig die Kontrollsysteme mit falschen Messwerten zu überlisten. So blieb das Umprogrammieren zunächst unentdeckt und führte schließlich zur physischen Zerstörung der Zentrifugen.[36]

Die eingehenden Kenntnisse über die Zielsysteme, das Angriffsziel selbst und die umfassende technische Expertise, die *Stuxnet* zugrunde lag, deuteten auf einen staatlichen Akteur hin.[37] Zudem erklärten Vertreter der US-Administration, dass *Stuxnet* durch die USA in Zusammenarbeit mit Israel eingesetzt wurde, mit dem Ziel iranische Atomanlagen zu manipulieren und die dortige Urananreicherung zu sabotieren.[38] Die israelische und die US-amerikanische Regierung selbst hingegen bestreiten, in die weitreichende Umsetzung des Angriffs involviert gewesen zu sein,[39] und auch die iranische Regierung hat trotz der eindeutigen Hinweise keinen Staat völkerrechtlich zur Verantwortung gezogen.[40]

---

36 *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (403 f.); *R. Langner*, Der Langner-Report: Stuxnet und Die Folgen, Was die Schöpfer von Stuxnet erreichen wollten, was sie erreicht haben, und was das für uns alle bedeutet, 2017, abrufbar unter: https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf (geprüft am 15.05.2020).

37 Vgl. *S. Gaycken*, Cyberwar, 2011, S. 175; *M. Schulze*, Hacking back? Technische und politische Implikationen digitaler Gegenschläge, SWP-Aktuell 59/2017, S. 3; *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 17.

38 Siehe *D. E. Sanger*, Obama Ordered Sped Up Wave of Cyberattacks Against Iran, The New York Times, 1 June 2012, abrufbar unter: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (geprüft am 15.05.2020).

39 *S. P. McGurk*, (Acting Director, National Cybersecurity and Communications Integration Center, Office of Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security), Statement for the Record Before the United States Senate Homeland Security and Governmental Affairs Committee, Washington DC, 17 November 2010, abrufbar unter: http://www.hsgac.senate.gov/download/2010–11–17-mcgurk-testimony-revised (geprüft am 15.05.2020).

40 *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (638).

## III. Informationsausbeutung durch Schadprogramme „Duqu“ und „Flame“

Im Jahr 2011 wurde das Schadprogramm *Duqu* und im Jahr 2012 das Schadprogramm *Flame* entdeckt. Die Programme waren auf das Sammeln und Löschen großer Mengen von Informationen spezialisiert.[41] *Duqu* und *Flame* sind vom Arbeitsaufwand und der dahinterstehenden Intelligenz mit *Stuxnet* vergleichbar. Doch im Gegensatz zu Letzterem zielten die beiden Programme nicht darauf ab, bestimmte Prozesse zu manipulieren und physischen Schaden zu verursachen, sondern wurden eingesetzt, um informationstechnische Systeme staatlicher Behörden, Unternehmen und Industrieanlagen abzuhören und auszuspionieren.[42] Entweder sollten die Informationsausbeutungen Schwachstellen in den befallenen Systemen identifizieren, um später für Informationsangriffe genutzt zu werden oder sie zielten lediglich auf die Stärkung wirtschaftlicher Wettbewerbsfähigkeit.[43]

Während *Flame* lokal auf den Nahen Osten ausgerichtet war und insbesondere Computer im Iran befiel, ließen sich bei *Duqu* keine geografischen Präferenzen erkennen.[44] Codeanalysen zeigen, dass *Duqu* und *Flame* wohl derselben Quelle wie *Stuxnet* entstammen.[45] Auch das Entwicklungsniveau der Programme und die Angriffsziele deuten darauf hin, dass staatliche Akteure, etwa Geheimdienste der USA und Israel, für die Entwicklung

---

41 *B. Bencsáth/G. Pék/L. Buttyán/M. Félegyházi*, The Cousins of Stuxnet: Duqu, Flame, and Gauss, Future Internet 4 (2012), S. 971 (971).

42 *Id.*, S. 979 f.

43 *David P. Fidler*, Tinker, Tailor, Soldier, Duqu, IJCIP *5* (2012), S. 28 (28); *M. Hauck/J. Kuhn*, Computervirus Duqu entdeckt, Wie gefährlich ist der Stuxnet-Bruder?, Süddeutsche Zeitung, 19. Oktober 2011, abrufbar unter: https://www.sueddeutsche.de/digital/computervirus-duqu-entdeckt-wie-gefaehrlich-ist-der-stuxnet-bruder-1.1168324 (geprüft am 15.05.2020).

44 *M. Hauck/J. Kuhn*, Computervirus Duqu entdeckt, Wie gefährlich ist der Stuxnet-Bruder?, Süddeutsche Zeitung, 19. Oktober 2011, abrufbar unter: https://www.sueddeutsche.de/digital/computervirus-duqu-entdeckt-wie-gefaehrlich-ist-der-stuxnet-bruder-1.1168324 (geprüft am 15.05.2020); *D. McElroy/C. Williams*, Flame: world's most complex computer virus exposed, The Telegraph, 28 May 2012, abrufbar unter: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html (geprüft am 15.05.2020).

45 *B. Bencsáth/G. Pék/L. Buttyán/M. Félegyházi*, The Cousins of Stuxnet: Duqu, Flame, and Gauss, Future Internet 4 (2012), S. 971 (971); *A. Gostev*, Cyber weapons, Kaspersky Security Bulletin 2012, abrufbar unter: https://securelist.com/kaspersky-security-bulletin-2012-cyber-weapons/36762/ (geprüft am 15.05.2020).

und den Einsatz der Programme verantwortlich sind.[46] Diese Mutmaßungen genügten aber nicht, um völkerrechtliche Reaktionen der betroffenen Länder auszulösen.[47]

## IV. Informationsausbeutung durch Geheimdienste „Five Eyes"

Staatliche Nachrichtendienste sind in immer größerem Umfang damit beschäftigt, private Daten von Politikern und anderen Bürgern im In- und Ausland auszuspähen, indem sie die Telekommunikation, den E-Mail-Verkehr und die Internetaktivitäten systematisch überwachen. Die Informationsgewinnung steht im fundamentalen Widerspruch zum Recht auf Privatheit.[48]

Im Jahr 2013 begannen der britische Guardian und die amerikanische Washington Post, geheime Dokumente zu veröffentlichen, die sie vom früheren Mitarbeiter des amerikanischen Geheimdienstes der National Security Agency (NSA), Edward Snowden, bekommen hatten. Diese Dokumente enthüllten ein weltweites Netz von Spionagesystemen der NSA und deren engster Partner, den Nachrichtendiensten Großbritanniens, Neuseelands, Kanadas und Australiens – den sogenannten *Five Eyes*. Eine unzählige Liste an Schadprogrammen, wie beispielsweise *PRISM*, *Tempora* und *Boundless Informant*, wurden eingesetzt, um private Kommunikation abzuhören, aber auch Regierungsstellen, insbesondere von Mitgliedstaaten der Europäischen Union und ihren Institutionen, auszuspionieren.[49] Dies führte zwar zu politischen Spannungen, allerdings folgten keine völkerrechtlichen Konsequenzen. Im Gegenteil forderten die *Five Eyes* zuletzt in einem gemeinsamen Statement von Anbietern von Informations- und

46 *D. Weissbrodt*, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minn. JIL 22 (2013), S. 347 (353 f.).

47 *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. 24.

48 *I. Pernice*, Vom Völkerrecht des Netzes zur Verfassung des Internets, HIIG Discussion Paper Series, Discussion Paper No. 2017–02, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959257 (geprüft am 15.05.2020), S. 1 (5 ff.).

49 *Norddeutscher Rundfunk/Das Erste*, "Snowden exklusiv": der Wortlaut des Interviews von NDR Autor Hubert Seipel, 26 Januar 2014, abrufbar unter: https://www.presseportal.de/pm/69086/2648795 (geprüft am 15.05.2020).

Kommunikationstechnologie sogar ihre Verschlüsselungsmethoden derart abzuschwächen, dass ein staatlicher Zugriff möglich wird.[50]

## V. Informationsausbeutung durch Hackergruppe „Guardians of Peace"

Im Jahr 2014 kam es zu einem elektronischen Einbruch in die Server des US-amerikanischen Unternehmens Sony Pictures Entertainment.[51] Eine Gruppe, die sich selbst als *Guardians of Peace* bezeichnete, erbeutete mehrere Terabyte an Daten und veröffentlichte vertrauliche Informationen, wie etwa bis dahin unveröffentlichte Filme, interne E-Mails und Sozialversicherungsnummern von Mitarbeitern. Darüber hinaus wurden alle Daten auf den betroffenen Computern und Servern gelöscht.[52] Hintergrund des Angriffs war der Film „The Interview", in dem es um einen fiktiven Mordanschlag auf den nordkoreanischen Machthaber Kim Jong-Un ging. Die Hackergruppe drohte weitere sensible Daten zu veröffentlichen, sofern die Veröffentlichung des Filmes durch Sony Pictures nicht gestoppt werde.[53] Der Schaden durch die beschädigten Computersysteme, die Einnahmeausfälle und die Veröffentlichung von Betriebsgeheimnissen beläuft sich auf Millionenbeträge.[54]

---

50 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).

51 *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (605 f.); *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (567 f.); *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1462 f.).

52 *D. Robb*, Sony Hack: A Timeline, DEADLINE, 22 December 2014, abrufbar unter: http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501 (geprüft am 15.05.2020).

53 *C. Shoard*, Sony Hack: the plot to kill The Interview – a timeline so far, The Guardian, 18 December 2014, abrufbar unter: http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline (geprüft am 15.05.2020).

54 *L. Brinded*, The Interview tipped to cost Sony Pictures $200m following hack and cancellation, International Business Times, 18 December 2014, abrufbar unter: http://www.ibtimes.co.uk/interview-tipped-cost-sony-pictures-200m-total-followinghack-cancellation-1480157 (geprüft am 15.05.2020); *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (606); *C. Kang*, Sony Pictures Hack cost the movie studio at least $15 million, The Washington Post, 4 February 2015, abrufbar unter: https://www.washingtonpost.com/news/business/wp/2015/02/04/sony-pictures-hack-cost-the-movie-studio-at-least-15-million/?utm_term=.db5b8a3b9915 (geprüft am 15.05.2020).

Die US-Regierung reagierte mit Sanktionen gegen Nordkorea, weil sie das dortige Regime hinter dem Angriff vermutete.[55] Diese Anschuldigung gründete allerdings nicht auf eindeutigen Beweisen. Im Gegenteil fanden sich ebenso Anzeichen dafür, dass es sich um einen Angriff aus den Reihen des Unternehmens selbst handeln könnte.[56]

## VI. Informationsausbeutung und -angriff auf das „Democratic National Committee"

In den Jahren 2015 und 2016 sorgten Zugriffe auf Datenbanken der Dachorganisation der Demokratischen Partei der USA, das *Democratic National Committee* (DNC), für weitreichende Konsequenzen. Die Veröffentlichung der entwendeten vertraulichen Informationen durch Wikileaks und andere Plattformen schädigte die Demokratische Partei mit Blick auf die anstehenden Kongresswahlen und war auch im Zusammenhang mit den Präsidentschaftswahlen von Bedeutung. Daneben sollen US-Wahlsysteme ein Ziel von Informationsangriffen gewesen sein, wobei aber eine erfolgreiche Manipulation dieser Systeme nicht nachgewiesen wurde.[57]

Die US-Geheimdienste bewerteten diese Informationsoperation als Kampagne zur Einflussnahme auf die US-Wahl durch Russland, welche die Erfolgsaussichten der Präsidentschaftskandidatin Hillary Clinton im Rahmen der Präsidentschaftswahl schmälern und Zweifel am demokratischen Wahlprozess der Vereinigten Staaten im Allgemeinen begründen

---

55 U.S. Department of the Treasury, Press Center, Treasury Imposes Sanctions Against the Government of the Democratic People's Republic Of Korea, 2 January 2015, abrufbar unter: https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx (geprüft am 15.05.2020); *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (607 f.).

56 *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (607) m.w.N.; *J. Goldsmith*, The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance, LAWFARE, 19 December 2014, abrufbar unter: https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance (geprüft am 15.05.2020); *K. Zetter*, Critics Say New Evidence Linking North Korea to the Sony Hack Is *Still* Flimsy, WIRED, 8 January 2015, abrufbar unter: http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy (geprüft am 15.05.2020).

57 *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1487 ff.); *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (609 ff.).

sollte.[58] Die US-Regierung erklärte, dass aufgrund des Ausmaßes dieser Bestrebungen nur Russlands ranghöchste Beamte diese Informationsoperation genehmigt haben könnten und reagierte infolgedessen mit Sanktionen gegen Russland und der Ausweisung russischer Diplomaten.[59] Neben den wirtschaftlichen Schäden hatte diese Informationsoperation enorme – wenn auch nicht quantifizierbare – negative politische Auswirkungen.[60]

### C. *Völkerrechtswidrigkeit*

In den vergangenen Jahren diskutierten Völkerrechtler umfassend Rechtsfragen zum Themenkomplex der Informationskriegsführung. Unter der Schirmherrschaft des North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) etwa beschäftigten sich Experten seit 2009 mit völkerrechtlichen Normen, die auf virtuelle Kriegsführung Anwendung finden. Sie erstellten ein entsprechendes Handbuch mit dem Titel „Tallinn Manual on the International Law Applicable to Cyber Warfare" (Tallinn Manual), in dem ausführlich die Anwendung militärischer bzw. bewaffneter Gewalt sowie Aspekte des humanitären Völkerrechts im Zusammenhang mit Informationsoperationen thematisiert werden.[61] Zunehmend werden auch völkerrechtliche Normen, die Informationsoperationen zu Friedenszeiten reglementieren,

---

58 *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (609 ff.); *T. Hamburger/K. Tumulty*, WikiLeaks releases thousands of documents about Clinton and internal deliberations, The Washington Post, 22 July 2016, abrufbar unter: https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/ (geprüft am 15.05.2020); *D. E. Sanger/C. Savage*, U.S. Says Russia Directed Hacks to Influence Elections, The New York Times, 7 October 2016, abrufbar unter: http://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html (geprüft am 15.05.2020).

59 The White House, Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 29 December 2016, abrufbar unter: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (geprüft am 15.05.2020); *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (611 ff.).

60 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (568).

61 *M. N. Schmitt* (Hg.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Groups of Experts at the Invitation of the NATO CCD COE, 2013.

näher beleuchtet. Beispielsweise veröffentlichte das NATO CCD COE eine multidisziplinäre Untersuchung zum Themenkomplex Informationsoperationen unter der Überschrift „Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy“[62] sowie das Folgeprojekt zum Tallinn Manual mit dem Titel „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations“ (Tallinn Manual 2.0)[63]. Diese Handbücher beschreiben Rechte und Pflichten von Staaten im virtuellen Raum, wie sie sich aus speziellen Bereichen des Völkerrechts – etwa dem internationalen Telekommunikationsrecht, Seerecht, Weltraumrecht, Luftfahrtrecht, Gesandtschaftsrecht oder den Menschenrechten – entnehmen lassen.[64] Dabei konzentrieren sich die Werke auf Aspekte der Völkerrechtswidrigkeit von Informationsoperationen. Der Analyse der Völkerrechtler ist gemein, dass sie in der Regel zu dem Ergebnis kommen, im Völkerrecht bestehe mit Blick auf Informationsoperationen eine „Grauzone“[65].

Die Schwierigkeiten bei der völkerrechtlichen Reglementierung von Informationsoperationen verdeutlichen auch die Entwicklungen im Rahmen der Arbeiten der „Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security“ (GGE). Sie wurden von den Vereinten Nationen eingesetzt, um sich mit der Anwendbarkeit völkerrechtlicher Bestimmungen auf den virtuellen Raum und den bestehenden Grenzen auseinanderzusetzen und unterschiedliche Lösungen im zwischenstaatlichen Austausch zu diskutieren.[66] Während die Expertengruppe im Jahr 2013 noch für die Klarstellung gerühmt wurde, dass bestehendes Völkerrecht, allen voran

62 *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013.

63 *M. N. Schmitt* (Hg.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO CCD COE, 2017.

64 Tallinn Manual 2.0, Teil II; *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, Teil II.

65 *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (1 ff.); *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 98. *R. Crootof* weist daraufhin, dass die Grenze zwischen rechtmäßigen und unrechtmäßigen Informationsoperationen zusehends verwischt. *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (620).

66 GV Resolution 66/24 vom 02.12.2011, Rn. 4

die VN-Charta, auch im virtuellen Raum anwendbar ist,[67] konnte sich die Expertengruppe im Jahr 2017 nicht auf einen abschließenden Konsensbericht zu anwendbaren Normen, Regeln und Prinzipien im virtuellen Raum einigen.[68] Diese Zäsur in den multilateralen Bemühungen ist unter anderem dem Umstand geschuldet, dass Informationsoperationen nicht ohne Weiteres in die völkerrechtlichen Verbotskategorien passen. Die dargebotenen Lösungsansätze beschränken sich vornehmlich auf Bestrebungen die „Grauzone" entweder durch eine extensive Interpretation von Voraussetzungen für Völkerrechtsverstöße oder durch die Schaffung neuer Verbotstatbestände einzudämmen.

## I. Informationskrieg und Informationskriegsführung

In Ermangelung spezifischer Regeln für die virtuelle Welt ist die Völkerrechtswidrigkeit von Informationskrieg und Informationskriegsführung anhand der auf konventionelle Angriffe zugeschnittenen Vorgaben der VN-Charta und des humanitären Völkerrechts zu beurteilen.

