Sara Pangrazzi

Cyberangriffe und Völkerrecht

Zur Verhältnismässigkeit staatlicher Gegenmassnahmen

EIZ Publishing

Cyberangriffe und Völkerrecht

Zur Verhältnismässigkeit staatlicher Gegenmassnahmen

Dissertation
der Rechtswissenschaflichen Fakultät
der Universität Zürich
zur Erlangung der Würde einer Doktorin der Rechtswissenschaft

vorgelegt von

Sara Pangrazzi
von Zürich

genehmigt auf Antrag von
Prof. Dr. Oliver Diggelmann
und
Prof. Dr. Urs Saxer

Die Rechtswissenschaftliche Fakultät gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 5. Oktober 2022

Der Dekan: Prof. Dr. Thomas Gächter

Autor: Sara Pangrazzi
Verlag: EIZ Publishing (eizpublishing.ch)
Produktion, Satz & Vertrieb: buch & netz (buchundnetz.com)
ISBN:
978-3-03805-586-0 (Print – Softcover)
978-3-03805-587-7 (Print – Hardcover)
978-3-03805-588-4 (PDF)
978-3-03805-589-1 (ePub)
DOI: https://doi.org/10.36862/eiz-587
Version: 1.04 – 20230919

Die Dissertation wurde publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die vorliegende Dissertation wurde von Sara Pangrazzi eingereicht und von der Rechtswissenschaftlichen Fakultät der Universität Zürich, vertreten durch den Dekan Prof. Dr. Thomas Gächter, am 5. Oktober 2022 abgenommen.
Sie wurde betreut von Prof. Dr. Oliver Diggelmann und Prof. Dr. Urs Saxer.

Das Werk ist als gedrucktes Buch und als Open-Access-Publikation in verschiedenen digitalen Formaten verfügbar: https://eizpublishing.ch/publikationen/cyberangriffe-und-voelkerrecht-zur-verhaeltnismaessigkeit-staatlicher-gegenmassnahmen/.

Die Publikation ist auch auf der Webseite der Zentralbibliothek Zürich abrufbar:
https://www.zb.uzh.ch/de/

Vorwort und Dank

Seit dem Beginn der Recherchearbeiten für die vorliegende Dissertation im Januar 2018 haben sicherheitspolitisch relevante Cyberangriffe auf alltägliche Infrastrukturen massiv zugenommen. So gehen regelmässig Meldungen ein, dass aufgrund digitaler Ausfälle ganze Flughafen-Dienstleister[1], globale Netzwerke sozialer Medien[2], Versorgungssysteme von Öl und Treibstoff[3] oder digitale Infrastrukturen in Spitälern oder Grossunternehmen[4] aussteigen. Die damit verbundenen Risiken werden mittlerweile gar zu den »grössten sicherheitspolitischen Herausforderungen des 21. Jahrhunderts« gezählt.[5]

Was für eine Funktion hat und soll nun bei diesen Entwicklungen das Völkerrecht haben? Die Frage nach der Funktion von Völkerrecht sowie die damit einhergehenden Grenzen zur Politik beschäftigen die Wissenschaft schon lange. So hat Hersch Lauterpacht die Frage nach der Funktion des Völkerrechts in der internationalen Staatengemeinschaft bereits 1933 aufgeworfen.[6] Da Cyberangriffe mittlerweile zu einem prioritären Thema internationaler Sicherheitspolitik wurden, behalten diese Fragen auch angesichts moderner Phänomene ihre Relevanz. Wie verhält sich das Völkerrecht also zu neuartigen Phänomenen und wie reagiert es auf sich ändernde Umstände?

Vor dem Hintergrund der internationalen Stabilität und Kontinuität ist es zunächst wichtig, dass das Vertrauen in bewährte Institutionen und Mechanismen durch neue Generationen von Betrachtern immer wieder von neuem bestätigt wird.[7] Dies gilt daher auch für die Regulierung neuer Phänomene wie sicherheitspolitisch relevanter Cyberangriffe. Der Cyberraum betrifft darüber hinaus mittlerweile *jeden* digital aufgestellten Staat, was eine internationale Lösungssuche zu sich stellenden Fragen unumgänglich macht und ein staatenübergreifendes Interesse am Thema nahelegt. Die Komplexität von

---

1 Schürpf, NZZ vom 04.02.2022.

2 Hurtz, Süddeutsche Zeitung vom 05.10.2021.

3 Mäder, NZZ vom 04.02.2022; Nakashima et al., Washington Post vom 08.05.2021.

4 Betschon, NZZ vom 15.05.2017; Newman, Wired vom 23.12.2019.

5 UN Doc. A/65/201, (2010), S. 2.

6 Lauterpacht Hersch, The Function of Law in the International Community, Oxford 1933 (neue Aufl. mit Einleitung von Martti Koskenniemi 2011).

7 Diggelmann, in: Gjon, Plädoyer vom 20.11.2017, S. 14 f.

Cybertechnologien führt zudem dazu, dass zunehmend interdisziplinäre Zusammenarbeiten und Beiträge aller Stakeholder (d.h. der Wissenschaft, der Privatwirtschaft sowie des öffentlichen Sektors) erforderlich sind.

Während der Ausarbeitung des Manuskripts hatte ich das grosse Glück und die Ehre, mich mit inspirierenden Persönlichkeiten aus Wissenschaft und Praxis auszutauschen. Dies erlaubte es mir, wertvolle Anregungen und Rückmeldungen zu aktuellen Entwicklungen in der Cybersicherheit sowie zu meinen Gedanken, Ideen und Herangehensweisen zu erhalten, die letztlich in dieser Dissertation reflektiert sind.

Allen voran möchte ich mich bei meinem Doktorvater, Prof. Dr. iur. Oliver Diggelmann, für seine wertvolle Unterstützung bedanken. Die Zusammenarbeit mit ihm hat es mir nicht nur erlaubt, einen wissenschaftlichen Zugang zu meinem Thema zu finden, sondern mir ebenfalls wegweisende, zentrale Einsichten in das internationale Recht mitgegeben. Ebenso danke ich Prof. Dr. iur. Urs Saxer, dass er sich bereit erklärt hat, das Zweitgutachten dieser Dissertation zu übernehmen.

Nachdrücklich danke ich auch dem Forschungskredit der Universität Zürich, Verfügung Nr. [FK-20-012], der es mir ermöglicht hat, mich eingehend meinem Dissertationsprojekt widmen zu können. Beim Schweizerischen Nationalfonds bedanke ich mich für die grosszügige Übernahme der Kosten der Open-Access-Publikation.

Im Rahmen dieser Dissertation hatte ich ferner das Glück, einen Forschungsaufenthalt am Lauterpacht Center for International Law an der Universität Cambridge (UK) wahrzunehmen. Daher gilt ein grosser Dank der Institution und den damit einhergehenden Recherche- und Netzwerkmöglichkeiten vor Ort. Mitunter hatte ich die Chance, mich mit Prof. Dapo Akande, Prof. Christine Gray und weiteren Experten auszutauschen und anregende Rückmeldungen zu meinen Gedanken zu erhalten. Die Arbeiten dieser Völkerrechtsexperten haben damit als wichtige Quellen Eingang in verschiedene Abschnitte der vorliegenden Dissertation gefunden.

Über diese Dissertation wurde ich auch Teil eines interdisziplinär aufgestellten Forschungsprojekts der Digital Society Initiative (DSI) der Universität Zürich sowie deren interdisziplinären Community, die sich zurzeit noch im Aufbau befindet. Das betreffende Projekt »für eine Schaffung eines ethischen und rechtlichen Governance-Rahmens für vertrauenswürdige Cybersicherheit in der Schweiz« ist Teil des Nationalen Forschungsprogrammes NRP-77 »Digitale

Transformation« und erlaubte mir einen regelmässigen Austausch mit Wissenschaftlern der Universität Zürich und Lausanne sowie dem GovCERT des Nationalen Zentrums für Cybersicherheit der Schweiz (NCSC). In diesem Rahmen möchte ich mich insb. bei PD Dr. sc. (Techn.) Markus Christen und Dr. Melanie Knieps für all die Gespräche und das Vertrauen in der Zusammenarbeit rund um Cybersicherheit bedanken. Selbstverständlich gilt der Dank auch dem breiteren DSI-Netzwerk. Namentlich erwähnt sei auch Prof. (em.) Dr. sc. (Techn.) Peter Heinzmann, dem ich im Rahmen einer seiner IT-Sicherheits- und Datenschutzweiterbildungskurse grundlegende Einsichten zu den technischen Aspekten von Cyberangriffen und Informationssicherheit zu verdanken habe.

Diese Dissertation hat es mir zudem ermöglicht, während dieser Zeit Teil des Netzwerks von ICT4Peace zu werden. Für den damit verbundenen Austausch zu Cyberfragen danke ich insbesondere Dr. Martin Dahinden und Dr. Daniel Stauffacher.

Ein ausserordentlicher Dank gilt auch dem Europa Institut an der Universität Zürich (EIZ) und dem Woodrow Wilson Center for Scholars in Washington D.C. In der Schlussphase der Dissertation hatte ich die Chance, als letzte Swiss Fellow im Namen des EIZ einen Forschungsaufenthalt am Woodrow Wilson Center wahrzunehmen. Der »Short-term Research Grant« des EIZ erlaubte es mir, Erfahrungen an einem der führenden US-Think Tanks zu machen und in die akademische und aussenpolitische Community in Washington D.C. eingebunden zu sein. Dies ermöglichte es mir, aufschlussreiche Einblicke in die US-amerikanischen Herangehensweisen rund um das Thema Cyber und Sicherheitspolitik zu erhalten und viel über die geopolitischen Herausforderungen im Kontext einer internationalen Grossmacht zu lernen. Eine Perspektive, die letztlich auch für das Völkerrecht (und den Diskurs um Cyber) massgeblich ist. Ein besonderer Dank gilt in diesem Zusammenhang auch der Schweizer Botschaft in Washington D.C. Ich hatte die Ehre, in einem sehr anregenden Austausch mit den dortigen Diplomaten und Vertetern zu stehen.

Schliesslich möchte ich meinem Umfeld danken. Der innigste Dank gilt dabei meiner Familie. Ich schätze es zutiefst, dass sie mir diesen Weg nicht nur ermöglicht, sondern mich auf diesem auch begleitet, weitergebracht und unterstützt hat. Dasselbe gilt für meine Freunde und Doktoratskollegen. Ohne all die Gespräche, die geteilten Freuden, die offenen Ohren und Hinweise – beim Kaffee am Rechtswissenschaftlichen Institut, in den Bibliotheken in Cambrige sowie auch privat – wäre dieser Weg nämlich nur halb so schön gewesen. Na-

mentlich erwähnt seien an dieser Stelle meine Lektorin, Larissa Tschudi, und RA Daniel Rüfli, die mir darüber hinaus wertvolle Rückmeldungen zum Manuskript gegeben haben.

Insgesamt hat mir die Arbeit an meiner Dissertation aufgezeigt, dass das Thema der Cybersicherheit nicht nur für Forschungsinstitutionen wichtig ist, sondern dies staatenübergreifend auch für weite Bereiche der Politik, der Strafverfolgung und der Privatwirtschaft ist. Zudem waren wesentliche Teile der Ausarbeitung sowie die Finalisation des Manuskripts der Dissertation von der Corona-Pandemie geprägt. Damit verbunden war es mir gerade auch aufgrund der Digitalisierung möglich, während meinen Auslandsaufenthalten weiterhin via Online-Gesprächen eng mit Kollegen der DSI der Universität Zürich im Kontakt zu sein. Vor diesem Hintergrund unverkennbar war und ist, dass eine fundamentale und zunehmende Digitalisierung unseres Alltags stattfindet, indem die berufliche und private Kommunikation (zeitenweise vollumfänglich) auf digitale Medien verschoben wurde. Gerade vor dem Hintergrund der Cybersicherheit bringen diese Entwicklungen neben einem hilfreichen Digitalisierungsschub selbstredend auch weitreichende Herausforderungen mit sich. Brennende Fragen der Cybersicherheit werden sich daher auch künftig aus verschiedener Sicht stellen.