### 1. Informationsangriff als Gewalt im Sinne der VN-Charta

Zunächst sind die Unsicherheiten bei der Anwendbarkeit der wesentlichen Elemente des Rechts zum Krieg (*ius ad bellum*) auf Informationsoperationen zu rekapitulieren. Die Frage, ob Informationsangriffe die Voraussetzungen des Gewaltbegriffs im Sinne des Art. 2 Abs. 4 VN-Charta erfüllen oder ob diese gar einen das Selbstverteidigungsrecht auslösenden bewaffneten Angriff im Sinne des Art. 51 VN-Charta darstellen, wurde

67 Vgl. GGE, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Doc. A/68/98, S. 8, Rn. 19.

68 United Nations Office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security, Fact Sheet, abrufbar unter: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/07/Information-Security-Fact-Sheet-July2018.pdf (geprüft am 15.05.2020); siehe auch *S. Soesanto/F. D`Incau*, The UN GGE is dead: Time to fall forward, European Council on Foreign Relations, 15 August 2017, abrufbar unter: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance (geprüft am 15.05.2020).

im Schrifttum bereits ausgiebig diskutiert.[69] Die Völkerrechtler sind sich grundsätzlich einig darüber, dass beide Kategorien bewaffnete Gewalt voraussetzen.[70] Damit sind allerdings nicht (mehr) nur herkömmliche (militärische) Waffen, die kinetische Energie freisetzen, gemeint. Mittlerweile werden auch biologische und chemische Waffen unter den Begriff subsumiert, so dass weitergedacht auch Angriffe mittels Informationstechnologie in den Anwendungsbereich der VN-Charta fallen können.[71] Entgegen Stimmen in der Völkerrechtsliteratur, die jegliche Art von Informationsoperation mit destruktiven Absichten und Folgen von gewisser Intensität ausreichen lassen wollen,[72] müssen die Auswirkungen aber auch qualitativ und quantitativ mit denen von kinetischer Gewaltanwendung vergleichbar sein.[73] Eine Vergleichbarkeit ist nur dann gegeben, wenn der Informationsangriff unmittelbar zu physischen Schäden an Menschen oder Sachwerten führt.[74] Wirtschaftlicher oder politscher Zwang fallen hingegen

---

69 Siehe zum Beispiel *H. H. Dinniss*, Cyber Warfare and the Laws of War, 2012, S. 37 ff.; *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (399 ff.); *R. Nguyen*, Navigating *Jus Ad Bellum* in the Age of Cyber Warfare, Cal. LR 101 (2013), S. 1079 (1079 ff.); *M. Roscini*, Cyber Operations and the Use of Force in International Law, 2014, S. 43 ff.; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 95 ff.; *J.-H. Woltag,* Cyber Warfare, 2014, S. 111 ff.

70 *H. H. Dinniss*, Cyber Warfare and the Laws of War, 2012, S. 40 ff.; *M. Roscini*, Cyber Operations and the Use of Force in International Law, 2014, S. 45; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 95; *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (5).

71 Vgl. Tallinn Manual 2.0, Teil III, Allgemeiner Kommentar zu Abschnitt 14, S. 328, Rn. 1; *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (10); *M. N. Schmitt*, Computer Network Attack and the Use of Force in International Law, Col. JTL 37 (1999), S. 885 (916); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 96 f.

72 *W. G. Sharp*, Cyberspace and the Use of Force, 1999, S. 133, 140; *N. Tsagourias*, Cyber-attacks, self-defence and the problem of attribution, JCSL 17 (2012), S. 229 (231).

73 *F. Dittmar*, Angriffe auf Computernetzwerke, 2005, S. 154; *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (406 ff.); *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (10); *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (6 f.).

74 *F. Dittmar*, Angriffe auf Computernetzwerke, 2005, S. 100; *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (10); *M. N. Schmitt*, Computer Network Attack and the Use of Force in International Law, Col. JTL 37 (1999), S. 885 (916 f.); *K. Zemanek*, Armed Attack, in: R. Wolfrum (Hg.), MPEPIL 2013, http://www.mpepil.com, Rn. 13.

nicht unter den Gewaltbegriff.[75] Zudem müssen die Auswirkungen ein gewisse Intensität erreichen;[76] weder unerhebliche Auswirkungen noch eine Abfolge kumulativer Angriffe geringer Intensität reichen in diesem Zusammenhang aus.[77]

Zweifelsfrei können Informationsangriffe zerstörerische Folgen haben, die ebenso gravierend sind wie die Wirkungen konventioneller Angriffe. So können Informationsoperationen in Steuerungs- und Kontrollsystemen kritischer Infrastrukturen, etwa von Chemiefabriken, Atomkraftwerken oder in der Flugsicherung, Funktionsstörungen hervorrufen und auf diese Weise Todesopfer, Verletzte oder erhebliche Sachschäden verursachen.[78] Bei Informationsoperationen fehlt es aber häufig am Kriterium der Unmittelbarkeit, da diese erst in einem gewissen zeitlichen Abstand zum ursächlichen Angriff oder erst zusammen mit weiteren Angriffen zu merklichen Schäden führen.[79] Außerdem sind im Rahmen vieler Informationsoperationen, beispielsweise bei der Störung von Kommunikations- und Informationskanälen oder der Entwendung und/oder Zerstörung von Daten,

---

75 *C. Greenwood*, Self-Defence, in: R. Wolfrum (Hg.), MPEPIL 2011, http://www.mpepil.com, Rn. 9; *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (11).

76 Der IGH hat in seiner *Nicaragua*-Entscheidung einen „scale and effects"-Standard aufgestellt, um zwischen Gewaltanwendung und schwerster Gewaltanwendung zu differenzieren. IGH, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986, S. 14 (101 Rn. 191, 103 Rn. 195). Zur damit einhergehenden Diskussion, ob und inwiefern Art. 2 Abs. 4 VN-Charta einerseits und Art. 51 VN-Charta andererseits unterschiedliche Intensitätsschwellen voraussetzen, siehe Tallinn Manual 2.0, Kommentar zu Regel 69, S. 332 f., Rn. 6 f.; *C. Lotriionte*, Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law, CDR 3, (2018), S. 73 (87 ff.).

77 Vgl. IGH, Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, ICJ Reports 2003, S. 161 (187 Rn. 51, 191 f. Rn. 64); vgl. auch *I. Brownlie*, International Law and the Use of Force by States, 1963, S. 278 f.; *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (10 f.). Nach anderer Auffassung können auch eine Reihe von weniger intensiven Angriffen gegen einen Staat, die denselben Ursprung haben und zusammenhängen, als Gewaltanwendung qualifiziert werden. Tallinn Manual 2.0, Kommentar zu Regel 71, S. 342, Rn. 11; *T. Ruys*, 'Armed Attack' and Article 51 of the UN Charter, 2010, S. 168 f.

78 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 18.

79 *F. Dittmar*, Angriffe auf Computernetzwerke, 2005, S. 156; *S. Gaycken*, Die vielen Plagen des Cyberwar, in: R. Schmidt-Radefeldt/C. Meissler (Hg.), Automatisierung und Digitalisierung des Krieges, 2012, S. 89 (95); *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (11).

keine direkten physischen Auswirkungen gegeben.[80] Gleichwohl kamen die Experten des Tallinn Manual zu dem Ergebnis, dass auch derartige Informationsoperationen unerlaubte Gewalt im Sinne der VN-Charta darstellen können.[81] Allerdings konnten sich die Experten nicht auf eine schlüssige Begriffsbestimmung einigen und stellten lediglich exemplarisch kontextbezogene Kriterien auf, die als Indikatoren für das Überschreiten der Schwelle zur unerlaubten Gewalt dienen.[82] Für die Qualifizierung einer Informationsoperation als Verstoß gegen das Gewaltverbot sprächen der Schweregrad der Auswirkungen, die zeitliche Unmittelbarkeit der Folgen, die direkte Ursächlichkeit der Maßnahme, der Grad des Eindringens in den fremdstaatlichen Bereich, die Messbarkeit der Effekte, ein militärischer Charakter, das Ausmaß staatlicher Beteiligung sowie *prima facie* einschlägige Verbotskategorien.[83] Dieser Kriterienkatalog trägt aber zur Unschärfe des Gewaltbegriffs bei, da dessen Evaluierung im konkreten Einzelfall von der einzelstaatlichen Interpretation abhängig ist.[84] Die Subjektivierung begünstigt ein opportunistisches Begriffsverständnis und führt zur Rechtsunsicherheit.[85] Außerdem birgt eine weite Interpretation des Gewaltbegriffs auch ein entsprechendes Eskalationspotenzial, indem die Voraussetzungen für nach Art. 49 Abs. 1 ASR erlaubte Gegenmaßnah-

80 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 98 f.

81 Tallinn Manual 2.0, Kommentar zu Regel 69, S. 333 ff., Rn. 9 f. So auch *M. N. Schmitt*, demzufolge „[armed attacks] also include those that seriously impair the functionality of critical infrastructure or that otherwise have devastating non-physical effects, such as crippling a State's economic system". *M. N. Schmitt*, Cyber Responses "By The Numbers" in International Law, EJIL:Talk!, 4 August 2015, abrufbar unter: https://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/ (geprüft am 15.05.2020); siehe auch *N. Tsagourias*, Cyber-attacks, self-defence and the problem of attribution, JCSL 17 (2012), S. 229 (231).

82 *M. Benatar*, The Use of Cyber Force, GOJIL 1 (2009), S. 375 (391 f.); *M. Roscini*, Cyber Operations and the Use of Force in International Law, 2014, S. 48; *M. N. Schmitt*, The 'Use of Force' in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 311 (314).

83 Tallinn Manual 2.0, Kommentar zu Regel 69, S. 333 ff., Rn. 8 f. Diese Kriterien basieren auf einem Vorschlag, der von *M. N. Schmitt* schon im Jahr 1999 ausgearbeitet wurde. *M. N. Schmitt*, Computer Network Attack and the Use of Force in International Law, Col. JTL 37 (1999) S. 885 (912 ff.).

84 *M. Benatar*, The Use of Cyber Force, GOJIL 1 (2009), S. 375 (391); *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (409); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 99; *C. Stelter*, Gewaltanwendung unter und neben der UN-Charta, 2007, S. 76.

85 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 99; *C. Stelter*, Gewaltanwendung unter und neben der UN-Charta, 2007, S. 76.

men auf Verletzungen des Gewaltverbotes aus Art. 2 Abs. 4 VN-Charta oder für bewaffnete Gewaltanwendung als Selbstverteidigung nach Art. 51 VN-Charta herabgesetzt werden.[86] Die Experten des Tallinn Manual 2.0 geben in diesem Zusammenhang selbst zu bedenken, dass insbesondere im virtuellen Raum das Risiko überstürzter Vergeltungsmaßnahmen besteht, die wenig Zeit für Überlegungen über mögliche Konsequenzen lassen.[87] Daher sollte an dem konventionellen Begriffsverständnis der Gewaltanwendung festgehalten werden und nur solche Informationsangriffe unter die Kategorie des *ius ad bellum* fallen, die unmittelbar zu Todesopfern, Verletzten oder erheblichen Sachschäden führen.[88]

### 2. Informationsangriff als Angriff im Sinne des humanitären Völkerrechts

Bei der Anwendbarkeit des Rechts im Krieg (*ius in bello*) auf den virtuellen Raum ist der Schutz von Zivilisten und zivilen Objekten während eines bewaffneten Konfliktes diskussionswürdig. Die Schutzvorschriften greifen, wenn die Informationsoperation als Angriff im Sinne des humanitären Völkerrechts zu qualifizieren ist.[89] Auch in diesem Zusammenhang sind zunächst die destruktiven physischen Auswirkungen auf Menschen oder Gegenstände maßgeblich.[90] Zudem suggeriert der Sinn und Zweck des humanitären Völkerrechts, dass es kein Unterschied sein darf, ob eine Informationsinfrastruktur physischen Schaden nimmt oder ob die Funktionalität derselbigen beeinträchtigt wird. Dementsprechend ist auch das Stören

86 Es finden sich unterdessen Stimmen, die nicht nur im Rahmen des Rechts auf Selbstverteidigung nach Art. 51 VN-Charta, sondern auch als Reaktion auf Gewalt im Sinne des Art. 2 Abs. 4 VN-Charta bewaffnete Gewalt als Reaktion völkerrechtlich zulassen wollen. Vgl. Tallinn Manual 2.0, Kommentar zu Regel 22, S. 125 f., Rn. 12.

87 Tallinn Manual 2.0, Kommentar zu Regel 21, S. 117, Rn. 2.

88 So auch *S.-H. Schulze*, der ausführt, dass nach Sinn und Zweck des Gewaltverbotes auch keine weite Interpretation des Gewaltverbotes angezeigt ist, weil betroffene Staaten in diesen Konstellationen, in denen es nicht (unmittelbar) zu Verletzungen oder dem Tod von Menschen kommt und auch keine Sachwerte zerstört werden, nicht unter demselben Handlungsdruck stehen. *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 99.

89 *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (17).

90 *Ibid*.

der Funktionsfähigkeit eines Objektes als Angriff zu werten.[91] Unsicherheiten bestehen allerdings bei der Bestimmung der Intensitätsschwelle, die eine nicht-physische Störung erreichen muss, um als Angriff zu gelten.[92] Entscheidend ist, ob die Störung mehr als eine „Unannehmlichkeit" verursacht.[93] So dürfte das zeitweise Aussetzen der Funktionsfähigkeit einer Informationsinfrastruktur nicht ausreichen, wenn keine physischen Schäden oder Verletzungen dadurch hervorgerufen werden.[94] Diese Vagheit des Angriffsbegriffs führt dazu, dass nicht eindeutig bestimmt werden kann, ob eine Informationsoperation darunter zu subsumieren ist und steht damit einem effektiven Schutz nach dem *ius in bello* entgegen.[95] Anlass für Bedenken bietet zudem die Tatsache, dass der durch das humanitäre Völkerrecht gewährte Schutz ziviler Objekte nicht dahingehend ausgeweitet werden kann, dass auch Daten *per se* unter den Schutzbereich fallen. So sind zwar Daten, die essenziell für das Funktionieren der Gesellschaft sind, zunehmend Zielscheibe von Informationsoperationen, deren Erlangung, Zerstörung, Schädigung oder Verfälschung im Rahmen bewaffneter Konflikte ist aber völkerrechtlich nicht geächtet.[96]

---

91 Tallinn Manual 2.0, Kommentar zu Regel 92, S. 417, Rn. 10; *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (17).

92 *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (18).

93 International Committee of the Red Cross (ICRC), International humanitarian law and the challenges of contemporary armed conflicts, Report on the 32nd International Conference of the Red Cross and Red Crescent (32IC/15/11), 2015, abrufbar unter: http://rcrcconference.org/app//uploads/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf (geprüft am 15.05.2020), S. 42. Das ICRC weist in diesem Zusammenhang zugleich daraufhin, dass der Begriff „Unannehmlichkeit" nicht definiert ist und im humanitären Völkerrecht nicht angewandt wird.

94 Vgl. Tallinn Manual 2.0, Kommentar zu Regel 92, S. 417, Rn. 10.

95 Vgl. *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (18).

96 *Ibid*.

## 3. Informationskrieg und Informationskriegsführung in der internationalen Praxis

Bei dem mehrwöchigen Informationsangriff auf Estland wurden gezielt informationstechnische Systeme von Regierungs- und Unternehmenswebseiten sowie anderer Onlinedienste gestört und es kam zum Zusammenbruch von estnischen Infrastrukturen. Der Angriff hatte, aufgrund des hohen Technisierungsgrades Estlands, zwar weitreichende Folgen für das wirtschaftliche und gesellschaftliche Leben, es kam dadurch aber weder zu Verletzungen oder Tod von Menschen noch zur Zerstörung bedeutender Sachwerte.[97] Eine Vergleichbarkeit mit Waffengewalt ist damit evident zu verneinen, so dass der Angriff nicht unter die völkerrechtliche Kategorie des Informationskrieges zu fassen ist.[98]

Der Informationsangriff im Kontext der militärischen Auseinandersetzung zwischen Russland und Georgien, bei dem staatliche und private informationstechnische Systeme außer Betrieb gesetzt wurden, beeinträchtigte zwar Kommunikations- und Informationskanäle und behinderte mithin Kommando- und Kontrollstrukturen des georgischen Militärs.[99] Gleichwohl erreichten die Auswirkungen nicht die erforderliche Intensität, um mit denjenigen von Waffengewalt vergleichbar zu sein oder als Angriff im Sinne des humanitären Völkerrechts gelten zu können. Daher ist auch in diesem Fall kein Informationskrieg gegeben.[100]

Von den bereits beschriebenen Informationsoperationen liefert einzig der Angriff durch das Schadprogramm *Stuxnet* auf das Überwachungs- und Steuerungssystem iranischer Atomanlagen Anhaltspunkte für Diskussionen darüber, inwiefern der Eingriff in das Industriesystem, die Manipulation von Daten und die Kontrolle über die Rotationsgeschwindigkeit der Zentrifugen der Kategorie des Informationskrieges zuzuordnen sind.[101] Der Fall gilt als Paradebeispiel für die Unsicherheiten, welche die unbe-

---

97 *R. Buchan*, Cyber Attacks, JCSL 17 (2012), S. 212 (219); *K. C. Hinkle*, Countermeasures in the Cyber Context, YIL Online 37 (2011), abrufbar unter: http://www.yjil.org/docs/pub/o-37-hinkle-countermeasures-in-the-cyber-context.pdf (geprüft am 15.05.2020), S. 11 (13 f.).

98 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 123.

99 *A. Hagen*, The Russo-Georgian War 2008, in: J. Healey (Hg.), A Fierce Domain, 2013, S. 194 (194 ff.); *D. Hollis*, Cyberwar Case Study: Georgia 2008, Small Wars Journal (2011), abrufbar unter: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (geprüft am 15.05.2020), S. 1 (6, 8).