Ich hoffe, dass dieses Buch eine wissenschaftliche Perspektive auf die Strukturen und Mechanismen völkerrechtlicher Selbsthilfe im Kontext von Cyberangriffen und damit einen Beitrag zu einigen der vielen sich stellenden Fragen bieten kann. Da diese Dissertation im Herbstsemester 2022 angenommen wurde, sind Entwicklungen, Literatur und Rechtsprechung bis zum 31. Mai 2022 berücksichtigt.

Zürich, im März 2023 Sara Pangrazzi

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Add.	Addendum
ARSIWA	Artikelentwurf für die Verantwortlichkeit von Staaten für völkerrechtswidriges Handeln, angenommen von der Völkerrechtskommission (ILC) auf ihrer 53. Sitzung (2001), aufgenommen von der Generalversammlung der Vereinten Nationen auf ihrer 56. Tagung (2001) in Resolution 56/83, bestätigt auf ihrer 59. Tagung (2004) in Resolution 59/35
ARSIWA-Kommentar	Kommentar zum Artikelentwurf für die Verantwortlichkeit von Staaten für völkerrechtswidriges Handeln auf ihrer 53. Sitzung (2001), nachgedruckt in: James Crawford (Hrsg.), The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries, Cambridge 2002
Art.	Artikel
Bd.	Band
bspw.	beispielsweise
Budapest-Konvention	Übereinkommen über Computerkriminalität vom 23. November 2001, Sammlung Europäischer Verträge Nr. 185
C	Commentary (=Kommentar zu den Regeln in den Tallinn Manuals)
CCDCOE	The NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team (=Computersicherheits-Ereignis- und Reaktionsteam)
CIA	Confidentiality, Integrity, Availability (=Vertraulichkeit, Integrität und Verfügbarkeit eines Computers)
CISA	Cybersecurity and Infrastructure Security Agency
DDoS	Denial-of-Service-Angriff
EGMR	Europäischer Gerichtshof für Menschenrechte
EJIL	European Journal of International Law
ENISA	European Union Agency for Cybersecurity

et al.	et alii (=und weitere)
etc.	et cetera
EU	Europäische Union
f./ff.	folgende (Seite/Seiten, Note/Noten)
Fn.	Fussnote
GA I	Genfer Abkommen vom 12. August 1949 zur Verbesserung des Loses der Verwundeten und Kranken der bewaffneten Kräfte im Felde, 32 UNTS 1950
GA II	Genfer Abkommen zur Verbesserung des Loses der Verwundeten, Kranken und Schiffbrüchigen der bewaffneten Kräfte zur See, 86 UNTS 1950
GA III	Genfer Abkommen vom 12. August 1949 über die Behandlung der Kriegsgefangenen, 136 UNTS 1950
GA IV	Genfer Abkommen vom 12. August 1949 über den Schutz von Zivilpersonen in Kriegszeiten, 288 UNTS 1950
gem.	gemäss
GovCERT	Government Computer Emergency Response Team (=Nationales Computersicherheits-Ereignis- und Reaktionsteam)
Hrsg.	Herausgeber/-in
i.d.R.	in der Regel
i.e.S.	im engeren Sinne
i.S.	im Sinne
i.S.v.	im Sinne von
i.w.S.	im weiteren Sinne
i.Z.m.	im Zusammenhang mit
ICJ	International Court of Justice (=Internationaler Gerichtshof)
ICRC	International Committee of the Red Cross (=Internationales Komitee vom Roten Kreuz)
IEEE	Institute of Electrical and Electronics Engineers
IGH	Internationaler Gerichtshof (=International Court of Justice/Cour Internationale de Justice)
IGH-Statut	Statut des Internationalen Gerichtshofs vom 26. Juni 1945, 33 UNTS 993

ILA	International Law Association
ILC	International Law Comission (=UNO-Völkerrechtskommission)
IMT	International Military Tribunal for the Trial of Major War Criminals (=Nürnberg-Tribunal)
insb.	insbesondere
IoT	internet of things (sog. Internet der Dinge)
IP	Internet-Protokoll
IStGJ	Internationaler Strafgerichtshof für Ex-Jugoslawien (=International Criminal Tribunal for the former Yugoslavia)
ITLOS	International Tribunal on the Law of the Sea (=Internationaler Seegerichtshof)
lit.	litera (=Buchstabe)
m.V.a.	mit Verweis auf
m.w.H.	mit weiteren Hinweisen
m.w.V.	mit weiteren Verweisen
MCAV	Verordnung über die militärische Cyberabwehr vom 30. Januar 2019, SR 510.921
MG	Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung, SR 510.10
MPEPIL	Max Planck Encyclopedias of Public International Law
NATO	North Atlantic Treaty Organization (=Nordatlantikpakt)
NCS-II	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken für die Jahre 2018-2022
NCSC	Nationales Zentrum für Cybersicherheit (der Schweiz)
NDG	Bundesgesetz vom 25. September 2015 über den Nachrichtendienst, SR 121
No.	Number
Nordatlantikvertrag	Nordatlantikvertrag vom 4. April 1949, 34 UNTS 243
Nr.	Nummer
NZZ	Neue Zürcher Zeitung
o.V.	ohne Verfasser

OEWG	United Nations Open-Ended Working Group on Developments in the Dield of Information and Telecommunications in the Context of International Security
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
R	Rule (=Regel gemäss Tallinn Manuals)
Res.	Resolution
reu	Reuters Presseagentur
RIAA	Reports of International Arbitral Awards
Römer-Statut	Römer-Statut des Internationalen Strafgerichthofs vom 17. Juli 1998, 2187 UNTS 3
S.	Seite(n)
SCADA	Supervisory Control and Data Acquisition (nachfolgend auch »Kontrollsystem« genannt)
SCO	Shanghai Cooperation Organisation (=Shanghaier Organisation für Zusammenarbeit)
Sess.	Session
sog.	sogenannte(r)
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 1. Januar 2023), SR 311.0
StIGH	Ständiger Internationaler Gerichtshof (=Permanent Court of International Justice/Cour permanente de Justice international; September 1922–April 1946)
u.a.	unter anderem
UK	United Kingdom of Great Britain (=Grossbritannien)
UN Doc.	UN-Dokument
UN GGE	United Nations Group of Governmental Experts (=UN-Expertengruppe)
UN-Charta	Charta der Vereinten Nationen vom 26. Juni 1945, UNTS I-1
UN/UNO	United Nations Organization (=Vereinte Nationen)
UNODA	United Nations Office for Disarmament Affairs (=Büro der Vereinten Nationen für Abrüstungsfragen)
UNTS	United Nations Treaty Series

US	United States (of America)
USA	United States of America
u.U.	unter Umständen
v.	versus
v.a.	vor allem
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
vgl.	vergleiche
Vol.	Volume
vs.	versus
WTO	World Trade Organization (=Welthandelsorganisation)
z.B.	zum Beispiel
Ziff.	Ziffer
zit.	zitiert
Zusatzprotokoll I	Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (angenommen in Genf am 8. Juni 1977), 4 UNTS 1979

Judikaturverzeichnis

IGH, Bosniengenozid-Urteil	International Court of Justice, Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Urteil vom 26. Februar 2007, I.C.J. Reports 2007, S. 43 ff.
IGH, Gabčíkovo-Nagymaros-Urteil	International Court of Justice, Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), Urteil vom 25. September 1997, I.C.J Reports 1997, S. 7 ff.
IGH, Grenzgebiets- und San Juan Strassenbau-Urteil	International Court of Justice, Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Urteil vom 16. Dezember 2015, I.C.J. Reports 2015, S. 665 ff.
IGH, Kongo-Urteil	International Court of Justice, Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Urteil vom 19. Dezember 2005, I.C.J. Reports 2005, S. 168 ff.
IGH, Korfu Kanal-Urteil	International Court of Justice, Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), Urteil vom 9. April 1949, I.C.J. Reports 1949, S. 4 ff.
IGH, Kroatien-Genozid-Urteil	International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia), Urteil vom 3. Februar 2015, I.C.J. 2015, Reports, S. 3 ff.
IGH, Nicaragua-Urteil	International Court of Justice, Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Urteil vom 27. Juni 1986, I.C.J. Reports 1986, S. 14 ff.

IGH, Nicaragua, Jurisdiktions-Urteil	International Court of Justice, Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction of the Court and Admissibility of the Application, Urteil vom 26. November 1984, I.C.J. Reports 1984, S. 392 ff.
IGH, Nuklearwaffen-Gutachten	International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Gutachten vom 8. Juli 1996, I.C.J. Reports 1996, S. 226 ff.
IGH, Ölplattformen-Urteil	International Court of Justice, Oil Platforms (Islamic Republic of Iran v. United States of America), Urteil vom 6. November 2003, I.C.J. Reports, S. 161 ff.
IGH, Schutzmauer-Gutachten	International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Gutachten vom 9. Juli 2004, I.C.J. Reports 2004, S. 136 ff.
IGH, Teheraner Geiselfall	International Court of Justice, Case Concerning United States Diplomate and Consular Staff in Tehran (United States of America v. Iran), Urteil vom 24. Mai 1980, I.C.J. Reports, S. 3 ff.
IGH, Zellstofffabriken-Fall	International Court of Justice, Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Urteil vom 20. April 2010, I.C.J. Reports 2010, S. 14 ff.
IMT, Nürnberg-Urteil	International Military Tribunal (Nuremberg) for the Trial of Major War Criminals, Urteil vom 1. Oktober 1946, nachgedruckt in: 41 American Journal of International Law 1947, S. 172 ff.
IStGJ, Tadić-Berufungskammerentscheid	International Criminal Tribunal for the former Yugoslavia, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Prosecutor v. Dusko Tadić), Entscheid der Berufungskammer vom 2. Oktober 1995, IT-94-1-I
IStGJ, Tadić-Urteil	International Criminal Tribunal for the former Yugoslavia, Appeals Chamber (Prosecutor v. Dusko Tadić), Urteil vom 15. Juli 1999, IT-94-1-A
Luftverkehrs-Schiedsspruch	Reports of International Arbitral Awards (RIAA) XVIII, Air Service Agreement of 27 March 1946 (United States of America v. France), Schiedsspruch vom 9. Dezember 1978, S. 417 ff.

Naulilaa-Schiedsspruch	Reports of International Arbitral Awards (RIAA) II (Portugal v. Germany), Schiedsspruch vom 31. Juli 1928, S. 1011 ff.
StIGH, Chorzów-Fall	Permanent Court of International Justice, Case Concering the Factory at Chorzów, (Germany v. Poland), Urteil vom 26. Juli 1927, PCIJ Series A, No. 17, S. 7 ff.
Trail-Smelter-Schiedsspruch	Reports of International Arbitral Awards (RIAA) III (United States of America v. Canada), Schiedsspruch vom 11. März 1941, S. 1905 ff.

Literaturverzeichnis

Ablon Lillian/Bogart Andy, Zero Days, Thousands of Nights, The Life and Times of Zero-Day Vulnerabilities and their Exploits, Santa Monica 2017

Agenturmeldung reu, Deutsches Amt warnt vor möglichen Hackerangriffen auf Kraftwerke, NZZ vom 05.01.2020

Agenturmeldung reu/afp/dpa, Macron wird kurz vor Stichwahl Opfer von »massivem« Hackerangriff, NZZ vom 06.05.2017

Ago Robert, Addendum to the Eight Report on State Responsibility, The Internationally Wrongful Act of the State, Source of International Responsibility (Doc. A/CN.4/318/Add.5–7), II(1) Yearbook of the International Law Commission 1980, S. 13 ff.

Akande Dapo/Coco Antonio/Dias Talita de Souza, Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond, European Journal of International Law (EJIL) Blog vom 05.01.2021, abrufbar unter: <https://www.ejil-talk.org/old-habits-die-hard-applying-existing-international-law-in-cyber-space-and-beyond/> (zuletzt besucht: März 2023)

Akande Dapo/Liefländer Thomas, Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense, 107 American Journal of International Law 2013, S. 563 ff.

Aldrich Richard W., How Do You Know You Are at War in the Information Age?, 22 Houston Journal of International Law 2000, S. 224 ff.