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

101 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (591).

stimmten Schwellenvoraussetzungen der kriegsrechtlichen Kategorien in der virtuellen Welt begründen.[102] Die veränderte Rotationsgeschwindigkeit und damit einhergehende Behinderung der iranischen Urananreicherung für sich stellt keine Beschädigung oder Zerstörung von Sachwerten dar und würde für sich genommen aus dem Anwendungsbereich des Informationskrieges fallen. Allerdings führte der Informationsangriff zugleich zur Zerstörung von etwa eintausend Zentrifugen.[103] Diese physischen Auswirkungen überschreiten die Schwelle der Gewalt im Sinne des Art. 2 Abs. 4 VN-Charta.[104] Während zum Teil schon die vom Gewaltverbot geforderte Quantität und Qualität der Schädigung infrage gestellt wird,[105] ist jedenfalls entgegen anderer Auffassung[106] nicht davon auszugehen, dass der Vorfall den geforderten Schweregrad erreicht, um als ein das Selbstverteidigungsrecht auslösender bewaffneter Angriff im Sinne des Art. 51 VN-Charta zu gelten.[107] Auch wenn der Kriegsbegriff dem Wandel der Zeit entsprechend ausgelegt werden muss,[108] können letztlich nur Informationsoperationen, die mit herkömmlichen militärischen Schädigungshandlungen vergleichbar sind, als unerlaubte Gewalt im Sinne der VN-Charta gelten.[109] Einer extensiven Interpretation ist Einhalt zu gebie-

---

102 Tallin Manual 2.0, Kommentar zu Regel 71, S. 342, Rn. 10; *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (638); *D. P. Fidler*, Was Stuxnet an Act of War? Decoding a Cyberattack, IEEE Security and Privacy Magazine 9 (2011), S. 56 (57 ff.).

103 *D. Albright/P. Brannan/C. Walrond*, Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, Institute for Science and International Security Report of 15 February 2011, abrufbar unter: http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf (geprüft am 15.05.2020), S. 1, 3, 6, 8 f.; *S. J. Shackelford,/R. B. Andres*, State Responsibility for Cyber Attacks, Geo. JIL 42 (2010–2011), S. 971 (973).

104 Tallin Manual 2.0, Kommentar zu Regel 71, S. 342, Rn. 10; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 127; *D. Weissbrodt*, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minn. JIL 22 (2013), S. 347 (376 ff.).

105 *J.-C. Woltag*, Computer Network Operations Below the Level of Armed Force, ESIL Conference Paper Series 1 (2011), S. 1 (10).

106 *D. Weissbrodt*, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minn. JIL 22 (2013), S. 347 (378).

107 *C. Lotriont*e, Cyber Operations: Conflict Under International Law, Georgetown Journal of International Affairs, (2012), S. 15 (20); *M. E. O'Connell*, Cyber Security without Cyber War, JCSL 17 (2012), S. 187 (201 f.).

108 Vgl. Tallinn Manual 2.0, Teil III, Allgemeiner Kommentar zu Abschnitt 14, S. 328 f., Rn. 3.

109 Selbst wenn man also auf das Unmittelbarkeitskriterium verzichten wollte, dürfen die Parallelen zu den Auswirkungen konventioneller bewaffneter Angriff

ten, um eine Ausuferung von Gegenmaßnahmen und Gewaltanwendung in der virtuellen Welt zu verhindern.

In den überwiegenden Konstellationen erfüllen Informationsangriffe nicht die bezeichneten Schwellenvoraussetzungen und sind im Ergebnis als militärisch irrelevant einzuordnen.[110] Treffenderweise werden derartige Informationsoperationen auch als „Weapons of Mass Annoyance"[111] oder „Cyberkrawall"[112] bezeichnet.

## II. Informationsintervention

Aus dem Prinzip der souveränen Gleichheit von Staaten ergibt sich das völkergewohnheitsrechtliche Interventionsverbot.[113] Eine Informati-

---

nicht völlig verloren gehen. Maßgeblich ist nach *T. Stein/T. Marauhn* beispielsweise „ob nach der durch Computer bewirkten Störung der Elektronik eines Kernkraftwerkes der Kern durchzuschmelzen droht, ob nach dem Ausfall der Stromversorgung im Winter Menschen zu erfrieren drohen, oder ob die Ausschaltung jeglicher Flugsicherung den Absturz von Passagierflugzeugen zur unvermeidlichen Folge hätte. Das alles hätte auch eine quantitative Komponente; der Ausfall einzelner Beatmungsgeräte in Krankenhäusern würde einen massiven Gegenschlag kaum rechtfertigen." *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (8).

110 Vgl. *S. Gaycken*, Die vielen Plagen des Cyberwar, in: R. Schmidt-Radefeldt/C. Meissler (Hg.), Automatisierung und Digitalisierung des Krieges, 2012, S. 89 (93 ff.); *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (11).

111 *J. A. Lewis*, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, 2002, abrufbar unter: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (geprüft am 15.05.2020), S. 4, (unter Bezugnahme auf *Stewart Baker*).

112 *F. Rötzer*, DDoS-Angriffe auf estnische Server waren kein "Cyberwar", heise online, 12. Juni 2007, abrufbar unter: https://www.heise.de/newsticker/meldung/DDoS-Angriffe-auf-estnische-Server-waren-kein-Cyberwar-138918.html (geprüft am 15.05.2020), (unter Bezugnahme auf *James Hendler*).

113 IGH, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986, S. 14 (106 Rn. 202, 107 f. Rn. 205, 128 Rn. 251); Tallinn Manual 2.0, Kommentar zu Regel 66, S. 312 f., Rn. 1 m.w.N.; *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (409 f.). Bemerkenswert ist unterdessen, dass in dem Eingriff in die freie und unabhängige Ausübung souveräner Rechte gleichzeitig auch der Schaden zu erblicken ist, der damit nicht kausal auf dem schädigenden Verhalten beruht, sondern in dem Verhalten selbst liegt. Siehe hierzu *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. 176 ff.

onsoperation verstößt gegen das Interventionsverbot, wenn sie in die inneren oder äußeren Angelegenheiten (*domaine réservé*) eines anderen Staates eingreift und dabei als Zwang zu qualifizieren ist.[114] Die Unbestimmtheit dieser zwei Voraussetzungen führt zu Unsicherheiten bei der Reglementierung von Informationsoperationen.[115]

### 1. Informationstechnische Systeme als *domaine réservé*

Der *domaine réservé* betrifft nur solche Staatsangelegenheiten, die völkerrechtlich nicht erfasst sind.[116] So überlässt es das Völkerrecht grundsätzlich jedem Staat, über sein politisches, wirtschaftliches, soziales und kulturelles System ohne Einmischung von außen frei zu entscheiden und seine Außenpolitik zu gestalten.[117]

Die wachsenden internationalen Interdependenzen und zunehmenden transnationalen Kooperationen schränken die Bereiche, die der alleinigen Zuständigkeit eines Staates vorbehalten sind, aber immer weiter ein.[118] Gerade mit Blick auf informationstechnische Systeme verwischt die Grenze zwischen völkerrechtlichen und nationalen Angelegenheiten zusehends. Staaten obliegt beispielsweise das alleinige souveräne Recht, die Onlinekommunikation ihres Landes zu reglementieren. Gleichzeitig können aber internationale Regeln zum menschenrechtlichen Schutz der Meinungsfrei-

---

114 Tallinn Manual 2.0, Kommentar zu Regel 66, S. 314, Rn. 6; *P. Kunig*, Prohibition of Intervention, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 3, 5.

115 *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (7).

116 Tallinn Manual 2.0, Kommentar zu Regel 66, S. 314, Rn. 7; *K. S. Ziegler*, Domaine Réservé, in: R. Wolfrum (Hg.), MPEPIL 2013, http://www.mpepil.com, Rn. 1 ff.

117 IGH, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986, S. 14 (107 f. Rn. 205).

118 Tallinn 2.0, Kommentar zu Regel 66, S. 314, Rn. 6; *L. F. Damrosch*, Politics Across Borders, AJIL 83 (1989), S. 1 (10 f.); *K. S. Ziegler*, Domaine Réservé, in: R. Wolfrum (Hg.), MPEPIL 2013, http://www.mpepil.com, Rn. 3, 9 ff.; vgl. auch *R. Hofmann*, Modernes Investitionsschutzrecht, in: S. Kadelbach/K. Günther (Hg.), Recht ohne Staat?, 2011, S. 119 (125).

heit oder Privatsphäre die Interventionsfestigkeit dieses Bereichs durchbrechen.[119]

## 2. Informationsangriff als unerlaubter Zwang

Informationsoperationen, die einen Staat dazu zwingen, sich einem anderen Staat bei der Ausübung seiner souveränen Rechte unterzuordnen, sind als völkerrechtswidrig zu qualifizieren.[120] Das Zwangselement grenzt mithin die völkerrechtswidrige Informationsintervention von der völkerrechtlich nicht verbotenen Informationseinmischung ab.[121] Es fehlt dem Element allerdings an festen Konturen, so dass Fallgruppen aus der Staatenpraxis herangezogen werden, um die völkerrechtliche Qualität einer Informationsoperation zu bewerten.[122]

Zunächst gilt die Androhung oder Anwendung bewaffneter Gewalt (Art. 2 Abs. 4 VN-Charta) als Zwang.[123] Das virtuelle Eindringen in informationstechnische Systeme für sich genommen genügt dabei nicht, da es – auch wenn virtuelle Schutzmechanismen, wie eine Firewall oder Passwortbarrieren, durchbrochen werden – keiner Gewaltandrohung bzw. Gewaltanwendung gleicht.[124] Andererseits soll aber die finanzielle, logistische

---

119 *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (7); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 103 f.

120 *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (409 f.).

121 *I. Kilovaty*, Doxfare, Harv. NSJ 9 (2018), S. 146 (167 ff.); *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (8); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 104.

122 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 105.

123 IGH, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986, S. 14 (107 f. Rn. 205); *P. Kunig*, Prohibition of Intervention, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 5.

124 Tallin Manual 2.0, Kommentar zu Regel 66, S. 323, Rn. 33. Nach anderer Auffassung wird eine Souveränitätsverletzung angenommen, da das virtuelle Eindringen als Ausübung von Hoheitsgewalt und Anmaßung fremder Jurisdiktion zu werten sei. Vgl. *W. Heintschel von Heinegg*, Legal Implications of Territorial

oder ähnliche Unterstützung von Hackergruppen, die schädigende Informationsoperationen ausführen, unerlaubten Zwang darstellen können.[125] Des Weiteren können auch unterhalb der Gewaltschwelle verbleibende Maßnahmen als Zwang gelten. Dazu zählen wirtschaftliche, politische und sonstige Druckmittel, die eine willensbeugende Wirkung entfalten.[126] Im Rahmen von Informationsoperationen stellen sich in diesem Zusammenhang besondere Abgrenzungsschwierigkeiten, weil diese eine ganz neue Vielfalt an nicht-physischen, aber nichtsdestoweniger durchdringenden Mitteln der Einmischung kennen.[127] Während etwa die umsturzorientierte Rundfunk- oder Fernsehpropaganda unerlaubten Zwang darstellen kann, ist das Verbreiten von fundierter Kritik an der Politik eines Landes nicht mehr von dem Begriff erfasst.[128]

### 3. Informationseinmischung als Souveränitätsverletzung

Zur Regulierung von Informationsoperationen, denen es am interventionstypischen Zwangscharakter fehlt, möchten Völkerrechtler eine souveränitätsspezifische Primärnorm gelten lassen.[129] Diese völkerrechtliche

---

Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (11 f.).

125 Tallinn Manual 2.0, Kommentar zu Regel 66, S. 319, Rn. 22, unter Bezugnahme auf IGH, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986, S. 14 (124 Rn. 242).

126 *D. C. Dicke*, Die Intervention mit wirtschaftlichen Mitteln im Völkerrecht, 1978, S. 176 ff., 198 f. m.w.N.; *P. Kunig*, Prohibition of Intervention, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 6.

127 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (625 ff.).

128 *P. Kunig*, Prohibition of Intervention, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 24; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 107 m.w.N.

129 Tallinn Manual 2.0, Regel 4; *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (5). Gegen die Geltung einer Souveränitätsregel sprechen sich etwa *Gary P. Corn* (Staff Judge Advocate of the U.S. Cyber Command) und *Robert Taylor* (former Principal Deputy General Counsel of the U.S. Department of Defense) aus. *G. P. Corn/R. Taylor*, Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0, Sovereignty in the Age of Cyber, AJIL Unbound 111 (2017), S. 207 ff.

Souveränitätsregel sei mit dem Interventionsverbot zwar verwandt, überschneide sich aber nicht vollkommen mit Letzterem.[130] Demnach sollen auch zwangsfreie Informationsoperationen untersagt sein, die auf fremdstaatlichem Territorium ausgeführt werden[131] oder deren Folgen sich dort manifestieren.[132] Dabei muss die Verletzung der fremdstaatlichen territorialen Integrität eine gewisse Intensität erreichen oder einen Eingriff bzw. eine Anmaßung von regierungseigenen Funktionen bedeuten.[133] Zum einen besteht aber keine Einigkeit darüber, unter welchen Bedingungen diese Voraussetzungen erfüllt sein sollen.[134] Zum anderen führt eine derartige Souveränitätsregel dazu, dass Kategorien wie das Gewaltverbot und das Interventionsverbot obsolet werden.[135] Wollte man nämlich neben physischen Auswirkungen auch nicht-physische Auswirkungen, etwa in Gestalt von Funktionsausfällen informationstechnischer Systeme, ausreichen lassen, um eine Informationsoperation als völkerrechtswidrig zu qualifizieren,[136] würde man die speziellen Voraussetzungen des Gewaltverbotes umgehen, und wenn schon jede Form der Einmischung in regierungseigene Funktionen untersagt wäre,[137] hätte es keinen Sinn, speziell Interventionen mittels Zwang zu verbieten. Das Interventionsverbot ist

130 *M. N. Schmitt/L. Vihul*, Respect for Sovereignty in Cyberspace, Tex. LR 95 (2017), S. 1639 (1653 f.).

131 In diesem Sinne wird auch bei Informationsoperationen die physische Anwesenheit auf fremdem Hoheitsgebiet – beispielsweise zu Spionagezwecken – als Verletzung staatlicher Souveränität gewertet. In der weit verbreiteten entsprechenden Spionagepraxis sehen einige Experten einen völkergewohnheitsrechtlichen Ausnahmetatbestand zu diesem völkerrechtlichen Verbotstatbestand. Tallinn Manual 2.0, Kommentar zu Regel 4, S. 19, Rn. 7 f.

132 Tallinn Manual 2.0, Kommentar zu Regel 4, S. 19 f., Rn. 9.

133 Tallinn Manual 2.0, Kommentar zu Regel 4, S. 20, Rn. 10.

134 Tallinn Manual, Kommentar zu Regel 4, S. 20 f. Rn. 13 f.; S. 22 f., Rn. 16 ff.; *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (6 f.).

135 Vgl. *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1475).

136 *W. Heintschel von Heinegg*, Legal Implications of Territorial Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (11 ff.); *C. Joyner/C. Lotriionte*, Information Warfare as International Coercion, EJIL 12 (2001), S. 825 (843 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 (163).

137 Tallinn Manual 2.0, Kommentar zu Regel 4, S. 23, Rn. 19.

bereits Ausfluss staatlicher Souveränität[138] und kann durch dessen Voraussetzungen das Eskalationspotenzial durch mögliche Gegenmaßnahmen auf solche Informationsoperationen eingrenzen.[139] Zudem würde ein zu weites Verständnis den Staaten unrealistische positive Handlungspflichten zur Verhinderung von nicht-staatlichen Souveränitätsverletzungen aufbürden[140] und die Regulierung von Informationsoperationen behindern.[141]

### 4. Informationsintervention in der internationalen Praxis

Die Schwierigkeiten einer Abgrenzung von völkerrechtswidriger Informationsintervention und völkerrechtlich nicht verbotener Informationseinmischung werden am dargestellten Zugriff auf die Server des *DNC* deutlich. Die Informationsoperation betraf nationale politische Prozesse und damit die Ausübung souveräner Rechte, die den jeweiligen Staaten vorbehalten sind. Die Einmischung in den freien Wahlprozess unterläuft das nationale System demokratischer Willensbildung und schadet damit dem Staat und seinem Volk.[142] Nach einem weiten Verständnis von Zwang

---

138 *J. Crawford*, Brownlie's Principles of Public International Law, 2019, S. 431; *P. Kunig*, Prohibition of Intervention, in: R. Wolfrum (Hg.), MPEPIL 2008, http://www.mpepil.com, Rn. 9.

139 Vgl. *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (630 f.); *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1477).

140 Vgl. *E. T. Jensen/S. Watts*, A Cyber Duty of Due Diligence, Tex. LR 95 (2017), S. 1555 (1568 ff.).

141 *W. Banks* gibt gegen die Anerkennung einer derartigen Souveränitätsregel zu bedenken, dass damit von transnationalen terroristischen Informationsangriffen betroffenen Staaten die Möglichkeit genommen wird, völkerrechtmäßig in die informationstechnischen Systeme des Ursprungsstaates einzugreifen, um diese Angriffe zu stoppen. *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1512 f.). Nach *O. A. Hathaway* würde ein zu weites Verständnis staatliche Unterstützung für humanitäre Hilfsmaßnahmen negativ beeinflussen. *O. A. Hathaway*, The Drawbacks and Dangers of Active Defense, in: P. Brangetto/M. Maybaum/J. Stinissen, 2014 6th International Conference on Cyber Conflict, 2014, S. 39 (49). *B. A. Walton* weist daraufhin, dass in der Staatengemeinschaft keine Einigkeit über das Verständnis von Territorialität und Souveränität in der virtuellen Welt besteht, so dass diese keine geeigneten Anknüpfungspunkte für eine international anerkannte Verbotsnorm im Cyberkontext bieten. *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1475).

142 *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. 177.

bzw. bei Verzicht auf das Zwangselement, wäre der Informationsangriff als völkerrechtswidrige Intervention in den *domaine réservé* der USA zu werten.[143] Die Tatsache, dass die US-Regierung auf den Informationsangriff lediglich mit unfreundlichen Akten, sogenannten Retorsionen, und nicht mit Gegenmaßnahmen reagierte,[144] lässt den Schluss zu, dass sie selbst darin eben keine völkerrechtswidrige Intervention sah.[145] Ein extensiver Ansatz ist demnach nicht nur in der Wissenschaft, sondern ebenso in der internationalen Praxis umstritten. Der Informationsangriff könnte allenfalls dann als völkerrechtswidrige Intervention qualifiziert werden, wenn die Sicherheitslücken in elektronischen Abstimmungsgeräten genutzt worden wären, um Wahlergebnisse zu verfälschen, da derartige Maßnahmen mit subversiver umsturzorientierter Propaganda vergleichbar sind.[146] Der zwangsfreie Zugriff auf die informationstechnischen Systeme des *DNC* und die Verbreitung privater Informationen hingegen bewegt sich in einer Grauzone des internationalen Rechts.[147]

Anders ist jedoch der Informationsangriff auf informationstechnische Systeme Estlands zu bewerten. Die Entscheidung der estnischen Regierung über die Standortverlagerung der Statue eines Soldaten der Roten Armee stand in einem politischen Kontext, da sie als ideologische Annäherung

---

143 *D. B. Hollis*, Russia and the DNC Hack: What Future for a Duty of Non-Intervention?, OpinoJuris, 25 July 2016, abrufbar unter: http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/ (geprüft am 15.05.2020); *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. 177.

144 *D. Roberts*, Obama imposes new sanctions against North Korea in response to Sony Hack, The Guardian, 2 January 2015, abrufbar unter: http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview (geprüft am 15.05.2020).

145 *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1512); *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (643).

146 Tallinn Manual 2.0, Kommentar zu Regel 66, S. 313, Rn. 2; *B. J. Egan*, International Law and Stability in Cyberspace, BJIL 35 (2017), S. 169 (175).

147 *M. N. Schmitt* stellt in diesem Zusammenhang zutreffend fest: „By acting within legal grey zones, Russia makes it difficult for other States to definitively name and shame the country as having committed an internationally wrongful act." *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (2); *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1501).

Estlands an den Westen und die NATO verstanden wird.[148] Überdies steht es jedem Staat grundsätzlich frei, den Standort bedeutender Statuen zu bestimmen. Die Entscheidung über die Verlegung fällt mithin in den *domaine réservé* Estlands.[149] Während der Informationsangriff nicht die Voraussetzungen erfüllt, um Gewalt darzustellen, sprechen mehrere Aspekte dafür, dass er willensbeugende Wirkung entfalten sollte und daher als unzulässige Ausübung von Zwang zu qualifizieren ist. Die weitereichende Störung der informationstechnischen Systeme diente nämlich als Druckmittel, um die estnische Regierung zur Rücknahme ihrer Entscheidung zu bewegen.[150]

Unter dem Blickwinkel politischer Einflussnahme dürften auch die weitreichenden Angriffe gegen informationstechnische Systeme in Georgien erfolgt sein. Südossetien war und blieb integraler Bestandteil Georgiens und betraf damit innere Angelegenheiten des Staates.[151] Der Informationsangriff unterstützte mit seinen einschneidenden Auswirkungen südossetische Sezessionsbestrebungen und verhinderte die politische Interaktion zwischen Regierung und Bürgern sowie Alliierten. Demnach kann der Informationsangriff durchaus als unzulässige Ausübung von Zwang auf den *domaine réservé* Georgiens gewertet werden.[152]

Der Informationsangriff durch das Schadprogramm *Stuxnet* auf informationstechnische Systeme iranischer Atomanlagen, ist – wie gezeigt – als Gewalt im Sinne des Art. 2 Abs. 4 VN-Charta zu qualifizieren. Gewalt stellt die stärkste Form von unerlaubtem Zwang dar.[153] In dem Fall wurde

148 Vgl. *W. C. Ashmore*, Impact of Alleged Russian Cyber Attacks, BSDR 11 (2009), S. 4 (6); *S. Herzog*, Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 50 f.; *A. Schmidt*, The Estonian Cyber Attacks, in: J. Healey (Hg.), A Fierce Domain, 2013, S. 174 ff.

149 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 123 f.

150 *R. Buchan*, Russell, Cyber Attacks, JCSL 17 (2012), S. 212 (225 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. 126; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 124 f.

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

152 *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. 126; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 126.

153 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 127.

Zwang ausgeübt, um die Urananreicherung des Iran zu beeinträchtigen, so dass zugleich der *domaine réservé* des Staates betroffen war.[154]

## III. Informationsspionage

In aller Regel steht Spionage in nationalen Rechtsordnungen unter Strafe.[155] Dies hindert Staaten aber nicht daran, ausländische Regierungen, Wirtschaftsunternehmen und Privatpersonen auszuspähen. Daher stellt sich die Frage, ob Spionage auf internationaler Ebene einem Verbot unterliegt und mithin die Völkerrechtswidrigkeit von Informationsoperationen begründen kann.

### 1. Völkerrechtliche Verbote zur Informationsspionage

Zunächst können die Methoden der Informationsgewinnung gegen das Gewaltverbot oder Interventionsverbot verstoßen, ohne dass die Informationsausbeutung als solche völkerrechtswidrig ist.[156]

Des Weiteren existieren für spezifische völkerrechtliche Regelungsbereiche, wie das Diplomaten- und Konsularrecht, das Seerecht oder das Recht internationaler bewaffneter Konflikte, Normen, die sich mit Spionage auseinandersetzen und begrenzt Schutz vor entsprechenden Handlungen bieten.[157]

Auch im Wirtschaftsvölkerrecht gibt es völkervertragliche Bestimmungen, die Rechte am geistigen Eigentum und Urheberrechte unter den Schutz der Vertragsstaaten innerhalb ihres Hoheitsgebietes stellen und

---

154 Daran ändern auch der Atomwaffensperrvertrag, das geltende Inspektionsregime und die einschlägigen Resolutionen des Sicherheitsrates nichts. Es wird indes diskutiert, ob es sich bei *Stuxnet* um eine völkerrechtlich legale Gegenmaßnahme in Reaktion auf das völkerrechtswidrige Verhalten Irans im Atomstreit gehandelt haben könnte. Siehe *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 127 f.

155 Es ist zu beachten, dass sich aus der weitverbreiteten Kriminalisierung von Spionage in nationalen Rechtsordnungen kein allgemeiner Rechtsgrundsatz herleiten lässt. Siehe hierzu *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 425 (431 f.).

156 Tallinn Manual 2.0 Kommentar zu Regel, S. 170 f., Rn. 8.

157 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 11, Fn. 19 ff.; *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 443 ff.

somit Informationsausbeutung bis zu einem gewissen Grad beschränken. Diese Bestimmungen gehen aber nicht so weit, Wirtschaftsspionage durch fremde Staaten auf internationaler Ebene zu verbieten.[158] Die Mitgliedstaaten der WTO tolerieren fremdstaatliche Wirtschaftsspionage sogar – vermutlich, um sich selbst diese Möglichkeit zu erhalten.[159]

Schließlich sind menschenrechtliche Normen bei der Ausspähung von Individuen zu berücksichtigen.[160] Der Schutz der Privatsphäre und Vertraulichkeit der Kommunikation ist in internationalen und regionalen Menschenrechtsinstrumenten verankert.[161] Staaten, die Personen auf dem eigenen Hoheitsgebiet überwachen, oder auf informationstechnische Systeme zugreifen, die sich auf eigenem staatlichen Territorium befinden, können diese Rechte verletzen.[162] Dabei ist zu beachten, dass die Bestimmungen kein allgemeines Spionageverbot begründen. Eingriffe in die Rechte auf Privatsphäre und Vertraulichkeit der Kommunikation können nämlich durch nationale Vorschriften zum Schutz der öffentlichen Sicherheit erlaubt sein.[163] Der menschenrechtliche Schutz der Privatheit und Vertraulichkeit der Kommunikation bezieht sich zudem nur auf Individuen auf eigenem staatlichen Territorium und unter eigener staatlicher Hoheitsgewalt. Angehörige anderer Staaten im Ausland oder Daten, die auf Informationsinfrastrukturen in fremdem Hoheitsgebiet gespeichert sind oder diese durchlaufen, sind grundsätzlich nicht vom Schutzbereich erfasst.[164] Allerdings gibt es Bestrebungen, den Schutz auf extraterritoriale

158 *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 435 f.

159 *Id.*, S. 436.

160 *D. Korff*, First Do No Harm, in: B. Wagner/M. C. Kettemann/K. Vieth (Hg.), Research Handbook on Human Rights and Digital Technology, 2019, S. 129 ff.; *I. Pernice*, Vom Völkerrecht des Netzes zur Verfassung des Internets, HIIG Discussion Paper Series, Discussion Paper No. 2017–02, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959257 (geprüft am 15.05.2020), S. 1 (6 ff.).

161 Siehe *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 43.

162 Siehe *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 13.

163 *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 435, Fn. 51.

164 *C. Forcese*, Spies Without Borders, JNSLP 5 (2011), S. 179 (208); *R. D. Williams*, (Spy) Game Change, GWLR 79 (2011), S. 1162 (1176 ff.); *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 434.

Informationsausbeutung auszuweiten.[165] Die Speicherung und Weiterverarbeitung von Daten auf staatseigenem Territorium[166] oder die virtuelle Kontrolle durch einen Staat[167] etwa werden als Anknüpfungspunkte für die menschenrechtlichen Schutzpflichten vorgeschlagen. Hoheitsgewalt im Sinne der Konventionen zum Menschenrechtsschutz unterliegt allerdings einem physischen Begriffsverständnis. Sie kann grundsätzlich nicht durch außerhalb des eigenen Staatsgebiets stattfindende digitale Überwachungsmaßnahmen ausgeübt werden.[168] Zudem sind die juristischen Differenzen in der Staatengemeinschaft zum extraterritorialen Schutz der Menschenrechte derzeit zu groß, um extraterritoriale Informationsausbeutung völkerrechtlich zu ahnden.[169]

Zusammenfassend lässt sich festhalten, dass keine allgemeingültige Völkerrechtsnorm existiert, die Spionage *per se* verbietet.[170] Die durchdringenden und schädigenden Dimensionen der Ausbeutung informationstechnischer Systeme, die nicht mit denen der traditionellen Spionage vergleichbar sind, bieten aber Anlass zur Diskussion über ein neues völkergewohnheitsrechtliches Verbot der Informationsspionage.[171] Ein solches Verbot lässt sich jedoch nicht durch entsprechende Staatenpraxis und *opinio iuris* belegen. Insgesamt ist das Interesse an entsprechenden völkerrechtlichen

165 Ob sich der Interpretationsansatz des IACtHR, wonach Staaten es anderen Staaten nicht erschweren dürfen, den Menschenrechtsschutz im staatseigenen Hoheitsgebiet zu gewährleisten (siehe 1. Kapitel B. II. 3.), insbesondere auch außerhalb umweltrechtlicher Problemkreise durchsetzt, bleibt zu zeigen.

166 *H. P. Aust*, Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014 im 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages, abrufbar unter: https://www.bundestag.de/resource/blob/282870/fc52462f2ffd254849bce19d25f72fa2/mat_a_sv-4-1_aust-pdf-data.pdf (geprüft am 15.05.2020), S. 13 f., Rn. 35.

167 *A. Peters*, Surveillance without Borders, EJIL: Talk! 4 November 2013, abrufbar unter: www.ejil talk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/ (geprüft am 15.05.2020).

168 Tallinn Manual 2.0, Kommentar zu Regel 34, S. 185, Rn. 9; *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 13 f.

169 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 14.

170 Das Völkerrecht schweigt zu der Frage der Recht- oder Unrechtmäßigkeit von Spionage zu Friedenszeiten. *H. P. Aust*, Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014 im 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages, abrufbar unter: https://www.bundestag.de/resource/blob/282870/fc52462f2ffd254849bce19d25f72fa2/mat_a_sv-4-1_aust-pdf-data.pdf (geprüft am 15.05.2020), S. 14, Rn. 39.

171 *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 446 ff.

Reglementierungen in der Staatengemeinschaft gering.[172] Das fehlende Verbot der Informationsspionage bietet Staaten vielmehr Anreiz, ihre Kapazitäten zur Informationsausbeutung weiterzuentwickeln. Zugleich wird das Misstrauen zwischen den Staaten stärker. Dies führt wiederum zu einer verminderten internationalen Kooperationsbereitschaft zur Bekämpfung und Reglementierung von Informationsoperationen, die die internationale Sicherheit bedrohen.[173]

### 2. Informationsspionage in der internationalen Praxis

Der Informationsangriff auf die informationstechnischen Systeme des *DNC* unterliegt keinem völkerrechtlichen Verbot. Auch die Informationsausbeutung im Rahmen dieser Informationsoperation ist als völkerrechtlich nicht verbotene Spionage einzustufen, auf die Opferstaaten nur begrenzt mit Mitteln der Selbsthilfe reagieren können.[174]

*Duqu* und *Flame* demonstrieren, wie informationstechnische Systeme in großem Stil zur grundsätzlich erlaubten Militär- oder Wirtschaftsspionage genutzt werden.[175] Die Ausspähung durch die *Five Eyes* zeigt, wie es in der virtuellen Welt zur legalen Aushöhlung des Menschenrechtsschutzes kommt.[176]

Die Informationsausbeutung durch die *Guardians of Peace* veranschaulicht zum einen die immensen wirtschaftlichen Schäden, die durch Informationsausbeutung verursacht werden können.[177] Zum anderen zeigt die Reaktion der USA in diesem Fall, dass auch völkerrechtlich nicht verbotene Informationsoperationen zwischenstaatliche Spannungen begründen. Ohne benennen zu können, inwiefern die Informationsoperation gegen Völkerrecht verstößt, machte die US-Regierung Nordkorea für den „cyber-

172 Tallinn Manual 2.0, Kommentar zu Regel 32, S. 169, Rn. 5; vgl. *K. Ziolkowski*, Peacetime Cyber Espionage, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 437 ff.

173 *D. P. Fidler*, Tinker, Tailor, Soldier, Duqu, IJCIP 5 (2012), S. 28 (29).

174 Vgl. *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (570, 597 f.); *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (2, 8).

175 *D. P. Fidler*, Tinker, Tailor, Soldier, Duqu, 5 (2012), S. 28 (28 f.).

176 Vgl. *M. N. Schmitt/L. Vihul*, The Nature of International Law Cyber Norms, in: A.-M. Osula/H. Rõigas, International Cyber Norms, 2016, S. 23 (44).

177 *R. Crootof*, International Cybertorts, CLR 103 (2018), S. 565 (588, 592).

vandalism“[178] durch die *Guardians of Peace* verantwortlich und belegte den Staat mit Sanktionen.[179]

## *D. Zurechnung*

Staaten sind für völkerrechtswidrige Informationsoperationen verantwortlich, wenn diese ihnen zurechenbar sind.

### I. Zurechnungsregeln

In Ermangelung spezifischer Zurechnungsregeln für die virtuelle Welt haben die für die Staatenverantwortlichkeit etablierten Zurechnungsmechanismen zu gelten.[180] Dementsprechend beleuchtet auch das Tallinn Manual 2.0 deren Anwendbarkeit auf Informationsoperationen.[181]

Eine Zurechnung erfolgt zunächst bei Informationsoperationen, die durch staatliche Organe in amtlicher Eigenschaft ausgeführt werden (Regel 15 Alt. 1 Tallinn Manual 2.0). Zu diesen Organen zählen unter anderem das Militär, Geheimdienste, aber auch staatliche Cyber-Sicherheitszentren, Computersicherheitsereignis- und Reaktionsteams und Cyber-Einheiten, die auf Informationsoperationen spezialisiert sind und zunehmend von Staaten errichtet werden, um die Informationstechnik zum staatlichen Vorteil zu nutzen.[182] Um das Verhalten von Privaten mit dem von staat-

178 *E. Bradner*, Obama: North Korea’s Hack not war, but ‘cybervandalism’, CNN, 24 December 2014, abrufbar unter: http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism (geprüft am 15.05.2020).

179 Die Reaktion der US-Regierung steht exemplarisch für die wachsende Zahl an Konstellationen, in denen Staaten andere Staaten für Informationsoperationen verantwortlich machen, ohne aber genau darlegen zu können, welche völkerrechtliche Norm verletzt wurde. *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1463).

180 *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. 89 ff.; *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 129 ff.

181 Tallinn Manual 2.0, Teil I, Kapitel 4, Abschnitt 1, S. 79 ff.

182 *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. 95; *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 129 f.

lichen Organen geleichstellen zu können, wird eine komplette Abhängigkeit und Kontrolle der privaten Akteure vom und durch den jeweiligen Staat gefordert.[183] Eine Zurechnung in diesem Sinne kann schon in der materialen Welt kaum festgestellt werden und ist in der virtuellen Welt umso schwieriger darzulegen.[184]

Eine Zurechnung ist ferner möglich, wenn private Personen oder Einrichtungen zur Ausübung hoheitlicher Befugnisse ermächtigt sind (Regel 15 Alt. 2 Tallinn Manual 2.0)[185] oder in Ausübung eines konkreten staatlichen Auftrages handeln (Regel 17 lit. a Alt. 1 Tallinn Manual 2.0)[186]. So können private Unternehmen beispielsweise durch Rechtsakte zur defensiven und offensiven Verteidigung staatlicher Informationsinfrastrukturen ermächtigt sein[187] oder sonst mit der Ausführung von bestimmten Informationsoperationen betraut sein.[188] Sofern diese Akteure im Rahmen der übertragenen Befugnisse und Aufgaben völkerrechtswidrig agieren, entsteht eine Verantwortlichkeit des jeweiligen Staates.[189] Der geheime Charakter von Informationsoperationen verhindert in aller Regel, dass eine derartige Verbindung offengelegt werden kann.[190]

Daneben können Informationsoperationen durch staatliche Organe, etwa von Geheimdiensten, die einem anderen Staat zur Verfügung gestellt

183 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 (205 Rn. 393); siehe auch Tallinn Manual 2.0, Kommentar zu Regel 15, S. 88, Rn. 4; *J. Maddocks*, Outsourcing of Governmental Functions in Contemporary Conflict, Va JIL 59 (2019), S. 47 (57).