Alland Denis, The Definition of Countermeasures, in: James Crawford/Alain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 1127 ff.

Alvarez José E., State Sovereignty is Not Withering Away: A Few Lessons for the Future, in: Antonio Cassese (Hrsg.), Realizing Utopia: The Future of International Law, Oxford 2012, S. 26 ff.

Antolin-Jenkins Vida M., Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?, 51 Naval Law Review 2005, S. 132 ff.

Arangio-Ruiz Gaetano, Fourth Report on State Responsibility (Doc. A/CN.4/444 and Add.1–3), II(1) Yearbook of the International Law Commission 1992, S. 1 ff.

Arend Anthony Clark/Beck Robert J., International Law and the Use of Force, 2. Aufl., London 2021

Arquilla John/Ronfeldt David, Cyberwar is Coming!, 12/2 Comparative Strategy 1993, S. 141 ff.

Ashford Warwick, Cyber Collateral Damage a Concern for All, says Lancope, ComputerWeekly vom 15.11.2013, abrufbar unter: <https://www.computerweekly.com/news/2240209139/Cyber-collateral-damage-a-concern-for-all-says-Lancope> (zuletzt besucht: März 2023)

Badr Gamal Mourси, The Exculpatory Effect of Self-Defense in State Responsibility, 10 Georgia Journal of International and Comparative Law 1980, S. 1 ff.

Baezner Marie, Cybersicherheit in den US-chinesischen Beziehungen, Center for Security Studies (CSS) Analysen zur Sicherheitspolitik, ETH Zürich 2018

Baezner Marie/Cordey Sean, Nationale Cybersicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz, Center for Security Studies (CSS) Cyber Defense Report, ETH Zürich 2019

Baezner Marie/Robin Patrice, Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict, Center for Security Studies (CSS) Cyber Defense Project, ETH Zürich 2017 (zit. Baezner/Robin, Information Warfare)

Baezner Marie/Robin Patrice, Hotspot Analysis: Stuxnet, Center for Security Studies (CSS) Cyber Defense Project, ETH Zürich 2017 (zit. Baezner/Robin, Stuxnet)

Banks William C., The Role of Counterterrorism Law in Shaping ad Bellum Norms for Cyber War, 89/157 International Legal Studies 2013, S. 157 ff.

Banks William C./Criddle Evan J., Customary Constraints on the Use of Force: Article 51 with an American Accent, 29 Leiden Journal of International Law 2016, S. 67 ff.

Barnett Roger W., A Different Kettle of Fish: Computer Network Attack, in: Michael N. Schmitt/Brian T. O'Donnell (Hrsg.), Computer Network Attack and International Law, 76 International Law Studies 2002, S. 21 ff.

Baumgärtner Malk/Gebauer Matthias/Knobbe Martin/Rosenbach Marcel, Wer will die Verantwortung übernehmen, Unschuldige zu töten?, Der Spiegel vom 24.08.2018, abrufbar unter: <https://www.spiegel.de/politik/cyber-angriffe-auf-deutschland-wer-will-die-verantwortung-uebernehmen-a-00000000-0002-0001-0000-000159070517> (zuletzt besucht: März 2023)

Baumgärtner Malk/Gebauer Matthias/Knobbe Martin/Rosenbach Marcel/Wiedmann-Schmidt Wolf, So rüstet sich Deutschlands geheime Cyberarmee, Der Spiegel vom 24.11.2017, abrufbar unter: <https://www.spiegel.de/spiegel/deutschland-ruestet-im-cyberkrieg-auf-a-1179975.html> (zuletzt besucht: März 2023)

Benzing Markus, Evidentiary Issues, in: Andreas Zimmermann/Christian J. Tams (Hrsg.), The Statute of the International Court of Justice: A Commentary, Oxford 2019, S. 1371 ff.

Berkowitz Bruce, Warfare in the Information Age, 12 Issues in Science and Technology 1995, S. 59 ff.

Bethlehem Daniel, Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors, 106 American Journal of International Law 2012, S. 770 ff.

Betschon Stefan, Es gibt Cyberrisiken, die wir noch gar nicht kennen, Interview mit Vincent Lenders, NZZ vom 05.12.2019

Betschon Stefan, Noch nie wurden so schnell so viele Computer beschädigt, NZZ vom 15.05.2017

Betschon Stefan, Stuxnet ist zurück, NZZ vom 11.11.2013

Bing Christopher/Lynch Sarah, US Charges North Korean Hacker in Sony, WannaCry Cyberattacks, Reuters vom 06.09.2018, abrufbar unter: <https://www.reuters.com/article/us-cyber-northkorea-sony-idUSKCN1LM20W> (zuletzt besucht: März 2023)

Blank Laurie R., Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace, in: Jens David Ohlin/David Govern/Claire Finkelstein (Hrsg.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford 2015, S. 76 ff. (Blank Laurie, Cyberwar)

Blank Laurie R., International Law and Cyber Threats from Non-State Actors, 89 International Law Studies 2013, S. 406 ff. (Blank Laurie, Non-State Actors)

Blank Stephen J., Preparing for the Next War, 24 Strategic Review 1996, S. 17 ff.

Bodungen Clint E./Hilt Stephen/Scambray Joel/Shbeeb Aaron/Singer Bryan L./Wilhoit Kyle, Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions, New York 2016

Borger Julian, As France Becomes Latest Target, Are Election Hacks the New Normal?, The Guardian vom 06.05.2017, abrufbar unter: <https://www.theguardian.com/world/2017/may/05/french-election-hack-emmanuel-macron> (zuletzt besucht: März 2023)

Borghard Erica D./Schneider Jacquelyn, Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal, The Washington Post vom 09.05.2019, abrufbar unter: <https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/> (zuletzt besucht: März 2023)

Borys Christian, The Day a Mysterious Cyber-attack Crippled Ukraine, BBC vom 04.07.2017, abrufbar unter: <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine> (zuletzt besucht: März 2023)

Bossert Thomas, It's Official: North Korea Is Behind WannaCry, The Wall Street Journal vom 18.12.2017, abrufbar unter: <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537?shareToken=st2d38565d59c24132b421a4b03edb68b5&reflink=article_email_share> (zuletzt besucht: März 2023)

Bosshardt Matthias/Dübendorfer Thomas/Plattner Bernhard, Enhanced Internet Security by a Distributed Traffic Control Service Based on Traffic Ownership, 30 Journal of Network and Computer Applications 2007, S. 841 ff.

Boulos Sonia, The Tallinn Manual and Jus ad bellum: Some Critical Notes, in: J. Martín Ramírez/Luis A. García-Segura (Hrsg.), Cyberspace: Risks and Benefits for Society, Security and Development, Cham 2017, S. 231 ff.

Bowett D.W., Self-Defense in International Law, Manchester 1958

Bradford William C., The Duty to Defend Them: A Natural Law Justification for the Bush Doctrine of Preventive War, 79/4 Notre Dame Law Review 2004, S. 1365 ff.

Brenner Joel, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, New York 2011

Brewster Thomas, An NSA Cyber Weapon Might be Behind a Massive Global Ransomware Outbreak, Forbes vom 12.05.2017, abrufbar unter: <https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/> (zuletzt besucht: März 2023)

Broad William J./Markoff John/Sanger David E., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times vom 15.01.2011, abrufbar unter: <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html> (zuletzt besucht: März 2023)

Broeders Dennis/De Busser Els/Pawlak Patryk, Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates, The Hague Program for Cyber Norms Policy Brief, The Hague 2020

Brunner Isabella/Dobrić Marija/Pirker Verena, Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ, 25 Finnish Yearbook of International Law 2015, S. 75 ff.

Buchan Russell, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, in: 17/2 Journal of Conflict and Security Law 2012, S. 211 ff.

Burkart Patrick/McCourt Tom, Why Hackers Win: Power and Disruption in the Network Society, Oakland 2019

Bussolati Nicolò, The Rise of Non-State Actors in Cyberwarfare, in: Cyberwar, Law and Ethics for Virtual Conflicts, Jens David Ohlin/Kevin Govern/Claire Finkelstein (Hrsg.), Oxford 2015, S. 102 ff.

Caltagirone Sergio/Frincke Deborah, The Response Continuum, Proceedings of the Sixth Annual IEEE Workshop on Information Assurance and Security, New York, 15–17 June 2005, S. 258 ff.

Cannizzaro Enzo, Contextualizing Proportionality: *jus ad bellum* and *jus in bello* in the Lebanese War, 88 International Review of the Red Cross 2006, S. 779 ff. (Cannizzaro, Contextualizing Proportionality)

Cannizzaro Enzo, The of Proportionality in the Law of International Countermeasures, 12/5 European Journal of International Law 2001, S. 889 ff. (Cannizzaro, Countermeasures)

Cassese Antonio, International Law, 2. Aufl., Oxford 2005

Castañeda Frank/Sezer Emre Can/Xu Jun, Worm vs. Worm: Preliminary Study of an Active Counter-Attack Mechanism, in: Association for Computing Machinery (Hrsg.), Proceeding of the 2004 ACM Workshop on Rapid Malcode, Washington D.C. 2004, S. 83 ff.

Chesney Robert, Hackback Is Back: Assessing the Active Cyber Defense Certainty Act, Lawfare vom 14.06.2019, abrufbar unter: <https://www.lawfareblog.com/hack-back-back-assessing-active-cyber-defense-certainty-act> (zuletzt besucht: März 2023)

Chesterman Simon, Secret Intelligence, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2009

Clarke Richard A./Knake Robert K., Cyber War: The Next Threat to National Security and What to Do About It, New York 2010 (Clarke/Knake, Cyber War)

Clarke Richard/Knake Robert, The Fifth Domain: Defending our Country, our Companies, and Ourselves in the Age of Cyber Threats, New York 2019 (zit. Clarke/Knake, Fifth Domain)

Cobb Stephen/Lee Andrew, Malware is Called Malicious for a Reason: The Risks of Weaponizing Code, in: Pascal Brangetto/Markus Maybaum/Jan Stinissen (Hrsg.), 6th International Conference on Cyber Conflict, Tallinn 2014, S. 71 ff.

Coco Antonio/Dias Talita de Souza, 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law, 32/3 European Journal of International Law 2021, S. 771 ff.

Colarik Andrew M., Cyber Terrorism: Political and Economic Implications, London 2006

Collins Sean/McCombie Stephen, Stuxnet: The Emergence of a New Cyber Weapon and its Implications, 7 Journal of Policing, Intelligence and Counter Terrorism 2012, S. 80 ff.

Condron Sean M., Getting It Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harvard Journal of Law and Technology 2007, S. 404 ff.

Cook James L., Is There Anything Morally Special about Cyberwar?, in: Cyberwar, Law and Ethics for Virtual Conflicts, Jens David Ohlin/Kevin Govern/Claire Finkelstein (Hrsg.), Oxford 2015, S. 16 ff.

Corera Gordon, UK and US join Forces to Strike Back in Cyberspace, BBC News vom 18.11.2021, abrufbar unter: <https://www.bbc.com/news/technology-59335332> (zuletzt besucht: März 2023)

Corera Gordon, UK's National Cyber Force Comes out of the Shadows, BBC News vom 20.11.2020, abrufbar unter: <https://www.bbc.com/news/technology-55007946> (zuletzt besucht: März 2023)

Corn Geoffrey S., The Essential Link between Proportionality and Necessity in the Exercise of Self-Defense, in: Claus Kress/Robert Lawless (Hrsg.), Necessity and Proportionality in International Peace and Security Law, Lieber Studies, Vol. 5, Oxford 2021, S. 79 ff.

Corner Elizabeth, Cyber Attack Caused 2008 Pipeline Explosion?, World Pipelines vom 12.12.2014, abrufbar unter: <https://www.worldpipelines.com/business-news/12122014/cyber-attack-caused-2008-pipeline-explosion/> (zuletzt besucht: März 2023)

Corten Oliver, Necessity, in: Marc Weller (Hrsg.), The Oxford Handbook of the Use of Force in International Law, Oxford 2015, S. 861 ff. (zit. Corten, Necessity)

Corten Oliver, The 'Unwilling or Unable' Test: Has it Been, and Could it be, Accepted?, 29 Leiden Journal of International Law 2016, S. 777 ff. (zit. Corten, Unwilling or Unable)

Corten Oliver, The Law Against War, Oxford 2010 (zit. Corten, Law Against War)

Couzigou Irène, The Challenges Posed by Cyberattacks to the Law on Self-Defence, European Society of International Law, 4/16 Conference Paper Series 2014, S. 1 ff.