184 *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. 93.

185 Zur Zurechnung nach Art. 5 ASR siehe *J. Maddocks*, Outsourcing of Governmental Functions in Contemporary Conflict, Va JIL 59 (2019), S. 47 (47 ff.).

186 Zur Zurechnung nach Art. 8, 1. Alt ASR siehe *A. Epiney*, Zur Rechtsfigur des *de facto*-Organs im Recht der Staatenverantwortlichkeit, in: A. Fischer-Lescano/H.-P. Gasser/T. Marauhn/N. Ronzitti (Hg.), Frieden in Freiheit: Festschrift für Michael Bothe, 2008, S. 883 (885 ff.).

187 Tallinn Manual 2.0, Kommentar zu Regel 15, S. 89, Rn. 8.

188 Tallinn Manual 2.0, Kommentar zu Regel 17, S. 95 f., Rn. 4.

189 Eine Zurechnung im Sinne des Art. 15 Tallinn Manual 2.0 erfolgt auch bei *ultra vires* Handlungen. Tallinn Manual 2.0, S. 90 f., Rn. 12.

190 *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. 94; *J. Maddocks*, Outsourcing of Governmental Functions in Contemporary Conflict, Va JIL 59 (2019), S. 47 (83).

werden, die Verantwortlichkeit letzteren Staates begründen (Regel 16 Tallinn Manual 2.0). Auch die Hilfe oder Unterstützung, Leitung oder Kontrolle eines anderen Staates bei oder die Nötigung eines anderen Staates zur Begehung einer völkerrechtswidrigen Informationsoperation können einen verantwortungsbegründenden Zusammenhang herstellen (Regel 18 Tallinn Manual 2.0). Eine Verantwortlichkeit für Informationsoperationen, bei denen mehrere Staaten zu einem bestimmten Grad involviert sind, ist aber überaus schwierig zu begründen. Es lässt sich beispielsweise schon kaum nachweisen, ob ein Geheimdienst Informationen für einen fremden Staat sammelt, um dessen völkerrechtswidrige Informationsoperation zu ermöglichen.[191]

Schließlich ist die Zurechnung aufgrund staatlicher Kontrolle oder Leitung von besonderem Interesse (Regel 17 lit. a Alt. 2 Tallinn Manual 2.0),[192] denn Informationsoperationen erfolgen regelmäßig durch Akteure, die zwar in keiner Weise in den Staatsapparat eingegliedert sind, aber gleichzeitig in gewisser Verbindung zum Staat stehen.[193] In vielen Konstellationen finden sich Anzeichen, die auf eine staatliche Förderung der nicht-staatlichen Akteure hinweisen.[194] Zudem agieren sogenannte patriotische Hacker (*patriotic hacktivists*) oder staatliche Stellvertreter (*proxies*) oftmals im Einklang mit der politischen Agenda eines Staates.[195] Hier führen die unbestimmten Voraussetzungen für eine Zurechnung aufgrund staatli-

191 Vgl. *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. 96.

192 Der Völkerrechtskommission zufolge sind die Elemente der Leitung und der Kontrolle zwar separate Fallgruppen, sie werden in der Rechtsprechung aber regelmäßig zusammen besprochen. Tallinn Manual 2.0, Kommentar zu Regel 17, S. 96, Rn. 5.

193 *J. Maddocks*, Outsourcing of Governmental Functions in Contemporary Conflict, Va JIL 59 (2019), S. 47 (82 f.).

194 Vgl. *D. Garrie/S. R. Reeves*, So You're Telling Me There's A Chance, Harv. NSJ Online Features, 17 December 2015, abrufbar unter: https://harvardnsj.org/wp-content/uploads/sites/13/2016/01/Garrie-and-Reeves-Non-State-Actor-and-Self-Defense.pdf, (geprüft am 15.05.2020), S. 1 ff.; *M. Kahn*, FBI Director Christopher Wray's Remarks on Encryption to the International Conference on Cyber Security, LAWFARE 9 January 2018, abrufbar unter: https://www.lawfareblog.com/fbi-director-christopher-wrays-remarks-encryption-international-conference-cyber-security (geprüft am 15.05.2020).

195 *M. Gervais*, Cyber Attacks and the Laws of War, BJIL 30 (2012), S. 525 (546); *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. 27, 84, 110.

cher Kontrolle oder Leitung in der virtuellen Welt zu Unsicherheiten.[196] Das für eine Zurechnung erforderliche Maß an staatlicher Einflussnahme auf Private erfordert nach der Rechtsprechung des IGH eine sogenannte effektive Kontrolle.[197] Demnach muss der Staat jederzeit über Ziel, Durchführungsmethode und Beendigung des fraglichen privaten Verhaltens bestimmen können.[198] Diese auf kinetische Operationen zugeschnittenen Anforderungen werden mit Blick auf die anonyme und ubiquitäre virtuelle Welt als zu eng gewertet.[199] So gibt es Tendenzen zur Herabsetzung der Zurechnungsschwelle. Unter Bezugnahme auf die Rechtsprechung des Internationalen Strafgerichtshofs für das ehemalige Jugoslawien (IStGHJ) soll eine sogenannte staatliche Gesamtkontrolle über die Handlungen einer nicht-staatlichen Gruppe ausreichen.[200] Während der strenge Maßstab des IGH also die effektive Kontrolle über die konkrete Verletzungshandlung voraussetzt, genügt nach dem weniger strengen Maßstab des IStGHJ die allgemeine Kontrolle über das Tätigkeitsfeld der privaten Akteure, um einen zurechnungsrelevanten Zusammenhang zu begründen. Doch auch die Gesamtkontrolle erfordert staatliche Planung und Überwachung der fraglichen Operation.[201] Dementsprechend reicht das Ausrüsten mit Schadsoftware oder das Finanzieren der privaten Akteure nach keinem

196 Zur Zurechnung nach Art. 8, 2. Alt ASR siehe *A. Epiney,* Zur Rechtsfigur des *de facto*-Organs im Recht der Staatenverantwortlichkeit, in: A. Fischer-Lescano/H.-P. Gasser/T. Marauhn/N. Ronzitti (Hg.), Frieden in Freiheit: Festschrift für Michael Bothe, 2008, S. 883 (888 ff.).

197 IGH, Military and Paramilitary Activities in and against Nicaragua, (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986, S. 14 (64 f. Rn. 115).

198 *A. Epiney,* Zur Rechtsfigur des *de facto*-Organs im Recht der Staatenverantwortlichkeit, in: A. Fischer-Lescano/H.-P. Gasser/T. Marauhn/N. Ronzitti (Hg.), Frieden in Freiheit: Festschrift für Michael Bothe, 2008, S. 883 (890).

199 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 131 f.

200 IStGHJ, Appeals Chamber, Prosecutor v. Duško Tadić, Judgment of 15 July 1999, No. IT-94–1-A, ILM 38 (1999), S. 1518 (1541 Rn. 120, 1544 Rn. 131, 1544 f. Rn. 137, 1546 Rn. 145). Es finden sich Stimmen, die schon die bloße Unterstützung und Beherbergung von nicht-staatlichen Akteuren ausreichen lassen wollen, um einen zurechnungsrelevanten Zusammenhang zu begründen. Siehe hierzu *D. Jinks*, State Responsibility for the Acts of Private Armed Groups, Chi. JIL 4 (2003), S. 83 (83 ff.).

201 IStGHJ, Appeals Chamber, Prosecutor v. Duško Tadić, Judgment of 15 July 1999, No. IT-94–1-A, ILM 38 (1999), S. 1518 (1541 Rn. 120); *A. Cassese*, The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, EJIL 18 (2007), S. 649 (655 ff.).

der beiden Zurechnungsstandards aus, um Staaten eine nicht-staatliche Informationsoperation zuzurechnen.[202] Genauso wenig liegt eine staatliche Kontrolle vor, wenn private Hacker ungefragt Informationsoperationen zur Unterstützung staatlicher Politik ausführen.[203] Eine Verantwortlichkeit kann in diesem Zusammenhang allenfalls durch die staatliche Anerkenntnis und Annahme eines nicht-staatlichen Verhaltens angenommen werden (Regel 17 lit. b Tallinn Manual 2.0). Dabei reicht das bloße Befürworten von patriotischen Informationsoperationen allein nicht aus. Der Staat muss diese vielmehr für sich vereinnahmen, indem er beispielsweise die nicht-staatlichen Akteure vor gegnerischen Informationsoperationen schützt und damit die Fortführung der patriotischen Informationsoperation ermöglicht.[204]

Der IGH verdeutlicht indes durch seine Rechtsprechung, dass der allgemeine Grundsatz, nach dem Staaten nur für Handlungen ihrer *eigenen* Organe verantwortlich sind, nicht zu sehr ausgedehnt werden soll.[205] Gegen eine Lockerung der Zurechnungsmaßstäbe im Kontext von Informationsoperationen spricht zudem die Gefahr, dass Staaten vorschnell zu Unrecht für völkerrechtswidrige Handlungen verantwortlich gemacht werden könnten. Denn die Möglichkeit, den wahren Urheber eines Angriffs zu verschleiern oder gar falsche Spuren zu legen, ist für Informationsoperationen kennzeichnend.[206] Durch die irrtümliche Ausübung von Gegenmaßnahmen können dann zwischenstaatliche Spannungen provoziert oder gar unbeteiligte Staaten in einen Konflikt hineingezogen werden. Zu beachten ist überdies, dass die Auseinandersetzungen im virtuellen Raum schnell in militärische Konfrontation umschlagen können.[207]

---

202 Tallinn Manual 2.0, Kommentar zu Regel 17, S. 97, Rn. 8. Eine Verantwortlichkeit kann in dieser Konstellation aber dann entstehen, wenn diese staatliche Unterstützung für sich genommen das Völkerrecht verletzt. Tallinn Manual 2.0, Kommentar zu Regel 17, S. 92, Rn. 9.

203 *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (10).

204 Tallinn Manual 2.0, Kommentar zu Regel 17, S. 99, Rn. 16.

205 Vgl. *J. Kranz*, Die völkerrechtliche Verantwortlichkeit für die Anwendung militärischer Gewalt, AVR 48 (2010), S. 281 (289 ff.).

206 Siehe ausführlich hierzu *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 36 ff., 149 ff.

207 *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (13); *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 22.

Schließlich erübrigen sich Diskussionen zu Fragen der Übertragbarkeit der etablierten Zurechnungskriterien und der Herabsetzung der traditionellen Zurechnungsschwelle, wenn schon Ursprung und Urheber der Informationsoperation nicht festgestellt werden können.[208] Die IT-Forensik ist nicht ausreichend entwickelt, um die vielfältigen Rückverfolgungs- bzw. Identifizierungsprobleme zu lösen.[209] Selbst in Konstellationen, in denen ein Informationsangriff die Informationsinfrastruktur eines Staates durchläuft oder sogar von regierungseigenen informationstechnischen Systemen ausgeht, kann daraus nicht zweifelsfrei auf eine aktive Beteiligung des betreffenden Staates geschlossen werden. Die geografische Herkunft der Informationsoperation oder ein bestimmter Programmierstil können allenfalls Vermutungen begründen.[210]

Selbst wenn eine technische Zurechnung erfolgreich ist, bestehen immer noch die Nachweisschwierigkeiten hinsichtlich der rechtlichen Beziehung zwischen dem Urheber der Informationsoperation und dem beschuldigten Staat.[211] So lassen sich Zurechnungszusammenhänge in der komplexen virtuellen Welt grundsätzlich nur aus einem Zusammenspiel aus technischen Daten und spezifischen Informationen, etwa über politische Konfliktlagen und staatliche Interessen, konstruieren.[212] Aufgrund dieser rechtlichen und technischen Hürden im Rahmen der Zurechnung von Informationsoperationen sind die geltenden Beweisanforderungen zu hinterfragen. Im Völkerrecht trifft grundsätzlich den beeinträchtigten Staat die Pflicht, zugrunde liegende Sachverhalte aufzuklären und die

208 *S.-H. Schulze* weist richtigerweise daraufhin, dass die Frage nach der Zurechnungsschwelle sich nur stellt, wenn der Akteur zweifelsfrei identifiziert ist und der betroffene Staat sich allenfalls Beweisschwierigkeiten – nicht aber Identifizierungs- bzw. Rückverfolgungshürden – ausgesetzt sieht. *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 134. *J. D. Jolley* befasst sich ebenfalls ausführlich mit den technischen Hürden bei der Zurechnung von Informationsoperationen und kommt zu dem Ergebnis, dass die rechtliche Zurechnung schon aufgrund der Schwierigkeiten bei der technischen Zurechnung nicht möglich ist. *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), Kapitel 4.

209 *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), Kapitel 4; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 36 ff.

210 Tallinn Manual 2.0, Kommentar zu Regel 15, S. 91, Rn. 13 f.

211 *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (632 f.).

212 Vgl. Tallinn Manual 2.0, Allgemeiner Kommentar zu Teil I, Kapitel 4, Abschnitt 1, S. 81 f., Rn. 10.

nötigen Nachweise zu führen. Diese Beweispflicht unterliegt allerdings keinen definierten Standards.[213] Dem IGH zufolge sind die Beweisanforderungen umso höher, je schwerwiegender die Anschuldigungen und je weitreichender die Konsequenzen sind.[214] Die Experten des Tallinn Manual 2.0 bestätigen diesen allgemeinen Grundsatz zunächst, da entsprechend der Schwere des vorgeworfenen Völkerrechtsverstoßes auch die Schwere der zulässigen Reaktion wächst. Allerdings weisen die Experten zugleich darauf hin, dass es bei weniger schweren Angriffen einfacher sein dürfte, mehr Beweise für eine Zurechnung zu sammeln, als bei besonders verheerenden Angriffen, die eine sofortige Reaktion zu deren Beendigung erfordern. Demnach soll der Beweisstandard anhand des konkreten Einzelfalles bestimmt werden.[215] In Rechtsprechung und Literatur findet sich jedenfalls kein einheitliches Bild zu den Beweisanforderungen.[216] So werden unter anderem ein Nachweis „ohne jeden Zweifel"[217], „mit hinreichender Sicherheit"[218] bzw. „ohne begründete Zweifel"[219] oder auch eine „klare

213 *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1504 f.).

214 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).

215 Tallinn Manual 2.0, Allgemeiner Kommentar zu Teil I, Kapitel 4, Abschnitt 1, S. 82, Rn. 11.

216 *M. Roscini*, Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, in: J. D. Ohlin/K. Govern/C. Finkelstein (Hg.), Cyberwar, 2015, S. 215 (222 ff.).

217 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 (218 Rn. 422); *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (35).

218 Iran – US Claims Tribunal, Yeager v. The Islamic Republic of Iran, Award of 2 November 1987 (Award No. 324–10199–1), Iran-USCTR 17 (1987), S. 92 (101 f.).

219 *R. Wolfrum/M. Möldner*, International Courts and Tribunals, Evidence, in: R. Wolfrum (Hg.), MPEPIL 2013, http://www.mpepil.com, Rn. 75, 77.

und überzeugende Beweislage“[220] gefordert. Diese Beweisanforderungen wurden jedenfalls mit Blick auf kinetische Angriffe aufgestellt und können wegen der allenfalls indiziellen Beweiskraft der zur Verfügung stehenden Beweismittel in der virtuellen Welt kaum erfüllt werden.[221] Außerdem ist zu beachten, dass die Aufklärung von Informationsoperationen im Vergleich zu traditionellen Angriffsmethoden mehr Zeit erfordert.[222] Dies hat zur Folge, dass Gegenmaßnahmen durch beeinträchtigte Staaten regelmäßig aufgrund des Zeitablaufs völkerrechtswidrig sein werden. Denn wartet der beeinträchtigte Staat bis eine den Beweisanforderungen genügende Aufklärung der Zurechnungszusammenhänge möglich ist, unterfallen Gegenmaßnahmen aufgrund ihrer zeitlichen Begrenzung regelmäßig der Kategorie der völkerrechtswidrigen Bestrafung.[223] Reagiert der beeinträchtigte Staat hingegen vorschnell und ergibt sich, dass die Beweisanforderungen für eine Zurechnung nicht erfüllt sind, dann ist die Gegenmaßnahme ebenfalls als völkerrechtswidrig zu qualifizieren.[224]

Dementsprechend wird zuweilen die bloße Vermutung für eine Zurechnung von Informationsoperationen als ausreichend erachtet.[225] Maßgeblich sei der Kontext der Informationsoperation. Die Vermutung der Urhe-

---

220 *R. Geiß/H. Lahmann*, Freedom and Security in Cyberspace, in: K. Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 621 (624); *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. 130.

221 *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. 122, 129; *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 22; *S. J. Shackelford/R. B. Andres*, State Responsibility for Cyber Attacks, Geo. JIL 42 (2010–2011), S. 971 (986).

222 Tallinn Manual 2.0, Kommentar zu Teil I, Kapitel 4, Abschnitt 1, S. 81, Rn. 9; *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (632); *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 22.

223 *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 22; *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 80 f.

224 Tallinn 2.0, Kommentar zu Teil I, Kapitel 4, Abschnitt 1, S. 82 f., Rn. 12; *E. T. Jensen/S. Watts*, A Cyber Duty of Due Diligence, Tex. LR 95 (2017), S. 1555 (1564 f.).