Crawford James, Brownlie's Principles of Public International Law, 9. Aufl., Oxford 2019 (zit. Crawford, Brownlie's Principles)

Crawford James, Sovereignty as a Legal Value, in: James Crawford/Martti Koskenniemi (Hrsg.), The Cambridge Companion to International Law, Cambridge 2012, S. 117 ff. (Crawford, Sovereignty)

Crawford James, State Responsibility, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2006 (zit. Crawford, MPEPIL 2006)

Crawford James, State Responsibility, The General Part, Cambridge 2013 (zit. Crawford, State Responsibility)

Crawford James, Third Report on State Responsibility (Doc. A/CN.4/507/Add.3), II(1) Yearbook of the International Law Commission 2000, S. 3 ff. (zit. Crawford, Third Report)

Crawford James/Olleson Simon, The Character and Forms of International Responsibility, in: Malcolm D. Evans (Hrsg.), International Law, 5. Aufl., Oxford 2018, S. 415 ff.

D'Amato Anthony, International Law, Process and Prospect, 2. Aufl., New York 1995

D'Aspremont Jean, Cyber Operations and International Law: An Interventionist Legal Thought, 21/3 Journal of Conflict and Security Law 2016, S. 575 ff.

Dahm Georg/Delbrück Jost/Wolfrum Rüdiger, Völkerrecht Bd. I/3, Berlin 2002

David Eric, Primary and Secondary Rules, in: James Crawford/Alain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 27 ff.

De Frouville Olivier, Attribution of Conduct to the State: Private Individuals, in: James Crawford/Allain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 257 ff.

Deeks Ashley S., "Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense, 52 Virginia Journal of International Law 2012, S. 483 ff.

Del Mar Katherine, The International Court of Justice and Standards of Proof, in: Karine Bannelier/Théodore Christakis/Sarah Heathcote (Hrsg.), The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case, London 2012, S. 98 ff.

Delerue François, Cyber Operations and International Law, Cambridge 2020 (zit. Delerue, Cyber Operations)

Delerue François, Reinterpretation or Contestation of International Law in Cyberspace?, 52/3 Israel Law Review 2019, S. 295 ff. (zit. Delerue, Reinterpretation or Contestation)

Denning Dorothy E., Framework and Principles for Active Cyber Defense, 40 Computers and Security 2014, S. 108 ff. (zit. Denning, Active Cyber Defense)

Denning Dorothy E., Information Warfare and Security, Reading (Massachusetts) 1999 (zit. Denning, Information Warfare)

Dewar Robert S., Trend Analysis: Active Cyber Defense, Center for Security Studies (CSS), ETH Zürich 2017 (zit. Dewar, Active Cyber Defense)

Dewar Robert S., Trend Analysis: Contextualizing Cyber Operations, Center for Security Studies (CSS), ETH Zürich 2018 (zit. Dewar, Contextualizing)

Dewar Robert, The "Triptych of Cyber Security": A Classification of Active Cyber Defence, in: Pascal Brangetto/Markus Maybaum/Jan Stinissen (Hrsg.), 6th International Conference on Cyber Conflict, Tallinn 2014, S. 7 ff. (zit. Dewar, Triptych of Cyber Security)

Dewar Robert, Trend Analysis 2: Cyberweapons: Capability, Intent and Context in Cyberdefense, Center for Security Studies (CSS), ETH Zürich 2017 (zit. Dewar, Cyberweapons)

Dias Talita/Coco Antonio, Cyber Due Diligence in International Law, Project Report, Oxford 2021

Diggelmann Oliver, Es gibt kein Recht auf Krieg, NZZ vom 29.03.2018

Diggelmann Oliver, Militärische Gewalt bei Cyberattacken, NZZ vom 30.05.2013

Diggelmann Oliver, Völkerrecht, Geschichte und Grundlagen. Mit Seitenblicken auf die Schweiz, Baden 2018 (zit. Diggelmann, Völkerrecht)

Diggelmann Oliver/Hadorn Nina, Gewalt- und Interventionsverbot bei Cyberangriffen: Ausgewählte Schlüsselfragen, in: Christian Schubel/Stephan Kirste/Peter-Christian Müller-Graff/Oliver Diggelmann/Ulrich Hufeld (Hrsg.), Jahrbuch für Vergleichende Staats- und Rechtswissenschaften, Baden-Baden 2017, 255 ff.

Dinstein Yoram, Computer Network Attacks and Self-Defense, 76 International Law Studies 2002, S. 99 ff. (zit. Dinstein, Computer Network Attacks)

Dinstein Yoram, Implementing Limitations on the Use of Force: The Doctrine of Proportionality and Necessity, in: American Society of International Law (Hrsg.), Proceedings of Annual Meeting, Vol. 86, 1–4 April 1992, S. 54 ff. (zit. Dinstein, Proportionality and Necessity)

Dinstein Yoram, War, Aggression and Self-Defence, 6. Aufl., Cambridge 2017 (zit. Dinstein, War, Aggression and Self-Defence)

Dittrich David/Himma Kenneth Einar, Active Response to Computer Intrusions, in: Hossein Bidgoli (Hrsg.), The Handbook of Information Security, Vol. III, Hoboken (New Jersey) 2005, S. 664 ff.

Doffman Zak, Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First, Forbes vom 06.05.2019, abrufbar unter: <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/> (zuletzt besucht: März 2023)

Dörr Oliver, Prohibition of Use of Force, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2019

Dörr Oliver, Weitere Rechtsquellen des Völkerrechts, in: Knut Ipsen, Völkerrecht, Volker Epping/Wolff Heintschel von Heinegg (Hrsg.), 7. Aufl., München 2018, S. 536 ff.

Dunn Cavelty Myriam, Cyberkrieg – und keiner geht hin?, ETH Zukunftsblog vom 15.06.2018, abrufbar unter: <https://ethz.ch/de/news-und-veranstaltungen/eth-news/news/2018/06/blog-dunn-cyberwar-security.html> (zuletzt besucht: März 2023)

Dunn Cavelty Myriam, Warum Cyberangriffe nicht als Waffe taugen, ETH Zukunftsblog vom 18.01.2018, abrufbar unter: <https://ethz.ch/de/news-und-veranstaltungen/eth-news/news/2018/01/dunn-cavelty-cyberwar.html> (zuletzt besucht: März 2023)

Dunn Cavelty Myriam, Wie real ist der Cyberkrieg?, Computerworld vom 17.05.2013, abrufbar unter: <https://www.computerworld.ch/business/forschung/real-cyberkrieg-1330350.html> (zuletzt besucht: März 2023)

Dupuy Pierre-Marie/Hoss Cristina, Trail Smelter and Terrorism: International Mechanisms to Combat Transboundary Harm, in: Rebecca M. Bratspies/Russell A. Miller (Hrsg.), Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration, Cambridge 2006, S. 225 ff.

Dyzenhaus David, The Rule of (Administrative) Law in International Law, 68 Law and Contemporary Problems 127 2005, S. 127 ff.

Egan Brian J., International Law and Stability in Cyberspace, 35 Berkeley Journal of International Law 2017, S. 169 ff.

Egloff Florian/Wenger Andreas, Öffentliche Attribution von Cybervorfällen, Center for Security Studies (CSS) Analysen zur Sicherheitspolitik, ETH Zürich 2019

Elagab Omer Yousif, The Legality of Non-Forcible Counter-Measures in International Law, Oxford 1988

Epiney Astrid, Die völkerrechtliche Verantwortlichkeit von Staaten für rechtswidriges Verhalten im Zusammenhang mit Aktionen Privater, Baden-Baden 1992

Eriksson Johan/Giacomello Giampiero, The Information Revolution, Security, and International Relations: (IR)relevant Theory?, 27 International Political Science Review 2006, S. 221 ff.

Evron Gadi, Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War, 9/1 Georgetown Journal of International Affairs 2008, S. 121 ff.

Farrer Martin, New Zealand Stock Exchange hit by Cyber Attack for Second Day, The Guardian vom 26.08.2020, abrufbar unter: <https://www.theguardian.com/technology/2020/aug/26/new-zealand-stock-exchange-hit-by-cyber-attack-for-second-day> (zuletzt besucht: März 2023)

Finkelstein Claire/Govern Kevin, Introduction, Cyber and the Changing Face of War, in: Jens David Ohlin/David Govern/Claire Finkelstein (Hrsg.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford 2015, S. ix ff.

Fitzmaurice Malgosia A., The Corfu Channel Case and the Development of International Law, in: Nisuke Ando/Edward McWhinney/Rüdiger Wolfrum (Hrsg.), Liber Amicorum Judge Shigeru Oda, Vol. 1, Den Haag 2002, S. 119 ff.

Fleck dieter, Searching for International Rules Applicable to Cyber Warfare – A Critical Assessment of the New Tallinn Manual, 18 Journal of Conflict and Security 2013, S. 331 ff.

Fletcher George P./Ohlin Jens D., Defending Humanity: When Force Is Justified and Why, Oxford 2013

Focarelli Carlo, Self-Defence in Cyberspace, in: Nicholas Tsagourias/Russell Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl., Cheltenham 2021, S. 317 ff.

Franck Thomas Martin, On Proportionality of Countermeasures in International Law, 102/4 American Journal of International Law 2008, S. 715 ff. (zit. Franck, Proportionality)

Franck Thomas Martin, Recourse to Force, Cambridge 2002 (zit. Franck, Recourse to Force)

Franck Thomas Martin, The Power of Legitimacy Among Nations, New York 1990 (zit. Franck, Legitimacy Among Nations)

Friedmann Wolfgang, The Changing Structure of International Law, London 1964

Gady Franz-Stefan/Austin Greg, Russia, The United States, and Cyber Diplomacy: Opening the Doors, EastWest Institute Report, New York 2010

Gallagher Sean, Eternally Blue: Baltimore City Leaders Blame NSA for Ransomware Attack, Ars Technica vom 28.05.2019, abrufbar unter: <https://arstechnica.com/information-technology/2019/05/eternally-blue-baltimore-city-leaders-blame-nsa-for-ransomware-attack/> (zuletzt besucht: März 2023)

Gardam Judith Gail, Necessity, Proportionality and the Use of Force by States, Cambridge 2004 (zit. Gardam, Necessity, Proportionality)

Gardam Judith Gail, Proportionality and Force in International Law, 87/3 American Journal of International Law 1993, S. 391 ff. (zit. Gardam, Proportionality and Force)

Gattini Andrea, Evidentiary Issues in the ICJ's Genocide Judgment, 5 Journal of International Criminal Justice 2007, S. 889 ff.

Gaycken Sandro, Cyberwar: Das Internet als Kriegsschauplatz, München 2011

Gazzini Tarcisio/Werner Wouter G./Dekker Ige F., Necessity Across International Law: An Introduction, 41 Netherlands Yearbook of International Law 2010, S. 3 ff.

Geiss Robin/Lahmann Henning, Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention, in: Katharina Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, Tallinn 2013, S. 621 ff.

Gervais Michael, Cyber Attacks and the Laws of War, 30 Berkeley Journal of International Law 2012, S. 525 ff.

Ghorbani Ali A./Lu Wei/Travallaee Mahbod, Network Intrusion Detection and Prevention: Concepts and Techniques, New York 2010

Giles Keir/Hagestad William, Divided by a Common Language: Cyber Definitions in Chinese, Russian and English, in: Karlis Podins/Jan Stinissen/Markus Maybaum (Hrsg.), 5th International Conference on Cyber Conflict, Tallinn 2013, S. 413 ff.

Giles Keir/Hartmann Kim, Socio-Political Effects of Active Cyber Defence Measures, in: Pascal Prangetto/Markus Maybaum/Jan Stinissen (Hrsg.), 6th International Conference on Cyber Conflict, Tallinn 2014, S. 23 ff.