225 *W. Heintschel von Heinegg*, Cyberspace, in: R. Schmidt-Radefeldt/C. Meissler (Hg.), Automatisierung und Digitalisierung des Krieges, 2012, S. 159 (172). *S.-H. Schulze* schlägt zudem eine Umkehr der Beweislast vor. *S.-H. Schulze*, Cyber-„War“ – Testfall der Staatenverantwortlichkeit, 2015, S. 149 ff.

berschaft treffe etwa denjenigen Staat, dem die Informationsoperation von Nutzen ist[226] oder der nicht bereit ist, bei der Aufklärung mitzuwirken[227]. Sofern kritische Infrastrukturen betroffen sind, wollen einige Stimmen in der Literatur gänzlich auf das Nachweiserfordernis für eine Zurechnung verzichten.[228] Diese Ansätze könnten abermals aufgrund der erwartbaren Gegenmaßnahmen auf völkerrechtswidriges Verhalten eskalatorische Wirkung entfalten. Der Sinn und Zweck der völkerkriegsrechtlichen Bestimmungen, zwischenstaatliche Gewaltanwendung so weit wie möglich zu begrenzen, wird konterkariert, wenn schon Vermutungen ausreichen, um mit Selbstverteidigung zu reagieren.[229] Im Ergebnis muss daher zumindest mit klaren und überzeugenden Beweisen belegt werden, dass ein Staat hinter einem Informationsangriff steht, um dessen Verantwortlichkeit zu begründen.[230]

## II. Zurechnung in der internationalen Praxis

Betrachtet man aber die bereits dargestellten Beispiele von Informationsoperationen unter diesen theoretischen Aspekten, wird deutlich, dass eine Zurechnung völkerrechtswidriger Informationsoperationen nahezu unmöglich ist.[231]

---

226 Vgl. *M. C. Libicki*, Cyberdeterrence and Cyberwar, 2009, S. 43 ff.

227 *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 f.

228 *S. M. Condron*, Getting it Right, Harv. JOLT 20 (2007), S. 403 (416); siehe auch *T. O. Keber/P. N. Roguski*, Ius ad bellum electronicum?, AVR 49 (2011), S. 399 (416).

229 Vgl. *E. T. Jensen/S. Watts*, A Cyber Duty of Due Diligence, Tex. LR 95 (2017), S. 1555 (1568); *H. Krieger* spricht – unter Verweis auf *M. Bothe*, Terrorism and the Legality of Pre-emptive Force, EJIL 14 (2003), S. 227 (232) – von einer unzulässigen Verbindung des *ius ad bellum* mit dem Vorsorgegebot. *H. Krieger*, Krieg gegen anonymous, AVR 50 (2012), S. 1 (12 f.)

230 *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. 130; *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 22.

231 Vgl. auch *J. S. Davis II/B. Boudreaux/J. W. Welburn/J. Aguirre/C. Ogletree/G. McGovern/M. S. Chase*, Stateless Attribution, 2017, S. 9 ff.; *D. Efrony/Y. Shany*, A Rule

Die Informationsoperation, von der Estland betroffen war, veranschaulicht die Schwierigkeiten bei der Zurechnung von Informationsoperationen durch patriotische Hackergruppen.[232] Die Angriffe wurden zu Internetadressen in Russland zurückverfolgt[233] und teilweise der regierungsnahen russischen Jugendorganisation *Nashi* zugeschrieben.[234] Auch wenn die Informationsoperation als Reaktion auf die Verbringung des Kriegsgefallenendenkmals in Einklang mit den Interessen der russischen Regierung stand, wurde keine Ermächtigung oder Beauftragung durch Russland festgestellt.[235] Zudem verneinte die russische Regierung jedwede Beteiligung an den Angriffen.[236] Allerdings finanziert und unterstützt Russland die Jugendorganisation, so dass durchaus eine gewisse Verbindung zum Staat besteht.[237] Eine Leitung oder Kontrolle der Organisation durch die russische Regierung ist hingegen nicht gegeben, so dass kein zurechnungsrelevanter Zusammenhang hergestellt werden kann.[238]

Die Informationsangriffe auf Georgien wurden mit Russland in Verbindung gebracht, weil diese sich zeitlich im Vorlauf und Parallel zum kinetischen Konflikt mit Russland ereigneten und von russischen Internet-

---

Book on the Shelf?, AJIL 112 (2018), S. 583 (632); *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. 81 f., 100, 216.

232 *T. Payne*, Teaching Old Law New Tricks, LCLR 20 (2016), S. 683 (706 f.).

233 *N. Anderson*, Massive DDOS attacks target Estonia; Russia accused, ars Technica, 14 May 2007, abrufbar unter: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ (geprüft am 15.05.2020); *K. Flook*, Russia and the Cyber Threat, Critical Threats, 13 May 2009, abrufbar unter: http://www.criticalthreats.org/russia/russia-and-cyber-threat (geprüft am 15.05.2020). Der Angriff erfolgte indes über infizierte Computer weltweit, so dass die Beweiskraft der Rückverfolgung relativiert wird. *S. Herzog,* Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 49 (52).

234 *E. Tikk/K. Kadri/L. Vihul*, International Cyber Incidents, 2010, S. 23.

235 *S. Herzog,* Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 49 (53); *E. Tikk/K. Kadri/L. Vihul*, International Cyber Incidents, 2010, S. 23 f.

236 *K. Flook*, Russia and the Cyber Threat, Critical Threats, 13 May 2009, abrufbar unter: http://www.criticalthreats.org/russia/russia-and-cyber-threat (geprüft am 15.05.2020); *S. Herzog,* Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 49 (53).

237 *S. L. Myers*, Youth Groups Created by Kremlin Serve Putin's Cause, The New York Times, 8 July 2007, abrufbar unter: https://www.nytimes.com/2007/07/08/world/europe/08moscow.html?mtrref=www.google.com&gwh=A2CDBA35318FF4A9402F71EECFBA0E21&gwt=pay&assetType=REGIWALL (geprüft am 15.05.2020).

238 *T. Payne*, Teaching Old Law New Tricks, LCLR 20 (2016), S. 683 (707).

adressen stammten.[239] In Anbetracht des militärischen Konflikts um die Region Südossetien wird diskutiert, ob eine faktische Ausübung hoheitlicher Gewalt durch staatliche Stellvertreter zu bejahen ist, indem diese ohne explizite Ermächtigung durch die eigene Regierung, Angriffe gegen fremde Staaten starten, um einen Konflikt zu unterstützen oder ihrer Missbilligung gegenüber dem fremdstaatlichen Verhalten im Rahmen des zwischenstaatlichen Konflikts Ausdruck zu verleihen.[240] Für eine Zurechnung unter diesem Gesichtspunkt ist aber unter anderem eine Aufforderung durch den Staat erforderlich.[241] Der russischen Regierung könnte hier allenfalls der Vorwurf einer stillschweigenden Zustimmung durch ein bewusstes Wegschauen gemacht werden.[242] Dies genügt allerdings nicht, um eine Zurechnung zu begründen.

Ebenso wenig wurde ein Staat für *Stuxnet* – oder dessen Abwandlungen *Duqu* und *Flame* – verantwortlich gemacht. Allerdings deuten Programmierstil, erforderlicher Aufwand und technische Expertise auf einen staatlichen Akteur hin und die mögliche Motivation für eine derartige Informationsoperation indiziert eine Urheberschaft der USA und Israel.[243] Darüber hinaus bezeugen Aussagen von Vertretern der US-Administration, dass die US-Regierung hinter *Stuxnet* steht.[244] Dies kann zwar durchaus als klare und überzeugende Beweislage gelten. Allerdings erfolgte durch den Iran keine Zurechnung der verbotenen Gewaltanwendung zu den USA oder Israel.[245] Dies verdeutlicht den Widerwillen der Staatengemeinschaft einen Präzedenzfall für die Zurechnung von völkerrechtswidrigen Informationsoperationen zu schaffen, vermutlich um einer potenziellen ei-

---

239 *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. 22.

240 *Id.*, S. 110.

241 Vgl. ASR, Kommentar zu Artikel 9, S. 49, Abs. 6.

242 *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. 111.

243 *C. Morton*, Stuxnet, Flame, and Duqu, in: J. Healey (Hg.), A Fierce Domain, 2013, S. 212 (212 ff.); *S. J. Shackelford, Scott J./R. B. Andres*, State Responsibility for Cyber Attacks, Geo. JIL 42 (2010–2011), S. 971 (991).

244 *D. E. Sanger*, Obama Ordered Sped Up Wave of Cyberattacks Against Iran, The New York Times, 1 June 2012, abrufbar unter: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (geprüft am 15.05.2020).

245 *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. 24.

genen Staatenverantwortlichkeit für derartige Operationen zu entgehen.[246] Im Zusammenhang mit völkerrechtlich nicht verbotenen Informationsoperation hingegen erfolgt eine Zurechnung durch betroffene Staaten schon eher.

Die durch die US-Regierung erfolgte Zurechnung der – wenngleich völkerrechtmäßigen – Informationsoperation gegen das *DNC* zu Russland verdeutlicht dabei, wie langwierig und aufwendig die Beweisführung im Kontext von Informationsoperationen ist.[247] Zudem erfolgte die Zurechnung, ohne dass entsprechende Beweise dargetan wurden.[248] Die Zurechnungsanalyse betraf nämlich eine als geheim eingestufte Informationsgewinnung und Staaten trifft keine Pflicht, ihre Beweisführung offenzulegen.[249] Die Zurechnung begründete nicht nur politische Spannungen, sondern bezeugt auch, dass die unbestimmten Beweisstandards einen für das Recht der Staatenverantwortlichkeit zu großen Spielraum lassen.[250] Letztlich kann selbst eine umfassende Zusammenschau von technischen Indizien und nachrichtendienstlichen Erkenntnissen Zweifel an der Urheberschaft nicht beseitigen.[251] So sieht sich auch die von der US-Regierung erfolgte Zurechnung der völkerrechtlich nicht verbotenen Informationsoperation durch die *Guardians of Peace* zu Nordkorea der Kritik ausgesetzt,

246 Vgl. *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (635).

247 Ausführlich zur Beweisführung bei der Informationsoperation gegen das DNC siehe *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1487 ff.).

248 *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1489 ff.).

249 Vgl. Tallinn Manual 2.0, Kommentar zu Teil I, Kapitel 4, Abschnitt 1, S. 83, Rn. 13; *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (633).

250 Vgl. *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1491 f., 1510 f.); *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (633); *J. Goldsmith*, Yet More Thoughts on the DNC Hack: Attribution and Precedent, LAWFARE, 27 July 2016, abrufbar unter: https://www.lawfareblog.com/yet-more-thoughts-dnc-hack-attribution-and-precedent (geprüft am 15.05.2020); *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. 82 f.

251 *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. LR 95 (2017), S. 1487 (1507 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. 82 f.

da nunmehr unternehmensinterne Urheber hinter den Angriffen vermutet werden.[252] Schließlich verdeutlichen die Enthüllungen über die Informationsausbeutung durch die *Five Eyes*, wie umfassend die Beweislage sein muss, um eine Zurechnung unstreitig vornehmen zu können. Im Ergebnis blieb aber auch dieser Fall wegen der fehlenden Völkerrechtswidrigkeit ohne völkerrechtliche Konsequenzen.[253]

Im Ergebnis bleibt wegen der unsicheren Beweislage im virtuellen Raum lediglich die Erwartung, dass beeinträchtigte Staaten „vernünftig" auf Informationsoperationen reagieren.[254]

### *E. Verletzung positiver Verpflichtungen*

Die aufgezeigte Zurechnungslücke zwischen schadhaften Informationsoperationen und der Verantwortlichkeit von Staaten möchten Völkerrechtler durch eine allgemeine Sorgfaltsregel schließen.[255] Dabei wird jedoch verkannt, dass es sich bei der gebotenen Sorgfalt um einen Annex zu primären Pflichten und nicht gleichzeitig um eine selbstständige Norm handelt. Entsprechend unübersichtlich sind die Begründungsansätze für diese allgemeine Sorgfaltsregel und deren Elemente. So erklären die Experten des Tallinn Manual 2.0 zirkelschlüssig: „Properly understood, due diligence is the standard of conduct expected of States when complying

---

252 *J. Goldsmith*, The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance, LAWFARE, 19 December 2014, abrufbar unter: https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance (geprüft am 15.05.2020); *K. Zetter*, Critics Say New Evidence Linking North Korea to the Sony Hack Is *Still* Flimsy, WIRED, 8 January 2015, abrufbar unter: http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy (geprüft am 15.05.2020).

253 Vgl. *M. N. Schmitt/L. Vihul*, The Nature of International Law Cyber Norms, in: A.-M. Osula/H. Rõigas, International Cyber Norms, 2016, S. 23 (44).

254 Tallinn Manual 2.0, Kommentar zu Teil I, Kapitel 4, Abschnitt 1, S. 81 f., Rn. 10; *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (633).

255 Tallinn Manual 2.0, Regel 6 und 7; *K. Bannelier-Christakis*, Cyber Diligence, Baltic YBIL 14 (2014), S. 23 (27 ff.); *E. T. Jensen/S. Watts*, A Cyber Duty of Due Diligence, Tex. LR 95 (2017), S. 1555 (1565); *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (199 ff.); *M. N. Schmitt*, In Defense of Due Diligence in Cyberspace, The Yale LJ Forum 125 (2015), S. 68 (79 f.); *S. J. Shackelford/S. Russell/A. Kuehn*, Unpacking the International Law on Cybersecurity Due Diligence, Chi. JIL 17 (2016), S. 1 (1 ff.); *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (168).

with this [due diligence] principle."[256] Außerdem verwischt dieser Ansatz die Grenze zwischen dem Konzept der Staatenhaftung und demjenigen der Staatenverantwortlichkeit. Denn eine Verletzung der Sorgfaltsregel sei danach gegeben, wenn durch die Informationsoperation Rechte anderer Staaten betroffen seien und zugleich erhebliche negative Auswirkungen für andere Staaten entstünden.[257] Die im *Trail Smelter*-Schiedsspruch aufgestellte haftungsbegründende Voraussetzung „serious consequence"[258] einerseits und die im Sinne der *Korfu Kanal*-Entscheidung für die Verantwortlichkeit erforderlichen „acts contrary to the rights of other States"[259] andererseits werden folgewidrig in einer Sorgfaltsregel für den virtuellen Raum vermischt.[260] Dies verhindert eine klare Abgrenzung zwischen der Schadensvermeidungspflicht und der Verhinderungspflicht.[261]

Sinnvoll ist zwar, dass die Sorgfaltsregel in Bezug auf nicht-staatliche Informationsoperationen nur dann greift, wenn die Operation, hätte der Staat diese selbst vorgenommen, völkerrechtswidrig wäre.[262] Allerdings wird selbst diese Voraussetzung nicht konsequent beibehalten. Demnach erstreckt sich die Sorgfaltsregel auch auf nicht-staatliche Informationsoperationen, die nicht *per se* völkerrechtswidrig sind, aber dennoch erhebliche

256 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 30, Rn. 1.

257 Tallinn Manual 2.0, Regel 6; siehe auch *I. Y. Liu*, The due diligence doctrine under Tallinn Manual 2.0, CLSR 33 (2017), S. 390 (392).

258 Trail Smelter Arbitration (United States v. Canada), Award of 16 April 1938 and 11 March 1941, 3 UNRIAA (1941), S. 1905 (1965).

259 IGH, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ Reports 1949, S. 4 (22).

260 Vgl. Tallinn Manual 2.0, Kommentar zu Regel 6, S. 34, Rn. 15, S. 36 f., Rn. 25; *R. Buchan*, Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm, JCSL 21 (2016), S. 429 (449 f.); *E. T. Jensen/S. Watts*, A Cyber Duty of Due Diligence, Tex. LR 95 (2017), S. 1555 (1565 ff.); *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (11 f.).

261 *J. D. Jolley* erklärt, dass „the duty to prevent and due diligence obligation are closely intertwined. This chapter sets them apart as two distinct theories within international law", ohne jedoch eine genaue Abgrenzung vorzunehmen. *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. 236 f. Siehe auch *S.-H. Schulze*, der betont, dass die allgemeine Verhinderungspflicht nicht mit dem völkergewohnheitsrechtlich geltenden (Umwelt-)Schädigungsverbot zu verwechseln ist. *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 117.

262 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 35, Rn. 18.

negative Auswirkungen auf fremde Staaten haben.[263] Dies führt zu dem paradoxen Ergebnis, dass die Staaten selbst derartige Informationsoperationen ausüben dürfen, aber dazu verpflichtet sind, nicht-staatliche Akteure davon abzuhalten.[264] In diesem Zusammenhang sind auch die Anleihen aus dem Umweltvölkerrecht und die Diskussionen hinsichtlich der Voraussetzungen der erheblichen Schädigung deplatziert.[265] Diese gehören vielmehr zur Schadensvermeidungspflicht aus dem Konzept der Staatenhaftung. Denn im Rahmen staatlicher Verantwortlichkeit wird allenfalls der Eintritt eines immateriellen Schadens gefordert, der aber bereits durch die verantwortlichkeitsbegründende Rechtsverletzung, das heißt „acts contrary to the rights of other States" gegeben ist.[266] Die Bezugnahme auf das Umweltvölkerrecht geht ferner deswegen fehl, weil die für die virtuelle Welt postulierte Sorgfaltsregel keine staatlichen Präventionspflichten, wie etwa die Sicherung der Informationsinfrastruktur und die Überwachung verdächtiger Netzwerkaktivitäten, begründet.[267] Das Umweltvölkerrecht ist aber gerade von dem Gedanken der Prävention gekennzeichnet, da Umweltschäden regelmäßig unumkehrbar sind.[268]

In Anbetracht dieser Unzulänglichkeiten überzeugt die Sorgfaltsregel für den virtuellen Raum nicht.

---

263 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 35 f., Rn. 21.

264 *B. A. Walton*, Duties Owed, Yale LJ 126 (2017), S. 1460 (1498).

265 Vgl. Tallinn Manual 2.0, Kommentar zu Regel 6, S. 36 f., Rn. 25.

266 Siehe 2. Kapitel B. I. 1. Vgl. hingegen *R. Buchan*, der unter Bezugnahme auf die *Korfu Kanal*-Entscheidung und das *Nuklearwaffen*-Gutachten zwar ausführt, dass für die Verletzung der völkergewohnheitsrechtlichen Verhinderungspflicht grundsätzlich kein zusätzliches Schadenselement gefordert wird, dann aber den *Trail Smelter*-Schiedsspruch heranzieht, um zu zeigen, dass Schadensverursachung die Staatenverantwortlichkeit für Informationsoperationen bedingt. *R. Buchan*, Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm, JCSL 21 (2016), S. 429 (449 f.).