Gjon David, Stabilität fällt nicht vom Himmel, Plädoyer vom 20.11.2017, S. 14 f.

Glennon Michael J., The New Interventionism: The Search for a Just International Law, 78/3 Foreign Affairs 1999, S. 2 ff.

Glenny Misha, A Weapon We Can't Control, The New York Times vom 24.06.2012, abrufbar unter: <https://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html> (zuletzt besucht: März 2023)

Goldsmith Jack, How Cyber Changes the Laws of War, 24 European Journal of International Law 2013, S. 129 ff.

Goodin Dan, NSA-leaking Shadow Brokers just dumped its most damaging release yet, Ars Technica vom 14.04.2017, abrufbar unter: <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/> (zuletzt besucht: März 2023)

Gordon Edward, Article 2(4) in Historical Context, 10 The Yale Journal of International Law 1985, S. 271 ff.

Gowlland-Debbas Vera, Responsibility and the United Nations Charter, in: James Crawford/Alain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 115 ff.

Gray Christine, International Law and the Use of Force, 4. Aufl., Oxford 2018 (zit. Gray, Use of Force)

Gray Christine, The Charter Limitations on the Use of Force: Theory and Practice, in: Vaughan Lowe/Adam Roberts/Jennifer Welsh/Dominik Zaum (Hrsg.), The United Nations Security Council and War, The Evolution of Thought and Practice since 1945, Oxford 2008, S. 86 ff. (zit. Gray, The Charter Limitations)

Gray Christine, The Limits of Force, in: The Hague Academy of International Law (Hrsg.), Collected Courses of The Hague Academy of International Law, Vol. 376, The Hague 2014, S. 101 ff. (zit. Gray, Limits of Force)

Green James A., The International Court of Justice and Self-Defence in International Law, Oxford 2009

Greenberg Andy, Sandworm, A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, New York 2019

Greenberg Andy, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired vom 22.08.2018, abrufbar unter: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (zuletzt besucht: März 2023)

Greenwood Christopher, Self-Defence, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2011

Gross Michael L., Proportionate Self-Defense in Unarmed Conflict, in: Michael L. Gross/Tamar Meisels (Hrsg.), Soft War, The Ethics of Unarmed Conflict, Cambridge 2017, S. 217 ff.

Halberstam Manny, Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks, 46/1 George Washington International Law Review 2013, S. 199 ff.

Hargrove John Lawrence, The Nicaragua Judgement and the Future of the Law of Force and Self-defense, 81 American Journal of International Law 1987, S. 135 ff.

Harrison Dinniss Heather, Cyber Warfare and the Laws of War, Cambridge 2012

Hathaway Oona A., The Drawbacks and Dangers of Active Defense, in: Pascal Brangetto/Markus Maybaum/Jan Stinissen (Hrsg.), 6th International Conference on Cyber Conflict, Tallinn 2014, S. 39 ff. (zit. Hathaway, Active Defense)

Hathaway Oona A./Crootof Rebecca/Levitz Philip/Nix Haley/Nowlan Aileen/Perdue William/Spiegel Julia, The Law of Cyber-Attack, 100 California Law Review 2012, S. 817 ff.

Hathaway Oona A./Shapiro Scott J., Outcasting: Enforcement in Domestic and International Law, 121 The Yale Law Journal 2011, S. 252 ff. (zit. Hathaway/Shapiro, Enforcement)

Hathaway Oona/Shapiro Scott, The Internationalist: How a Radical Plan to Outlaw War Remade the World, New York 2017 (zit. Hathaway/Shapiro, The Internationalist)

Heathcote Sarah, Necessity, in: James Crawford/Alain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 491 ff. (zit. Heathcote, Necessity)

Heathcote Sarah, State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility, in: Karine Bannelier/Théodore Christakis/Sarah Heathcote (Hrsg.), The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case, London 2012, S. 295 ff. (zit. Heathcote, State Omissions)

Heckman Kristin E./Walsh Michael J./Stech Frank J./O'Boyle Todd A./DiCato Stephen R./ Herber Audra F., Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment, 37 Computers & Security 2013, S. 72 ff.

Heintschel von Heinegg Wolff, Friedenssicherung, 14. Kapitel, in: Knut Ipsen, Völkerrecht, Volker Epping/Wolff Heintschel von Heinegg (Hrsg.), 7. Aufl., München 2018, S. 1131 ff. (zit. Heintschel von Heinegg, Friedenssicherung)

Heintschel von Heinegg Wolff, Informationskrieg und Völkerrecht: Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung, in: Volker Epping/Horst Fischer/Wolff Heintschel von Heinegg (Hrsg.), Brücken bauen und begehen: Festschrift für Knut Ipsen zum 65. Geburtstag, München 2000, S. 129 ff. (zit. Heintschel von Heinegg, Informationskrieg)

Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, in: Christian Czosseck/Rain Ottis/Katharina Ziolkowski (Hrsg.), 4th International Conference on Cyber Conflict, Tallinn 2012, S. 7 ff. (zit. Heintschel von Heinegg, Territorial Sovereignty)

Heinze Eric A., Nonstate Actors in the International Legal Order: The Israeli-Hezbollah Conflict and the Law of Self-Defense, 15 Global Governance 2009, S. 87 ff.

Henriksen Anders, The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace, 5 Journal of Cybersecurity 2019, S. 1 ff.

Herrmann Dominik/Pridöhl Henning, Basic Concepts and Models of Cybersecurity, in: Markus Christen/Bert Gordijn/Michele Loi (Hrsg.), The Ethics of Cybersecurity, Cham 2020, S. 11 ff.

Hershey Amos S., The Essentials of International Public Law, New York 1918

Hessbruegge Jan Arno, The Historical Development of the Doctrines of Attribution and Due Diligence in International Law, 36 New York University Journal of International Law and Politics 2004, S. 265 ff.

Higgins Rosalyn, Problems and Process: International Law and How We Use it, Oxford 1994

Higgins Rosalyn/Webb Philippa/Akande Dapo/Sivakumaran Sandesh/Sloan James, Oppenheim's International Law: United Nations, Oxford 2017

Hinkle Katharine C., Countermeasures in the Cyber Context: One More Thing to Worry About, 37 The Yale Journal of International Law Online 2017, S. 11 ff.

Huang Zhixiong, The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations, 14 Baltic Yearbook of International Law 2014, S. 41 ff.

Hundley Richard O./Anderson Robert H., Emerging Challenge: Security and Safety in Cyberspace, IEEE Technology and Society 1995/96, S. 19 ff.

Hurtz Simon, Was hinter dem Facebook-Ausfall steckte, Süddeutsche Zeitung vom 05.10.2021, abrufbar unter: <https://www.sueddeutsche.de/wirtschaft/facebook-whatsapp-instagram-ausfall-internet-1.5430610> (zuletzt besucht: März 2023)

Jacobs Dov, Standard of Proof and Burden of Proof, in: Göran Sluiter/Håkan Friman/Suzannah Linton et al. (Hrsg.), International Criminal Procedure: Principles and Rules, Oxford 2013, S. 1128 ff.

Jennings Robert Y., The Caroline and McLeod Cases, 32 American Journal of International Law 1938, S. 82 ff.

Jensen Eric Talbot, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38/2 Stanford Journal of International Law 2002, S. 207 ff. (Jensen, Critical National Infrastructure)

Jensen Eric Talbot, Cyber Deterrence, 26 Emory International Law Review 2012, S. 773 ff. (Jensen, Cyber Deterrence)

Jensen Eric Talbot, The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law 2017, S. 735 ff. (Jensen, Tallinn Manual 2.0)

Jensen Eric Talbot/Watts Sean, A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer, 95 Texas Law Review 2017, S. 1555 ff.

Johnson Blake/Caban Dan/Krotofil Marina/Scali Dan/Brubaker/Glyer Christopher, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, Mandiant vom 14.12.2017, abrufbar unter: <https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton> (zuletzt besucht: März 2023)

Johnson David R./Post David, Law and Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1996, S. 1367 ff.

Joyner Christopher C./Lotrionte Catherine, Information Warfare as International Coercion: Elements of a Legal Framework, 12 European Journal of International Law 2001, S. 825 ff.

Kaikobad Kaiyan Homi, Self-Defence, Enforcement Action and the Gulf Wars 1980-1988 and 1990-1991, 63 British Yearbook of International Law 1992, S. 299 ff.

Kambourakis Georgios/Kolias Constantinos/Stavrou Angelos, The Mirai Botnet and the IoT Zombie Armies, IEEE Military Communications Conference, Baltimore, 23–25 October 2017, S. 267 ff.

Kammerhofer Jörg, The Resilience of the Restrictivist Rules of Self-Defence, in: Marc Weller/Alexia Solomou/Jake William Rylatt (Hrsg.), The Oxford Handbook on the Use of Force in International Law, Oxford 2015, S. 627 ff. (zit. Kammerhofer, Restrictivist Rules)

Kammerhofer Jörg, Uncertainties of the Law on Self-Defence in the United Nations Charter, 35 Netherlands Yearbook of International Law 2004, S. 143 ff. (zit. Kammerhofer, Uncertainties)

Kammerhofer Jörg, Uncertainty in International Law: A Kelsenian Perspective, New York 2011 (zit. Kammerhofer, Kelsenian Perspective)

Kamto Maurice, The Time Factor in the Application of Countermeasures, in: James Crawford/Alain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 1169 ff.

Kanuck Sean, Sovereign Discourse on Cyber Conflict Under International Law, 88 Texas Law Review 2010, S. 1571 ff.

Katselli Elena, Countermeasures by Non-Injured States in the Law on State Responsibility, Florence Founding Conference of the European Society of International Law 2005, S. 1 ff.

Katyal Neal, Community Self-Help, 1/1 Journal of Law, Economics and Policy 2005, S. 33 ff.

Keber Tobias O./Roguski Przemysław, Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis, 49. Bd. Archiv des Völkerrechts 2011, S. 399 ff.

Kees Alexander, Responsibility of States for Private Actors, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2011

Kennedy David, Of War and Law, Princeton 2006

Kerschischnig Georg, Cyberthreats and International Law, The Hague 2012

Kesan Jay P./Hayes Carol Mullins, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 Harvard Journal of Law and Technology 2012, S. 429 ff.

Kessler Oliver/Wouter Werner, Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyber Warfare, 26 Leiden Journal of International Law 2013, S. 793 ff.

Kilovaty Ido, Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare, 5 American University National Security Law Brief 2014, S. 91 ff. (Kilovaty, Jus Ad Bellum)

Kilovaty Ido, Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information, 9 Harvard National Security Journal 2018, S. 146 ff. (Kilovaty, Doxfare)

Kilovaty Ido, Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter, Journal of Law and Cyber Warfare 2015, S. 210 ff. (Kilovaty, Economic Cyber Warfare)

Kirgis Frederic/Morrison Fred L./Norton Patrick M./Lobel Jules L./Dinstein Yoram/Magraw Daniel B., The Jurisprudence of the Court in the Nicaragua Decision, in: American Society of International Law (Hrsg.), Proceedings of the Annual Meeting, Vol. 81, 8–11 April 1987, S. 258 ff.

Knell Yolande, New Cyber Attack hits Israeli Stock Exchange and Airline, BBC News vom 16.01.2012, abrufbar unter: <https://www.bbc.com/news/world-16577184> (zuletzt besucht: März 2023)

Komov Sergei/Korotkov Sergei/Dylevski Igor, Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law, in: Kerstin Vignard (Hrsg.), UNIDIR, Disarmament Forum, ICT and International Security, Genf 2007, S. 35 ff.

Kormann Judith, Interview mit Sandra Joyce, Cyberangriffe waren früher Plan D – heute sind sie für viele Länder die erste Wahl, NZZ vom 31.03.2020

Kranz Jerzy, Die völkerrechtliche Verantwortlichkeit für die Anwendung militärischer Gewalt: Massstäbe der Zurechenbarkeit, 48. Bd. Archiv des Völkerrechts, Tübingen 2010, S. 281 ff.

Kress Claus, The International Court of Justice and the "Principle of Non-Use of Force", in: Marc Weller (Hrsg.), The Oxford Handbook of the Use of Force in International Law, Oxford 2015, S. 561 ff.

Kretzmer David, The Inherent Right to Self-Defence and Proportionality in Jus ad Bellum, 24/1, European Journal of International Law 2013, S. 235 ff.

Krieger Heike, Krieg gegen Anonymous: Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, 50. Bd. Archiv des Völkerrechts, Tübingen 2012, S. 1 ff.

Krieger Heike/Peters Anne, Due Diligence and Structural Change in the International Legal Order, in: Heike Krieger/Anne Peters/Leonhard Kreuzer (Hrsg.), Due Diligence in the International Legal Order, Oxford 2020, S. 351 ff.

Krieger Heike/Peters Anne/Kreuzer Leonhard, Due Diligence in the International Legal Order, Oxford 2020

Kunig Philip, Prohibition of Intervention, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2008

Kunz Josef L., Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations, 41 American Journal of International Law 1947, S. 872 ff.

Lahmann Henning, Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution, Cambridge 2020

Langer Marie-Astrid, Biden macht den Solarwinds-Cyberangriff zur Chefsache, NZZ vom 12.02.2021

Langner Ralph, To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve, The Langner Group, Arlington, November 2013

Lauber Jürg/Eberli Lukas, From Confrontation to Consensus: Taking Stock of the OEWG Process, in: The Hague Centre for Strategic Studies/Global Commission on the Stability of Cyberspace (Hrsg.), Cyberstability Paper Series, The Hague 2021, S. 1 ff.

Laursen Andreas, The Judgment by the International Court of Justice in the Oil Platforms Case, 73 Nordic Journal of International Law 2004, S. 135 ff. (zit. Laursen, Oil Platforms Case)

Laursen Andreas, The Use of Force and (the State of) Necessity, 37 Vanderbilt Journal of Transnational Law 2004, S. 485 ff. (zit. Laursen, Necessity)

Lauterpacht Hersch, The Function of Law in the International Community, Oxford 1933

Leben Charles, Les Contre-Mesures Inter-Étatiques et les Réactions à l'Illicite dans la Société Internationale, 28 Annuaire Fraînçais de Droit International 1982, S. 9 ff.

Lehtinen Rick/Russell Deborah/Gangemi G.T., Computer Security Basics, 2. Aufl., Sebastopol 2006

Lehto Marja, The Rise of Cyber Norms, in: Nicholas Tsagourias/Russell Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl., Cheltenham 2021, S. 32 ff.

Lesaffer Randall, Too Much History: From War as Sanction to the Sanctioning of War, in: Marc Weller (Hrsg.), The Oxford Handbook of the Use of Force in Inter-national Law, Oxford 2015, S. 35 ff.

Li Sheng, When Does Internet Denial Trigger the Right of Armed Self-Defense, 38 Yale Journal of International Law 2013, S. 179 ff.

Libicki Martin, Escalation in Cyberspace, in: Paul J. Springer (Hrsg.), Cyber Warfare: A Reference Handbook, Oxford 2015, S. 110 ff.

Lipson Howard F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, Special Report 2002, S. 1 ff.

Lipton Eric/Sanger David E./Shane Scott, The Perfect Weapon: How Russian Cyberpower Invaded the U.S., The New York Times vom 13.12.2016, abrufbar unter: <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html> (zuletzt besucht: März 2023)

Lipton Eric/Shane Scott, Democratic House Candidates Were Also Targets of Russian Hacking, The New York Times vom 13.12.2016, abrufbar unter: <https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html> (zuletzt besucht: März 2023)

Litan Avivah, Widespread APTs targeting Energy and Critical Infrastructure, Gartner Blog Network vom 02.11.2017, abrufbar unter: <https://blogs.gartner.com/avivah-litan/2017/11/02/widespread-apts-targeting-energy-and-critical-infrastruc-ture/> (zuletzt besucht: März 2023)

Lotrionte Catherine, Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law, 3/2 The Cyber Defense Review 2018, S. 73 ff.

Lu Wenlian/Xu Shouhuai/Yi Xinlei, Optimizing Active Cyber Defense, in: Sajal K. Das/Cristina Nita-Rotaru/Murat Kantarcioglu (Hrsg.), 4th International Conference on Decision and Game Theory for Security, 11–12 November 2013, Fort Worth, S. 206 ff.

Lucas George, Ethics and Cyber Warfare, The Quest for Responsible Security in the Age of Digital Warfare, Oxford 2017

Luhmann Niklas, Law as a Social System, Oxford 2004

Lundgren Björn/Möller Niklas, Defining Information Security, 25 Science and Engineering Ethics 2019, S. 419 ff.

Mačák Kubo, Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors, 21/3 Journal of Conflict and Security Law 2016, S. 405 ff.

Macdonald R. St. J., The Nicaragua Case: New Answers to Old Questions?, 127 Canadian Yearbook of International Law 1986, S. 127 ff.

Mäder Lukas, Cyberangriffe stören die europäische Versorgung mit Öl und Treibstoff – ein Ende ist nicht absehbar, NZZ vom 04.02.2022

Mäder Lukas, Das Schweizer Stromnetz ist völlig ungenügend gegen Cyberangriffe geschützt, NZZ vom 02.07.2021

Mäder Lukas, Trotz Cyberangriffen: Russland, China und die USA können sich bei der Cybersicherheit überraschend einigen, NZZ vom 28.03.2021

Mäder Lukas, Wie russische IT-Firmen mitarbeiten: Die USA legen neue Informationen zu Cyberangriffen offen, NZZ vom 16.04.2021

Mäder Lukas/Sansano Georg Hänsler, Ein Cyberangriff der Armee würde Monate oder Jahre dauern, NZZ vom 06.01.2021

Markoff John/Kramer Andrew, U.S. and Russia Differ on a Treaty for Cyberspace, The New York Times vom 27.06.2009, abrufbar unter: <https://www.nytimes.com/2009/06/28/world/28cyber.html> (zuletzt besucht: März 2023)

Maurer Tim, Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security, Discussion Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge (Massachusetts) 2011

May Larry, The Nature of War and the Idea of "Cyberwar", in: Jens David Ohlin/Kevin Govern/Claire Finkelstein (Hrsg.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford 2015, S. 3 ff.

Mazzetti Mark/Goldman Adam, The Game Will Go On as U.S. Expels Russian Diplomats, The New York Times vom 30.12.2016, <https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html> (zuletzt besucht: März 2023)

Mefford Aron, Lex Informatica: Foundations of Law on the Internet, 5 Indiana Journal of Global Legal Studies 1997/1998, S. 211 ff.

Meisner Jeffrey, Taking Down Botnets: Microsoft and the Rustock Botnet, Microsoft News vom 17.03.2011, abrufbar unter: <https://blogs.microsoft.com/blog/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet/> (zuletzt besucht: März 2023)

Middleton Alex, Stuxnet: The World's First Cyber… Boomerang?, 2 Interstate – Journal of International Affairs 2016, S. 1 ff.

Mikanagi Tomohiro, Application of the Due Diligence Principle to Cyber Operations, 97 International Law Studies 2021, S. 1019 ff.

Mikanagi Tomohiro/Mačák Kubo, Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case, 9/1 Cambridge International Law Journal 2020, S. 51 ff.

Mimran Tal/Shany Yuval, Israel, Cyberattacks and International Law, Lawfare vom 30.12.2020, abrufbar unter: <https://www.lawfareblog.com/israel-cyberattacks-and-international-law> (zuletzt besucht: März 2023)

Moret Erica/Biersteker Thomas/Giumelli Francesco/Portela Clara/Veber Marusa/Bastiat-Jarosz Dawid/Bobocea Cristian, The New Deterrent? International Sanctions Against Russia Over the Ukraine Crisis: Impacts, Costs and Further Action, Geneva 2016

Moret Erica/Pawlak Patryk, The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?, 24 European Union Institute for Security Studies 2017, S. 1 ff.

Münkler Herfried, Die neuen Kriege, 4. Aufl., Reinbek bei Hamburg 2003 und 7. Aufl., Reinbek bei Hamburg 2018

Murphy Sean D., Contemporary Practice of the United States Relating to International Law, 93 American Journal of International Law 1999, S. 161 ff.

Nakashima Ellen, Biden Administration holds Meeting on Ransomware Threats with more than 30 Nations and E.U., The Washington Post vom 14.10.2021, abrufbar unter: <https://www.washingtonpost.com/national-security/ransomware-security-threat/2021/10/14/a84f257a-2cfd-11ec-8ef6-3ca8fe943a92_story.html> (zuletzt besucht: März 2023)

Nakashima Ellen, Biden's new Cyber Czar is Pushing for Collecting Defense inside Government and out, The Washington Post vom 28.10.2021, abrufbar unter: <https://www.washingtonpost.com/national-security/inglis-national-cyber-director-plans/2021/10/27/af7da21a-373c-11ec-9bc4-86107e7b0ab1_story.html> (zuletzt besucht: März 2023)

Nakashima Ellen, Pentagon to Boost Cybersecurity Force, The Washington Post vom 27.01.2013, abrufbar unter: <https://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html> (zuletzt besucht: März 2023)

Nakashima Ellen/Rucker Philip, US Declares North Korea Carried out Massive WannaCry Cyberattack, The Washington Post vom 19.12.2017, abrufbar unter: <https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html> (zuletzt besucht: März 2023)

Nakashima Ellen/Torbati Yeganeh/Englund Will, Ransomware Attack leads to Shutdown of Major U.S. Pipeline System, The Washington Post vom 08.05.2021, abrufbar unter: <https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/> (zuletzt besucht: März 2023)

Nazario Jose, DDoS Attack Evolution, 7 Network Security 2008, S. 7 ff.

Newman Lily Hay, Hacker Lexicon: What is the Attribution Problem?, Wired vom 24.12.2016, abrufbar unter: <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/> (zuletzt besucht: März 2023)

Newman Lily Hay, Menacing Malware Shows the Dangers of Industrial System Sabotage, Wired vom 18.01.2018, abrufbar unter: <https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/> (zuletzt besucht: März 2023)

Newman Lily Hay, The Worst Hacks of the Decade, Wired vom 23.12.2019, abrufbar unter: <https://www.wired.com/story/worst-hacks-of-the-decade/> (zuletzt besucht: März 2023)

Newton Michael/May Larry, Proportionality in International Law, Oxford 2014

Nicoll Alexander, Stuxnet: Targeting Iran's Nuclear Programme, 17 The International Institute for Strategic Studies (IISS) Strategic Comments 2011, S. 1 ff.

Nolte Georg, Article 2(7), in: Bruno Simma et al. (Hrsg.), The Charter of the United Nations: A Commentary, 3. Aufl., Oxford 2012, S. 280 ff. (zit. Nolte, Article 2(7))

Nolte Georg, Multipurpose Self-Defence, Proportionality Disoriented: A Response to David Kretzmer, 24/1 European Journal of International Law 2013, S. 283 ff. (zit. Nolte, A Response to Kretzmer)

O.V., 2008 Turkish Oil Pipeline Explosion may have been Stuxnet Precursor, Homeland Security News Wire vom 17.12.2014, abrufbar unter: <http://www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor> (zuletzt besucht: März 2023)

O'Connell Mary Ellen, Cyber Security without Cyber War, 17 Journal of Conflict and Security Law 2012, S. 187 ff. (zit. O'Connell, Cyber Security)

O'Connell Mary Ellen, Lawful Self-Defense to Terrorism, 63 University of Pittsburgh Law Review 2002, S. 889 ff. (zit. O'Connell, Self-Defense)

O'Connell Mary Ellen, The Power and Purpose of International Law: Insights from the Theory and Practice of Enforcement, Oxford 2008 (zit. O'Connell, Power and Purpose)

O'Keefe Roger, Proportionality, in: James Crawford/Alain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 1157 ff.

Ochoa-Ruiz Natalia/Salamanca-Aguado Esther, Exploring the Limits of International Law relating to the Use of Force in Self-defence, 16/3 European Journal of International Law 2005, S. 499 ff.