267 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 41 f., Rn. 42, Kommentar zu Regel 7, S. 44 f. Rn. 7 ff.; zustimmend *I. Y. Liu*, The due diligence doctrine under Tallinn Manual 2.0, CLSR 33 (2017), S. 390 (395). Nach anderer Auffassung soll die Sorgfaltsregel auch präventive Maßnahmen umfassen. *S. J. Shackelford/S. Russell/A. Kuehn*, Unpacking the International Law on Cybersecurity Due Diligence, Chi. JIL 17 (2016), S. 1 (35 ff.); *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (165 ff.).

268 Vgl. *A. Proelß*, Raum und Umwelt im Völkerrecht, in: W. Graf Vitzthum/ders. (Hg.), Völkerrecht, S. 361 (427 Rn. 112); *M. V. Soto*, General Principles of International Environmental Law, ILSA J. Intl. & Comp. L. 3 (1996), S. 193 (199 f.).

Ein anderer Lösungsansatz für die Zurechnungsprobleme in der virtuellen Welt wird aus den Reaktionen auf die Anschläge des 11. September 2001 hergeleitet. Bekanntermaßen befand die US-Regierung, dass sie das Recht hatte, Selbstverteidigungsmaßnahmen gegen Afghanistan zu ergreifen, weil die Taliban-Regierung Mitglieder des terroristischen Netzwerks *Al-Qaida* beherbergte. Während einige darin eine Herabsetzung der Zurechnungsschwelle erblicken und damit eine Verantwortlichkeit der Taliban-Regierung für die Handlungen von *Al-Qaida* konstruieren,[269] sehen andere in der Reaktion der Staatengemeinschaft auf die Anschläge eine neue Ausnahme von den völkergewohnheitsrechtlichen Zurechnungsregeln der Staatenverantwortlichkeit. Demnach sei ein Staat grundsätzlich auch für nicht-staatliche Völkerrechtsverletzungen verantwortlich, wenn er vorherige Kenntnis von deren Begehung erlangt hatte und nichts dagegen unternommen hat.[270] Eine Verantwortlichkeit für nicht-staatliches Verhalten verstößt aber gegen den Grundsatz der Nicht-Zurechnung reinen Privathandelns.[271] Außerdem wird aufgrund der Entwicklungen nach den terroristischen Anschlägen eine spezifische Verhinderungspflicht mit Blick auf terroristische Handlungen vertreten. Ein Staat habe nunmehr die negative Pflicht, (Cyber-)Terroristen nicht wissentlich sicheren Unterschlupf auf eigenem Staatsgebiet zu gewähren.[272]

Es ist richtig, dass die staatliche Untätigkeit in Kenntnis von nicht-staatlichen, an sich völkerrechtswidrigen Handlungen ausschlaggebend für staatliche Verantwortlichkeit sein muss. Allerdings entsteht diese Verant-

---

269 *D. Jinks*, State Responsibility for the Acts of Private Armed Groups, Chi. JIL 4 (2003), S. 83 (83 ff.).

270 *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. 270 ff.

271 In Bezug auf mögliche Menschenrechtsverletzungen scheinen diese Ansätze auf den ersten Blick zwar begrüßenswert, allerdings dürfen andere rechtliche Konsequenzen nicht außer Acht gelassen werden. Die Umgehung der Zurechnungsvoraussetzungen wäre insbesondere mit Blick auf den *ius ad bellum* Kontext problematisch. Wenn die bloße Duldung von völkerrechtswidrigen Maßnahmen für eine Zurechnung ausreichte, dann könnte dem duldenden Staat ohne Weiteres ein Angriff auf einen anderen Staat zugerechnet werden. Dies würde wiederum Selbstverteidigungsmaßnahmen gegen den duldenden Staat rechtfertigen. Daher ist eine Zurechnung nur möglich, wenn eine Ausübung staatlicher Aufgaben, eine staatliche Kontrolle oder eine nachträgliche Anerkennung gegeben ist. *A. Seibert-Fohr*, Die völkerrechtliche Verantwortung des Staats für das Handeln von Privaten, ZaöRV 73 (2013), S. 37 (42).

272 *J. Bäumler,* Das Schädigungsverbot im Völkerrecht, 2017, S. 296; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 153 ff., 157 ff.

wortlichkeit für staatliches Fehlverhalten und nicht für nicht-staatliche Aktivitäten. Dabei handelt es sich nicht um eine neue Ausnahmeregel der Staatenverantwortlichkeit bzw. um eine spezifische Pflicht in Bezug auf nicht-staatliches Verhalten, sondern lediglich um die altbewährte Regel des internationalen Rechts, dass Staaten nicht nur für völkerrechtswidriges Handeln, sondern auch für völkerrechtswidriges Unterlassen verantwortlich sind.[273]

Es ist im Ergebnis also gar nicht notwendig, dem Konzept der gebotenen Sorgfalt den Status einer selbstständigen Primärpflicht zu verleihen oder eine neue Regel der Staatenverantwortlichkeit zu konstruieren. Wie im Rahmen der Rechtsprechungsanalyse deutlich wurde, haben Staaten positive Handlungspflichten, dafür zu sorgen, dass das nationale Territorium nicht für völkerrechtswidrige Handlungen missbraucht wird und dass unter ihrer staatlichen Hoheitsgewalt keine Verbrechen oder Menschenrechtsverletzungen verübt werden (I.). Die gebotene Sorgfalt spielt als Annex zu dieser positiven Handlungspflicht bei den Elementen „reale Handlungsmöglichkeit" (II.) und „Kenntnis" (III.) eine Rolle.[274] Im Folgenden ist zu zeigen, inwiefern die völkerrechtliche Verhinderungs- bzw. Schutzpflicht in der virtuellen Welt zur Anwendung gelangt (IV.).

## I. Territorium bzw. Hoheitsgewalt

Die virtuelle Welt wird teilweise als Gemeinschaftsgut betrachtet, welches sich der einzelstaatlichen Souveränität entzieht.[275] Die virtuelle Welt kann aber nicht losgelöst von informationstechnischen Infrastrukturen (Com-

273 Siehe 2. Kapitel A. I. 2.

274 Siehe 1. Kapitel B. II.

275 Stellungnahme Deutschlands in: Report of the Secretary-General, Developments in the field of information and telecommunications in the context of international security, Replies received from Governments, UN Doc. A/68/156/Add.1 vom 09.09.2013, S. 7; *M. Aaltola/J. Sipilä/V. Vuorisalo*, Securing Global Commons, A Small State Perspective, The Finnish Institute of International Affairs, Working Paper 71 (2011), abrufbar unter: https://www.fiia.fi/wp-content/uploads/2017/01/wp71.pdf (geprüft am 15.05.2020), S. 9; *J. P. Barlow*, A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, 1996, abrufbar unter: https://www.eff.org/de/cyberspace-independence (geprüft am 15.05.2020); *D. Mandsager* (Hg.), Sanremo Handbook on Rules of Engagement, 2009, S. 15; *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 7; *T. Stein/T. Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 (21 f.).

putern, Sendeanlagen, Kabelnetzen und anderen Einrichtungen) bestehen und auch die Nutzer der informationstechnischen Systeme sind zu berücksichtigen. Diese physischen Komponenten befinden sich nämlich innerhalb staatlicher Territorien und unterliegen mithin der auf der Souveränität beruhenden Hoheitsgewalt der jeweiligen Staaten.[276] Zur Begründung extraterritorialer Hoheitsgewalt ist die Ausübung tatsächlicher Kontrolle über Einrichtungen der Informationsinfrastruktur maßgeblich.[277] Im Ergebnis bilden Territorium und Hoheitsgewalt damit auch in der virtuellen Welt Anknüpfungspunkte für staatliche Verhinderungs- bzw. Schutzpflichten. So sind Staaten verpflichtet, völkerrechtswidrige Informationsoperationen, die ihren Ursprung auf ihrem Territorium oder unter ihrer Hoheitsgewalt haben, zu verhindern[278] und Personen unter ihrer Hoheitsgewalt vor menschenrechtsverletzenden Informationsoperationen zu schützen.[279]

Die grenzüberschreitende Vernetzung von informationstechnischen Systemen, die dezentrale Speicherung von Daten und der globale Datenverkehr über Internet-Knoten führen zugegebenermaßen zu Schwierigkeiten bei der Erfüllung der staatlichen Handlungspflichten.[280] In der Regel sind aber sensible Daten, wie nachrichtendienstliche und sonstige streng geheime Informationen, auf lokalen Datenbanken gespeichert und digitale Steuerungs- und Kontrollsysteme für kritische Infrastrukturen, wie etwa Atommeiler, in auf staatlichem Territorium befindlichen Netzwerken eingegliedert, so dass sich die Problematik der territorialen Zuordnung in Grenzen hält.[281] Die Tatsache, dass Staaten die Nutzung der virtuellen Welt entsprechend völkerrechtlich anerkannter Jurisdiktionstitel reglementieren, beweist zudem, dass eine einzelstaatliche Hoheitsgewalt auch hier möglich ist.[282] Problematisch ist aber, dass viele Informationsopera-

276 *W. Heintschel von Heinegg*, Legal Implications of Territorial Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (10, 13 f.); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 112; *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: dies. (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 135 (162).

277 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 33, Rn. 11.

278 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (137 f.).

279 Tallinn Manual 2.0, Kommentar zu Regel 36, S. 198, Rn. 6.

280 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 111.

281 *Ibid*.

282 Ausführlich zur Anwendbarkeit der völkerrechtlichen Jurisdiktionstitel im virtuellen Raum siehe Tallinn Manual 2.0, Teil I, Abschnitt 3.

tionen über Botnets erfolgen und die einzelnen Bots, aus denen sich das Botnet zusammensetzt, in verschiedenen Staaten lokalisiert sein können.[283] Auch einzelne Datenpakete können durch die Infrastruktur mehrerer Staaten weitergeleitet werden und erst am Zielstaat zusammengefasst erhebliche Auswirkungen haben.[284] Die staatliche Verhinderungspflicht greift aber nur dann, wenn die jeweilige Maßnahme auf staatlichem Territorium bzw. unter staatlicher Hoheitsgewalt für sich völkerrechtswidrig ist. Die völkerrechtswidrige Qualität einer Informationsoperation kann in den meisten Konstellationen hingegen nicht durch die einzelnen Bots in verschiedenen Staaten, sondern erst durch das gesamte Botnet begründet werden.[285] Auch Datenpakete, die durch einen bestimmten Staat fließen, betreffen nur dann dessen Verhinderungspflicht, wenn sie für sich die Intensität der Völkerrechtswidrigkeit erreichen und nicht schon dann, wenn erst das gesamte Datenwerk, welches durch mehrere Staaten fließt, am Endziel eine völkerrechtswidrige Informationsoperation verkörpert.[286]

## II. Reale Handlungsmöglichkeit

Auch wenn Staaten lediglich alle möglichen und zumutbaren Maßnahmen zur Verhinderung völkerrechtswidriger Informationsoperationen ergreifen müssen, stellt diese verhaltensbezogene Pflicht Ursprungs- bzw. Transitstaaten im virtuellen Raum vor Herausforderungen. In Anbetracht der Tatsache, dass die Verhinderungspflicht keine präventiven Maßnah-

283 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 38, Rn. 29; *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (12).

284 *W. Heintschel von Heinegg*, Legal Implications of Territorial Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (17).

285 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 38 f., Rn. 29, 31.

286 *W. Heintschel von Heinegg*, Legal Implications of Territorial Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (17). Die Experten des Tallinn Manual 2.0 hingegen sehen Transitstaaten in der Pflicht, wenn diese Kenntnis von der im Ergebnis völkerrechtswidrigen Informationsoperation haben und die Möglichkeit zu deren Beendigung besitzen. Tallinn Manual 2.0, Kommentar zu Regel 6, S. 33, Rn. 13.

men umfasst,[287] bleiben nämlich in der virtuellen Welt insbesondere aufgrund der Zeit-Raum-Kompression, also der durch die Virtualisierung und Vernetzung bedingten Verkürzung von Distanzen zwischen Zeit und Raum,[288] kaum wirksame Maßnahmen zur Verhinderung von Informationsoperationen.[289] Erschwerend kommt hinzu, dass Daten und Datenpfade, die für völkerrechtswidrige Informationsoperationen genutzt werden, nicht ohne Weiteres lesbar bzw. lenkbar sind. So wird es Staaten in aller Regel schwerfallen, unverzüglich wirksame Verhinderungsmaßnahmen zu ergreifen.[290] Informationsoperationen können unmittelbar von auf staatlichem Territorium befindlichen Infrastrukturen ausgehen, ohne dass der Staat überhaupt die Möglichkeit hat, rechtzeitig zu reagieren.[291]

Allerdings umfasst die positive Handlungspflicht nicht nur die Verhinderung des Eintritts der völkerrechtswidrigen Informationsoperation, sondern auch das Unterbinden von andauernden völkerrechtswidrigen Vorgängen und die Verfolgung sowie Bestrafung von Verursachern.[292] Aber selbst wenn potenziell völkerrechtswidrige Informationsoperationen entdeckt werden, ist es dem Ursprungs- bzw. Transitstaat oftmals nicht möglich, diese zu unterbinden, ohne gleichzeitig erhebliche negative Auswirkungen auf nationale Netzwerke in Kauf nehmen zu müssen. So ist unter Umständen die komplette Isolation des eigenen Netzwerks notwendig, um Informationsoperationen gegen fremde Staaten zu verhindern bzw. zu unterbinden. Dies beeinträchtigt wiederum die Nutzung informationstechnischer Systeme im Ursprungs- bzw. Transitsaat selbst.[293] Die Interessen des Ursprungs- bzw. Transitstaates einerseits und des Opferstaates andererseits müssen in einen vernünftigen Ausgleich gebracht werden,[294] mit der Fol-

287 Wie sich aus den Ausführungen im 1. Kapitel ergibt, ist die Schadensprävention im Konzept der Staatenhaftung zu verorten. Vgl. auch in Bezug auf die postulierte Sorgfaltsregel Tallinn Manual 2.0, Kommentar zu Regel 6, S. 41 f., Rn. 42, S. 46, Rn. 12 f.; *I. Y. Liu*, The due diligence doctrine under Tallinn Manual 2.0, CLSR 33 (2017), S. 390 (394 f.).

288 *S. Böschen/K. Weis*, Die Gegenwart der Zukunft, 2007, S. 83.

289 Vgl. Tallinn Manual 2.0, Kommentar zu Regel 7, S. 49, Rn. 24 f.; *J. Brunnée/T. Meshel,* Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (141).

290 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 34, Rn. 14.

291 *I. Y. Liu,* State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (232).

292 Vgl. IGH, United States Diplomatic and Consular Staff in Tehran (USA v. Iran), Judgment of 24 May 1980, ICJ Reports 1980, S. 3 (3 ff.); *M. J. Sklerov*, Solving the Dilemma of State Responses to Cyberattacks, Military Law Review 201 (2009), S. 1 (62).

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

294 *Ibid*.

ge, dass angesichts der Konsequenzen für den Ursprungs- bzw. Transitstaat regelmäßig wirksame Gegenmaßnahmen gerade nicht erwartet werden können.

Zudem bestehen in der virtuellen Welt besondere Hürden bei der Wahrnehmung staatlicher Schutzpflichten. Staaten können nämlich ausländische Informationsoperationen, die Rechte von Personen unter ihrer Hoheitsgewalt verletzen, kaum abwehren, verfolgen oder ahnden, da die Verursacher regelmäßig der Jurisdiktion eines anderen Staates unterfallen. Die Staaten können allenfalls Auslieferungsbegehren stellen oder den Ursprungsstaat auffordern, Untersuchungen anzustellen und Täter strafrechtlich zu verfolgen.[295] Im Ergebnis können die Staaten ihren Schutzpflichten damit nicht effektiv nachkommen.

Schließlich bestimmt sich die reale Handlungsmöglichkeit des pflichtigen Staates nach dessen technischen Kapazitäten und Ressourcen zur Abwehr der jeweiligen Informationsoperation.[296] In der Praxis ist es selbst entwickelten und technisierten Staaten nur selten möglich, die Quelle komplexer Informationsoperationen aufzuspüren und diese zu unterbinden, so dass eine reale Handlungsmöglichkeit zur Verhinderung von nichtstaatlichen bzw. fremdstaatlichen Rechtsverletzungen im virtuellen Raum nur in begrenzten Fällen gegeben sein wird.[297]

---

295 Die Hürden können durch das Übereinkommen über Computerkriminalität des Europarats vom 23.11.2001, (European Treaty Series – No. 185; BGBl. 2008 II S. 1242) für Vertragsstaaten zwar eingedämmt, aber nicht komplett beseitigt werden. Vgl. *E. T. Jensen*, Cyber Sovereignty, Tex. ILJ 50 (2014) S. 275 (278, 301); *M. F. Miquelon-Weismann*, The Convention on Cybercrime, J. Marshall J. Computer & Info. L. 23 (2005), S. 329 (335 f.).

296 *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. 230; *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (12).

297 *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 36 ff.