Ohlin Jens D., The Doctrine of Legitimate Defense, 91 International Legal Studies 2015, S. 119 ff. (zit. Ohlin, Legitimate Defense)

Ohlin Jens D., The Unwilling and Unable Test for Extraterritorial Defensive Force, Why Force is Permitted against the Territorial State, in: Claus Kress/Robert Lawless (Hrsg.), Necessity and Proportionality in International Peace and Security Law, Lieber Studies, Vol. 5, Oxford 2021, S. 113 ff. (zit. Ohlin, Unwilling and Unable)

Orakhelashvili Alexander, Current Developments: Oil Platforms (Islamic Republic of Iran v United States of America), Merits, Judgment of 6 November 2003, 53/3 International & Comparative Law Quarterly 2004, S. 753 ff.

Ossoff William, Hacking the Domaine Reserve: The Rule of Non-Intervention and Political Interference in Cyberspace, 62 Harvard International Law Journal 2021, S. 295 ff.

Owens William A./Dam Kenneth W./Lin Herbert S., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, Washington D.C. 2009

Palchetti Paolo, De Facto Organs of a State, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2017

Passeri Paolo, Cyber Attacks Statistics, Hackmageddon vom 16.02.23, abrufbar unter: <https://www.hackmageddon.com/2023/02/16/january-2023-cyber-attacks-statistics/> (zuletzt besucht: März 2023)

Patterson Dan, Cyberweapons are now in Play: From US Sabotage of a North Korean Missile Test to Hacked Emergency Sirens in Dallas, Tech Republic vom 01.06.2017, abrufbar unter: <https://www.techrepublic.com/article/cyberweapons-are-now-in-play-from-us-sabotage-of-a-north-korean-missile-test-to-hacked-emergency/> (zuletzt besucht: März 2023)

Patterson Steven Max, This Mirai Malware Vaccine Could Protect Insecure IoT Devices, Networkworld vom 25.08.2017, abrufbar unter: <https://www.networkworld.com/article/3219851/this-mirai-malware-vaccine-could-protect-insecure-iot-devices.html#tk.rss_all> (zuletzt besucht: März 2023)

Paul Kari et al., SolarWinds Hack was Work of "at least 1'000 Engineers", Tech Executives tell Senate, The Guardian vom 24.02.2021, abrufbar unter: <https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft> (zuletzt besucht: März 2023)

Perez Evan/Diaz Daniella, White House Announces Retaliation Against Russia: Sanction, Ejecting Diplomats, CNN vom 03.01.2017, abrufbar unter: <https://edition.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html> (zuletzt besucht: März 2023)

Perlroth Nicole/Shane Scott, In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc, The New York Times vom 25.05.2019, abrufbar unter: <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html> (zuletzt besucht: März 2023)

Peters Anne/Krieger Heike/Kreuzer Leonhard, Due Diligence in the International Legal Order, Dissecting the Leitmotif of Current Accountability Debates, in: Heike Krieger/Anne Peters/Leonhard Kreuzer (Hrsg.), Due Diligence in the International Legal Order, Oxford 2020, S. 1 ff. (zit. Peters/Krieger/Kreuzer, Dissecting the Leitmotif)

Peters Anne/Krieger Heike/Kreuzer Leonhard, Due Diligence: The Risky Risk Management Tool in International Law, 9/2 Cambridge International Law Journal 2020, S. 121 ff. (zit. Peters/Krieger/Kreuzer, Risk Management Tool)

Peters Anne/Petrig Anna, Völkerrecht, 5. Aufl., Zürich 2020

Petkis Stephen, Rethinking Proportionality in the Cyber Context, 47/4 Georgetown Journal of International Law 2016, S. 1431 ff.

Phillips Ian/Isachenkov Vladimir, Putin: Russia Doesn't Hack but "Patriotic" Individuals Might, U.S. News vom 01.06.2017, abrufbar unter: <https://www.usnews.com/news/world/articles/2017-06-01/putin-russian-state-has-never-been-involved-in-hacking> (zuletzt besucht: März 2023)

Pierrot Oliver, Computerviren, in: Ernst Stefan et al. (Hrsg.), Hacker, Cracker und Computerviren, Recht und Praxis der Informationssicherheit, Köln 2004, S. 29 ff.

Pierrot Oliver, Hacker, in: Ernst Stefan et al. (Hrsg.), Hacker, Cracker und Computerviren, Recht und Praxis der Informationssicherheit, Köln 2004, S. 1 ff.

Poroshyn Roman, Stuxnet: The True Story of Hunt and Evolution, Denver 2013

Raab Dominic, "Armed Attack" after the Oil Platforms Case, 17 Leiden Journal of International Law 2004, S. 719 ff.

Raltchev Christo C., Cybergewalt, Bestandesaufnahme und grundlegende Probleme aus völkerrechtlicher Sicht, Fribourg 2013

Randelzhofer Albrecht/Dörr Oliver, Article 2(4), in: Bruno Simma et al. (Hrsg.), The Charter of the United Nations: A Commentary, 3. Aufl., Oxford 2012, S. 200 ff.

Randelzhofer Albrecht/Nolte Georg, Article 51, in: Bruno Simma et al. (Hrsg.), The Charter of the United Nations: A Commentary, 3. Aufl., Oxford 2012, S. 1397 ff.

Rawls John, The Law of Peoples, with "The Idea of Public Reason Revisited", Cambridge 1999

Reisman Michael W., Allocating Competences to use Coercion in the post Cold-War World, Practises, Conditions, and Prospects, in: Lori Fisler Damrosch/David J. Scheffer (Hrsg.), Law and Force in the New International Order, New York 1991, S. 26 ff.

Rid Thomas, Cyberwar and Peace, Hacking Can Reduce Real-World Violence, 92/6 Foreign Affairs 2013, S. 77 ff. (zit. Rid, Cyberwar and Peace)

Rid Thomas, Cyberwar Will Not Take Place, London 2013 (zit. Rid, Cyberwar)

Riddell Anna/Plant Brendan, Evidence Before the International Court of Justice, London 2009

Riphagen Willem, Fourth Report on the Content, Forms and Degrees of International Responsibility (Doc. A/CN.4/366 and Add.1), II(1) Yearbook of the International Law Commission 1983, S. 3 ff. (zit. Riphagen, Fourth Report)

Riphagen Willem, Preliminary Report on the Content, Forms and Degrees of International Responsibility (Doc. A/CN.4/330), II(1) Yearbook of the International Law Commission 1980, S. 107 ff. (zit. Riphagen, Preliminary Report)

Roberts Anthea/Sivakumaran Sandesh, The Theory and Reality of the Sources of International Law, in: Malcolm D. Evans (Hrsg.), International Law, 5. Aufl., Oxford 2018, S. 89 ff.

Roberts Dan, Obama Imposes New Sanctions Against North Korea in Response to Sony Hack, The Guardian vom 02.01.2015, abrufbar unter: <https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview> (zuletzt besucht: März 2023)

Roberts Paul, New Variant of Blaster Worm »Fixes« Infected Systems, Computer-Weekly vom 19.08.2003, abrufbar unter: <https://www.computerworld.com/article/2571419/new-variant-of-blaster-worm-fixes-infected-systems.html> (zuletzt besucht: März 2023)

Robertson Jordan/Riley Michael, Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era, Bloomberg News vom 10.12.2014, abrufbar unter: <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar> (zuletzt besucht: März 2023)

Roguski Przemysław, Application of International Law to Cyber Operations: A Comparative Analysis of States' Views, The Hague Program for Cyber Norms Policy Brief, The Hague 2020

Rõigas Henry/Minárik Tomáš, 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law, CCDCOE Incyder News vom 31.08.2015, abrufbar unter: <https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/> (zuletzt besucht: März 2023)

Roscini Marco, Cyber Operations and the Use of Force in International Law, Oxford 2014 (zit. Roscini, Cyber Operations)

Roscini Marco, Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, in: Jens David Ohlin/David Govern/Claire Finkelstein (Hrsg.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford 2015, S. 215 ff. (zit. Roscini, Evidentiary Issues)

Roscini Marco, World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force, 14 Max Planck Yearbook of United Nations Law 2010, S. 85 ff. (zit. Roscini, World Wide Warfare)

Rosenzweig Paul, Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World, Santa Barbara 2013

Rüesch Andreas, Hackerangriff auf die USA: Als Vergeltung verhängt Washington Sanktionen und weist russische Diplomaten aus, NZZ vom 15.04.2021

Ruys Tom, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge 2010

Sabbagh Dan, UK unveils National Cyber Force of Hackers to Target foes Digitally, The Guardian vom 19.11.2020, abrufbar unter: <https://www.theguardian.com/technology/2020/nov/19/uk-unveils-national-cyber-force-of-hackers-to-target-foes-digitally> (zuletzt besucht: März 2023)

Sanger David E., Confront and Conceal, London 2012

Sanger David E./Perlroth Nicole, FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State, The New York Times vom 08.12.2020, abrufbar unter: <https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html> (zuletzt besucht: März 2023)

Sanger David E./Shane Scott, Russian Hackers Acted to Aid Trump in Election, U.S. Says, The New York Times vom 09.12.2016, abrufbar unter: <https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html> (zuletzt besucht: März 2023)

Sapiro Miriam, Iraq: The Shifting Sands of Pre-Emptive Self-Defence, 97/3 American Journal of International Law 2003, S. 599 ff.

Schachter Oscar, Dispute Settlement and Countermeasures in the International Law Commission, 88/3 American Journal of International Law 1994, S. 471 ff. (zit. Schachter, Dispute Settlement and Countermeasures)

Schachter Oscar, In Defense of International Rules on the Use of Force, 53 University of Chicago Law Review 1986, S. 113 ff. (zit. Schachter, In Defense of International Rules)

Schachter Oscar, International Law in Theory and Practice, Boston 1991 (zit. Schachter, International Law)

Schachter Oscar, Self-Defense and the Rule of Law, 83 American Journal of International Law 1989, S. 259 ff. (zit. Schachter, Rule of Law)

SCHACHTER OSCAR, The Right of States to Use Armed Force, 82/5 Michigan Law Review 1984, S. 1620 ff. (zit. SCHACHTER, Armed Force)

SCHELLING THOMAS, The Strategy of Conflict, Cambridge (Massachusetts) 1997

SCHMITT MICHAEL N. (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge 2013 (zit. Tallinn Manual 1.0)

SCHMITT MICHAEL N. (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Operations, 2. Aufl., Cambridge 2017 (zit. Tallinn Manual 2.0)

SCHMITT MICHAEL N., "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law, 54 Virginia Journal of International Law 2014, S. 697 ff. (zit. SCHMITT, Countermeasures Response Option)

SCHMITT MICHAEL N., "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, 19 Chicago Journal of International Law 2018, S. 30 ff. (zit. SCHMITT, Cyber Election Meddling)

SCHMITT MICHAEL N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Columbia Journal of Transnational Law 1999, S. 885 ff. (zit. SCHMITT, Computer Network Attack)

SCHMITT MICHAEL N., Cyber Activities and the Law of Countermeasures, in: Katharina Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, Tallinn 2013, S. 659 ff. (zit. SCHMITT, Law of Countermeasures)

SCHMITT MICHAEL N., Estonia Speaks Out on Key Rules for Cyberspace, Just Security vom 10.06.2019, abrufbar unter: <https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/> (zuletzt besucht: März 2023)

SCHMITT MICHAEL N., Grey Zones in the International Law of Cyberspace, 42/2 The Yale Journal of International Law Online 2017, S. 1 ff. (zit. SCHMITT, Grey Zones)

SCHMITT MICHAEL N., International Law and Cyber Attacks: Sony v. North Korea, Just Security vom 17.12.2014, abrufbar unter: <https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/> (zuletzt besucht: März 2023)

SCHMITT MICHAEL N., U.S. Security Strategies: A Legal Assessment, 27 Harvard Journal of Law and Public Policy 2004, S. 737 ff. (zit. SCHMITT, U.S. Security Strategies)

SCHMITT MICHAEL N./PITTS CHRISTOPHER M., Cyber Countermeasures and Effects on Third Parties: The International Legal Regime, 14 Baltic Yearbook of International Law 2014, S. 1 ff.