### III. Kenntnis

In der virtuellen Welt sind außerdem die Voraussetzungen, unter welchen das Kenntniserfordernis erfüllt ist, unbestimmt.[298]

Während der pflichtige Staat eine vorherige tatsächliche Kenntnis von den nicht-staatlichen bzw. fremdstaatlichen Informationsoperationen in aller Regel bestreiten wird und diese damit nicht ohne Weiteres nachweisbar ist,[299] wird tatsächliche Kenntnis jedenfalls ab dem Zeitpunkt bestehen, ab dem der Opferstaat den Ursprungs- bzw. Transitstaat von der Informationsoperation unterrichtet.[300] Dies spiegelt die Entscheidung des IGH im *Teheraner Geiselnahme*-Fall wieder, in der der Gerichtshof konstatierte, dass dem Iran die dringliche Notwendigkeit zur Ergreifung von Maßnahmen in Anbetracht der wiederholten Hilferufe an das iranische Außenministerium vollkommen bewusst war.[301] Schwieriger ist die Beantwortung der Frage, unter welchen Voraussetzungen mutmaßliche bzw. hypothetische Kenntnis in der virtuellen Welt angenommen werden kann. Dies soll insbesondere dann der Fall sein, wenn sich die Akteure der regierungseigenen Infrastruktur des Ursprungs- bzw. Transitstaates bedienen, wenn die Infrastruktur direkter staatlicher Kontrolle unterliegt oder ausschließlich öffentlichen Zwecken dient.[302] Es ist aber zu berücksichtigen, dass die Verschleierung der wahren Identität der Nutzer informati-

---

298 *J. Brunnée/T. Meshel*, Teaching an Old Law New Tricks, GYIL 58 (2015), S. 129 (142); *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. 195 ff.; *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (232 ff.).

299 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 40, Rn. 38; *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (233).

300 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 40, Rn. 37; *C. Antonopoulos*, State Responsibility in Cyberspace, in: N. Tsagourias/R. Buchan (Hg.), Research Handbook on International Law and Cyberspace, 2015, S. 55 (69); *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. 195.

301 IGH, United States Diplomatic and Consular Staff in Tehran (USA v. Iran), Judgment of 24 May 1980, ICJ Reports 1980, S. 3 (32 f. Rn. 68).

302 Tallinn Manual 2.0, Kommentar zu Regel 6, S. 41, Rn. 40; *W. Heintschel von Heinegg*, Legal Implications of Territorial Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (17); *B. Pirker*, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, in: *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 189 (205 f.).

onstechnischer Systeme (*Spoofing*) oder die Verschlüsselung von Transfer- und Verbindungsdaten und Anonymisierung der Internetnutzung (*Onion Routing*) in der virtuellen Welt Usus sind und Regierungsserver sogar manipuliert werden, um Konflikte zu provozieren.[303]

Dementsprechend stellen sich – ähnlich wie im Kontext der Zurechnung völkerrechtswidriger Informationsoperationen – auch im Zusammenhang mit der Kenntnis von derartigen Operationen Beweisschwierigkeiten im virtuellen Raum. Der Nachweis durch den Opferstaat kann oftmals nicht geführt werden, weil Informationsoperationen sich durch ihre Unsichtbarkeit und Heimlichkeit auszeichnen, netzinterne Vorgänge des Ursprungs- bzw. Transitstaates betreffen und gleichzeitig von ubiquitärem Charakter mit weitreichender Fernwirkung sind. Auch hier wird diskutiert, ob eine Umkehr der Beweislast angezeigt ist.[304] Während einige Stimmen in der Literatur eine widerlegliche Vermutung der Kenntnis bzw. des Kennenmüssens auf Informationsoperationen mittels staatlicher bzw. zu staatlichen Zwecken genutzter Infrastrukturen beschränken wollen,[305] möchten andere die Reichweite der Vermutung auf alle im staatlichen Hoheitsbereich befindliche Infrastrukturen ausweiten.[306] Der IGH lehnte in seiner *Korfu Kanal*-Entscheidung aber eine widerlegliche Vermutung in

303 *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (237); *M. Pihelgas*, Back-Tracing and Anonymity in Cyberspace, in: *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 31 (45); *B. Pirker*, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, in: *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 189 (212).

304 *S.-H. Schulze,* Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 134 f. mit Fn. 441, 151 ff. Es finden sich Vorschläge, die gänzlich auf das Element der Kenntnis verzichten wollen. In Anlehnung an das Umweltvölkerrecht sollen die Maßnahmen, die ein Staat allgemein zur Vermeidung von schadhaften Informationsoperationen unternimmt, maßgeblich sein. *M. J. Sklerov*, Solving the Dilemma of State Responses to Cyberattacks, Military Law Review 201 (2009), S. 1 (71). Der Verzicht auf das Kenntniserfordernis geht aber für das Regime der Staatenverantwortlichkeit zu weit. *B. Pirker*, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, in: *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 189 (205).

305 *W. Heintschel von Heinegg,* Legal Implications of Territorial Sovereignty in Cyberspace, in: C. Czosseck/R. Ottis/K. Ziolkowski (Hg.), 2012 4th International Conference on Cyber Conflict, 2012, S. 7 (17); *B. Pirker*, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, in: *K. Ziolkowski* (Hg.), Peacetime Regime for State Activities in Cyberspace, 2013, S. 189 (205 f.); *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015, S. 152.

306 *C. Antonopoulos,* State Responsibility in Cyberspace, in: N. Tsagourias/R. Buchan (Hg.), Research Handbook on International Law and Cyberspace, 2015,

Bezug auf die Kenntnis des Staates, den die Verhinderungspflicht trifft, eindeutig ab.[307] Die staatliche Kontrolle über ein Territorium führt nicht zu einer Beweislastumkehr.[308] Dem Opferstaat wird lediglich eine erleichterte Beweisführung zugestanden,[309] so dass Aspekte, wie die Haltung des beschuldigten Staates vor und nach der Informationsoperation und der Umstand, dass eine Reihe von gleichgelagerten Informationsoperationen ihren Ursprung in einem Staat haben, hinzugezogen werden können, um staatliche Kenntnis zu belegen.[310] Allerdings ist der geforderte Beweis, nach dem kein Raum für begründete Zweifel bleiben darf,[311] im Kontext von Informationsoperationen nur in den wenigsten Fällen führbar.[312] Trotzdem sollten die Anforderungen nicht herabgesetzt werden, da speziell in der virtuellen Welt die Gefahr besteht, dass Ursprungs- bzw. Transitstaaten zu Unrecht für ein Unterlassen verantwortlich gemacht werden.[313]

---

S. 55 (64); *D. J. Ryan/M. Dion/E. Tikk/J. J. C. H. Ryan*, International Cyberlaw, Geo. JIL 42 (2011), S. 1161 (1185, 1188 f.).

307 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).

308 *Ibid*.

309 *Ibid*.

310 *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. 196; *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (241 f.).

311 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).

312 *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. 122, 129; *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 18/2014, S. 22; *S. J. Shackelford/R. B. Andres*, State Responsibility for Cyber Attacks, Geo. JIL 42 (2010–2011), S. 971 (986).

313 *I. Y. Liu*, State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (237); vgl. auch *J. Stubbs/C. Bing*, Hacking the hackers: Russian group hijacked Iranian spying operation, officials say, Reuters, 21 October 2019, abrufbar unter: https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK (geprüft am 15.05.2020).

## IV. Positive Verpflichtungen in der internationalen Praxis

Steht also lediglich eine fehlende Zurechenbarkeit von an sich völkerrechtswidrigen Informationsoperationen einer Staatenverantwortlichkeit wegen der Verletzung negativer Pflichten entgegen, kann die Verletzung einer positiven Verhinderungs- bzw. Schutzpflicht eine entsprechende Verantwortlichkeit begründen.

In diesem Zusammenhang sind daher die völkerrechtswidrigen Informationsangriffe gegen Estland und Georgien näher zu betrachten.[314] Bei der Informationsintervention gegen Estland nutzten die Verursacher ein Botnet, welches Computer weltweit betraf.[315] Einige betroffene Staaten neutralisierten die auf ihrem Territorium infiltrierten Systeme freiwillig, das heißt ohne einer entsprechenden Rechtspflicht nachzukommen.[316] Der Großteil der Bots ist auf russische Internetadressen zurückzuführen, so dass die vom russischen Territorium ausgehenden Angriffe wohl schon für sich die Intensität der Völkerrechtswidrigkeit erreichten.[317] Estland unterrichtete Russland zwar nicht von den Geschehnissen,[318] so dass eine tatsächliche Kenntnis vor und während der Informationsoperation nicht bejaht werden kann. Jedoch stand die Informationsoperation zumindest im zeitlichen Zusammenhang mit den politischen Spannungen zwischen den Staaten.[319] Zudem weigerte sich Russland, bei der Identifizierung

---

314 Wie gezeigt, lässt die Beweislage im Fall *Stuxnet* eine Zurechnung der völkerrechtswidrigen Informationsoperation zur US-Regierung zu (siehe 3. Kapitel D. II.). Das Schadprogramm infiltrierte über verseuchte USB-Speichersticks Steuerungssysteme von Atomanlagen auf iranischem Hoheitsgebiet. Eine positive Verhinderungspflicht des Iran selbst ist allerdings mangels Kenntnis zu verneinen. Nach Kenntniserlangung wurde der Angriff überdies gestoppt und investigiert (siehe 3. Kapitel B. II.).

315 *E. Tikk/K. Kadri/L. Vihul,* International Cyber Incidents, 2010, S. 23 m.w.N.

316 *Id.*, S. 24.

317 *N. Anderson*, Massive DDOS attacks target Estonia; Russia accused, ars Technica, 14 May 2007, abrufbar unter: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ (geprüft am 15.05.2020); *K. Flook*, Russia and the Cyber Threat, Critical Threats, 13 May 2009, abrufbar unter: http://www.criticalthreats.org/russia/russia-and-cyber-threat (geprüft am 15.05.2020); *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (11).

318 *I. Y. Liu,* State Responsibility and Cyberattacks, IJICL 4 (2017), S. 191 (234).

319 *S. Herzog,* Revisiting the Estonian Cyber Attacks, JSS 4 (2011), S. 49 (50 f.).

der russischen Hacker behilflich zu sein oder diese strafrechtlich zu belangen.[320] Aufgrund der Verbindung zwischen der russischen Regierung und der Hackergruppe *Nashi*, der Instruktionen zur Beteiligung an den Angriffen auf russischsprachigen Internetseiten und der Dauer der Angriffe bleiben keine vernünftigen Zweifel daran, dass Russland mutmaßliche oder zumindest hypothetische Kenntnis von der Informationsoperation hatte.[321] Die Informationsoperation gegen Georgien glich derjenigen gegen Estland. Auch hier haben Sicherheitsexperten die Angriffe auf russische Internetadressen zurückverfolgt. Zudem werden die Angriffe im Kontext des kinetischen Konflikts zwischen Russland und Georgien beurteilt und als Vorbereitung und Unterstützung der militärischen Bodenoperation durch Russland gewertet.[322] Während das bewusste Wegschauen der russischen Regierung in diesem Fall für eine Zurechnung nicht ausreicht, begründet es zumindest eine mutmaßliche oder hypothetische Kenntnis von den Informationsangriffen. Dementsprechend kann eine Verantwortlichkeit Russlands wegen der Verletzung seiner Handlungspflichten angenommen werden. Russland hätte die Informationsinterventionen gegen Estland bzw. Georgien, wenn schon nicht im Vorhinein verhindern, zumindest die andauernden Operationen unterbinden oder im Nachhinein ahnden müssen.[323] Gleichwohl wurde die Verantwortlichkeit Russlands in der realen Welt in keinem der beiden Fälle völkerrechtlich geltend gemacht.[324] Dies liegt wohl daran, dass sich die Staaten noch unsicher bei der

320 *E. Tikk/K. Kadri/L. Vihul,* International Cyber Incidents, 2010, S. 27 f.

321 *Id.*, S. 18 ff.

322 *S. Blank*, Cyber War and Information War à la Russe, in: G. Perkovich/A. E. Levite, Understanding Cyber Conflict, 2017, S. 81 (88 ff.). *A. Hagen,* The Russo-Georgian War 2008, in: J. Healey (Hg.), A Fierce Domain, 2013, S. 194 (194 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. 22.

323 *J. Kulesza*, State responsibility for acts of cyber-terrorism, Global Internet Governance Academic Network, Annual Symposium, Vilnius 2010, S. 12; *M. N. Schmitt*, Grey Zones in the International Law of Cyberspace, YIL Online 42 (2017), abrufbar unter: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf (geprüft am 15.05.2020), S. 1 (11).

324 *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. 22.

Anwendbarkeit herkömmlicher Rechte und Pflichten auf den virtuellen Bereich sind.[325]

Die Fälle der Informationsspionage verstoßen für sich genommen nicht gegen das Völkerrecht und begründen mithin keine Verhinderungspflicht der Ursprungsstaaten. Auch ist eine extraterritoriale Schutzpflicht der Ursprungsstaaten für die Eingriffe in die Privatheit derzeit nicht völkerrechtlich etabliert.[326] Dem Grunde nach besteht zwar eine Schutzpflicht der Zielstaaten gegenüber Personen, die unter ihrer Hoheitsgewalt stehen.[327] Allerdings fehlt es in Konstellationen wie *Five Eyes* an der Kenntnis und der realen Handlungsmöglichkeit der betroffenen Staaten zum Schutz vor der fremdstaatlichen Missachtung der Menschenrechte.[328]

### *F. Zusammenfassung*

Das Recht der Staatenverantwortlichkeit ist zur Reglementierung von Informationsoperationen ungeeignet. Dies liegt zum einen daran, dass schon die besprochenen völkerrechtlichen Verbotstatbestände klar definierte rechtliche Umrisse vermissen lassen, und zum anderen daran, dass die spezifischen technischen Aspekte von Informationsoperationen die Übertragbarkeit dieser Verbote und entsprechender Handlungspflichten auf den virtuellen Raum erschweren.

Informationsoperationen unterfallen nur selten den herkömmlichen völkerrechtlichen Verbotskategorien, da deren Auswirkungen grundsätzlich nicht mit denen von unerlaubter Gewalt oder unerlaubtem Zwang vergleichbar sind. Der Schutz durch das humanitäre Völkerrecht kann

---

325 *P. von Wussow* stellt beispielsweise fest: „Der ursprüngliche Völkerrechtsenthusiasmus, wie er noch im sogenannten *Tallin Manual* (2013/2017) zum Ausdruck kam, weicht dabei immer mehr einem komplexeren Verständnis der Prozesse, in denen sich Normen für den Cyberkrieg erst herausbilden." *P. von Wussow*, „Cyberkrieg", Ethik und Militär 1 (2019), abrufbar unter: http://www.ethikundmilitaer.de/fileadmin/ethik_und_militaer/Ethik-und-Militaer-2019-1.pdf (geprüft am 15.05.2020), S. 11 (16).

326 Ausführlich zum Diskussionsstand über die extraterritoriale Geltung der Menschenrechte siehe *I. Kanalan*, Extraterritoriale Staatenpflichten jenseits der Hoheitsgewalt, AVR 52 (2014), S. 495 (495 ff.).

327 *W. Kälin/J. Künzli*, Universeller Menschenrechtsschutz, 2019, S. 148 f.

328 Kritisch in Bezug auf die behauptete Unkenntnis Deutschlands *K. von Notz*, Der demokratische Rechtsstaat und das Geheimnis der Dienste, Die Friedens-Warte 90 (2015), S. 17 (17 ff.).

ebenso wenig greifen, weil Informationsoperationen nicht ohne Weiteres unter den Angriffsbegriff subsumiert werden können.

Neben diesen Unsicherheiten sind bei der Staatenverantwortlichkeit für informationstechnische Systeme auch stets die wegen völkerrechtswidriger Informationsoperationen möglichen Gegenmaßnahmen zu berücksichtigen, so dass gerade in der virtuellen Welt ein restriktiver Ansatz geboten ist. Bestrebungen, neue Verbote für die virtuelle Welt aufzustellen bzw. bestehende Vorschriften extensiv auszulegen, um die Völkerrechtswidrigkeit von Informationsoperationen begründen zu können, sind aufgrund der fehlenden Grundlage in der Staatenpraxis sowie der Bedrohung für den zwischenstaatlichen Frieden wenig sinnvoll.

Jedenfalls scheitert die Zurechnung von völkerrechtswidrigen Informationsoperationen regelmäßig an den Beweisschwierigkeiten in der virtuellen Welt, denen – wegen des beschriebenen Eskalationspotenzials – nicht mit einer Absenkung der Anforderungen begegnet werden kann.

Schließlich ist eine Verletzung staatlicher Handlungspflichten in der virtuellen Welt regelmäßig mangels realer Handlungsmöglichkeit und/oder fehlenden Nachweises von staatlicher Kenntnis zu verneinen.

Die Fälle aus der internationalen Praxis belegen außerdem, dass die Staaten mit Blick auf das Recht der Staatenverantwortlichkeit und die entsprechenden Regeln des Tallinn Manuals eine Strategie der „silence and ambiguity" verfolgen.[329] Gründe dafür sind geo(-politische) Erwägungen, Geheimhaltungsinteressen hinsichtlich eigener nachrichtendienstlicher Erkenntnisquellen sowie technologischer Kompetenzen und nicht zuletzt Bestrebungen, eigene Informationsoperationen durchzuführen.[330] Insgesamt befinden sich die Staaten noch in einer Reflexionsphase zu der Anwendbarkeit völkerrechtlicher Pflichten in der virtuellen Welt. Aufgrund dieser abwartenden Haltung ist das Völkerrecht in der virtuellen Welt „chronically underenforced".[331] Dies bedeutet aber nicht, dass eine Möglichkeit zur Reglementierung von Informationsoperationen im Völkerrecht fehlt[332]; die Reaktionen der Staaten beweisen lediglich, dass das Regime der Staatenverantwortlichkeit nicht das richtige Instrument zur Regulierung neuer durch die Globalisierung bedingter Gefährdungslagen

329 So *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (583 ff.); vgl. auch *R. Hofmann*, Modernes Investitionsschutzrecht, in: S. Kadelbach/K. Günther (Hg.), Recht ohne Staat?, 2011, S. 119 (129 f.).

330 *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112 (2018), S. 583 (634 f.).

331 *Id.*, S. 583 (647).

332 So aber *id.*, S. 583 (648).

ist. Im Folgenden wird veranschaulicht, dass die Staatenhaftung die völkerrechtliche Lösung für diese Problematik bietet.