SCHMITT MICHAEL/VIHUL LIIS, International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, Just Security vom 30.06.2017, abrufbar unter: <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> (zuletzt besucht: März 2023)

Schröder Meinhard, Verantwortlichkeit, Völkerstrafrecht, Streitbeilegung und Sanktionen, in: Wolfgang Graf Vitzthum/Alexander Proelß (Hrsg.), Völkerrecht, 8. Aufl., Berlin 2019, S. 691 ff.

Schulze Sven-Hendrik, Cyber-„War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015

Schürpf Thomas (tsf), Hacker attackieren den Flughafen-Dienstleister Swissport, NZZ vom 04.02.2022

Seibert-Fohr Anja, Die völkerrechtliche Verantwortung des Staats für das Handeln von Privaten: Bedarf nach Neuorientierung?, 73 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 2013, S. 37 ff.

Shackelford Scott J./Andres Richard B., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, 42 Georgetown Journal of International Law 2011, S. 971 ff.

Sharp Walter Gary, Cyberspace and the Use of Force, Falls Church 1999

Shaw Malcolm N., International Law, 9. Aufl., Cambridge 2021

Sicilianos Linos-Alexander, Countermeasures in Response to Grave Violations of Obligations Owed to the International Community, in: James Crawford/Allain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 1137 ff. (zit. Sicilianos, Countermeasures)

Sicilianos Linos-Alexander, The Relationship Between Reprisals and Denunciation or Suspension of a Treaty, 4 European Journal of International Law 1993, S. 341 ff. (zit. Sicilianos, Reprisals and Denunciation)

Silver Daniel B., Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, in: Michael N. Schmitt/Brian T. O'Donnell (Hrsg.), Computer Network Attack and International Law, Newport 2002, S. 73 ff.

Simonite Tom, Stuxnet Tricks Copied by Computer Criminals, MIT Technology Review vom 19.09.2012, abrufbar unter: <https://www.technologyreview.com/2012/09/19/115189/stuxnet-tricks-copied-by-computer-criminals/> (zuletzt besucht: März 2023)

Simonite Tom, Welcome to the Malware-Industrial Complex, MIT Technology Review vom 13.02.2013, abrufbar unter: <https://www.technologyreview.com/2013/02/13/180063/welcome-to-the-malware-industrial-complex/> (zuletzt besucht: März 2023)

Singer P.W., Stuxnet and its Hidden Lessons on the Ethics of Cyberweapons, 47/1 Case Western Reserve Journal of International Law 2015, S. 79 ff.

Singer P.W./Friedman Allan, Cybersecurity and Cyberwar, What Everyone Needs to Know, Oxford 2014

Sklerov Matthew J., Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 Military Law Review 2009, S. 1 ff.

Sloane Robert D., On the Use and Abuse of Necessity in the Law of State Responsibility, 106 American Journal of International Law 2021, S. 447 ff. (zit. Sloane, Necessity)

Sloane Robert D., The Cost of Conflation: Preserving the Dualism of Jus ad Bellum and Jus in Bello in the Contemporary Law of War, 34 The Yale Journal of International Law 2009, S. 47 ff. (zit. Sloane, Cost of Conflation)

Sofaer Abraham D., International Law and the Use of Force, American Society of International Law (Hrsg.), Proceedings of Annual Meeting, Vol. 82, 20.–23.4.1988, S. 420 ff.

Soldatov Andrei/Borogan Irina, Russia's Approach to Cyber: The Best Defence is a Good Offence, in: Nicu Popescu/Stanislav Secrieru (Hrsg.), Hacks, Leaks and Disruptions: Russian Cyber Strategies, European Union Institute for Security Studies (ISSUE) Chaillot Paper No. 148, Paris 2018, S. 15 ff.

Sparks Tom/Peters Anne, Transparency Procedures, in: Lavanya Rajamani/Jaqueline Peel (Hrsg.), Oxford Handbook of International Environmental Law, 2. Aufl., Oxford 2021, S. 904 ff.

Springer Paul J., Cyber Warfare, A Reference Handbook, Santa Barbara 2015

Sreenivasa Rao Pemmaraju, Countermeasures in International Law: The Contribution of the International Law Commission, Editoriale Scientifica (Hrsg.), Giovanni Battaglini/Paolo Benvenuti/Antonio Cassese et al. (comitato promotore), Studi di diritto internazionale in onore di Gaetano Arangio-Ruiz, Vol. 2, Napoli 2004, S. 853 ff.

Starski Paulina, Right to Self-Defense, Attribution and the Non-State Actor: Birth of the "Unable or Unwilling" Standard?, 75 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 2015, S. 456 ff.

Stein Torsten/Marauhn Thilo, Völkerrechtliche Aspekte von Informationsoperationen, 60 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 2000, S. 1 ff.

Steinvorth Daniel, Nato schliesst Afghanistan-Kapitel ab, NZZ vom 14.04.2021

Stern Brigitte, The Elements of an Internationally Wrongful Act, in: James Crawford/Allain Pellet/Simon Olleson (Hrsg.), The Law of International Responsibility, Oxford Commentaries on International Law, Oxford 2010, S. 193 ff.

Stiennon Richard, Surviving Cyber War, Lanham 2010

Swanson Lesley, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, 32 Loyola of Los Angeles International and Comparative Law Review 2010, S. 303 ff.

Taft William H., Self-Defense and the Oil Platform Decision, 29 The Yale Journal of International Law 2004, S. 295 ff.

Tams Christian J., Enforcing Obligations »Erga Omnes« in International Law, Cambridge 2005 (zit. Tams, Enforcing Obligations)

Tams Christian J., The Use of Force against Terrorists, 20 European Journal of International Law 2009, S. 359 ff. (zit. Tams, Use of Force)

Tanzi Attila, Is Damage a Distinct Condition for the Existence of an Internationally Wrongful Act?, in: Marina Spinedi/Bruno Simma (Hrsg.), United Nations Codification of State Responsibility, New York 1987, S. 1 ff.

Tavares Pedro, The most dangerous vulnerabilities exploited in 2022, Infosec vom 17.08.2022, abrufbar unter: <https://resources.infosecinstitute.com/topic/most-dangerous-vulnerabilities-exploited/> (zuletzt besucht: März 2023)

Teitelbaum Ruth, Recent Fact-Finding Developments at the International Court of Justice, 6 The Law and Practice of International Courts and Tribunals 2007, S. 119 ff.

Tibori-Szabó Kinga, The "Unwilling or Unable" Test and the Law of Self-Defence, in: C. Paulussen et al. (Hrsg.), Fundamental Rights in International and European Law, The Hague 2016, S. 73 ff.

Tikk Eneken/Hovhannisyan Kristine/Kerttunen Mika/Salminen Mirva, Cyber Conflict Factbook, Effect-Creating State-on-State Cyber Operations, Tallinn 2019

Tikk Eneken/Kaska Kadri/Vihul Liis, International Cyber Incidents: Legal Considerations, Tallinn 2010

Tikk-Ringas Eneken, Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012, ICT4Peace Policy Brief, Geneva 2012

Trapp Kimberley N., Back to Basics: Necessity, Proportionality, and the Right of Self-Defence Against Non-State Terrorist Actors, 56 International and Comparative Law Quarterly 2007, S. 141 ff.

Tsagourias Nicholas, Cyber Attacks, Self-defence and the Problem of Attribution, 17 Journal of Conflict and Security Law 2012, S. 229 ff.

Van Steenberghe Raphaël, The Law against War or *Jus contra Bellum*: A New Terminology for a Conservative View on the Use of Force?, 24/3 Leiden Journal of International Law 2011, S. 747 ff.

von Carlowitz Leopold, Interpreting Self-Defense Restrictively: The World Court in the Oil Platforms Case, 23 Sicherheit und Frieden 2005, S. 79 ff.

Wakefield Jane, Tax Software Blamed for Cyber-Attack Spread, BBC News vom 28.06.2017, abrufbar unter: <https://www.bbc.com/news/technology-40428967> (zuletzt besucht: März 2023)

Waldron Jeremy, The Rule of Law, The Stanford Encyclopedia of Philosophy, Sommer 2020 Edition, abrufbar unter <https://plato.stanford.edu/archives/sum2020/entries/rule-of-law/> (zuletzt besucht: März 2023)

Walter Christian, Cyber Security als Herausforderung für das Völkerrecht, Heft 14/70 Juristenzeitung 2015, S. 685 ff.

Warell Helen, National Cyber Force will Target UK Adversaries Online, Financial Times vom 19.11.2020, abrufbar unter: <https://www.ft.com/content/a41b34e7-a8fc-4bce-92e4-508cd1c83ba9> (zuletzt besucht: März 2023)

Watts Sean, International Law and Proposed U.S. Responses to the D.N.C. Hack, Just Security vom 14.10.2016, abrufbar unter: <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/> (zuletzt besucht: März 2023)

Watts Sean, Low-Intensity Cyber Operations and the Principle of Non-Intervention, in: Jens David Ohlin/Kevin Govern/Claire Finkelstein (Hrsg.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford 2015, S. 249 ff.

Waxman Matthew C., Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 The Yale Journal of International Law 2011, S. 421 ff. (zit. Waxman, Cyber-Attacks)

Waxman Matthew C., The Use of Force Against States that *Might* Have Weapons of Mass Destruction, 31 Michigan Journal of International Law 2009, S. 1 ff. (zit. Waxman, States that *Might* Have Weapons of Mass Destruction)

Weekes Barbara/Tikk-Ringas Eneken, Cyber Security Affairs: Global and Regional Processes, Agendas and Instruments, ICT4Peace Policy Brief, Geneva 2013

Weisburd Mark, The Use of Force: The Practice of States since World War II, Pennsylvania 1997

Wheatley Steven, Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about "Coercion", 31 Duke Journal of Comparative and International Law 2020, S. 161 ff.

White Nigel D./Abass Ademola, Countermeasures and Sanctions, in: Malcolm D. Evans (Hrsg.), International Law, 5. Aufl., Oxford 2018, S. 521 ff.

Wicker Christian, The Concepts of Proportionality and State Crimes in International Law, in: Gilbert Gornig (Hrsg.), Schriften zum internationalen und zum öffentlichen Recht 2006, S. 1 ff.

Wilmshurst Elizabeth et al., The Chatham House Principles of International Law on the Use of Force in Self-Defence, 55/4 International and Comparative Law Quarterly 2006, S. 963 ff.

Wingfield Thomas, The Law of Information Conflict: National Security Law in Cyberspace, Virginia 2000

Winkler Peter, Die USA verhängen Strafmassnahmen gegen Russland, NZZ vom 16.04.2021

Wolf Joachim, Die Haftung der Staaten für Privatpersonen nach Völkerrecht, Berlin 1997

Wolfendale Jessica, Defining War, in: Michael Gross/Tamar Meisels (Hrsg.), Soft War: The Ethics of Unarmed Conflict, Cambridge 2016, S. 16 ff.

Woltag Johann-Christiph, Cyber Warfare, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2015

Woltag Johann-Christoph, Cyber Warfare, Military Cross-Border Computer Network Operations under International Law, Cambridge 2014

Zegart Amy, Cyberwar, TED vom 29.06.2015, abrufbar unter: <https://www.youtube.com/watch?v=JSWPoeBLFyQ> (zuletzt besucht: März 2023)

Zemanek Karl, Armed Attack, in: Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedias of Public International Law (MPEPIL), Oxford 2013

Zemanek Karl, Schuld- und Erfolgshaftung im Entwurf der Völkerrechtskommission über Staatenverantwortlichkeit, in: Emanuel Diez/Jean Monnier/Jörg P. Müller/Heinrich Reimann/Luzius Wildhaber (Hrsg.), Festschrift für Rudolf Bindschedler zum 65. Geburtstag am 8. Juli 1980, Bern 1980, S. 315 ff. (zit. Zemanek, Schuld- und Erfolgshaftung)

Zemanek Karl, The Unilateral Enforcement of International Obligations, 47 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 1987, S. 32 ff. (zit. Zemanek, Unilateral Enforcement)

Zetter Kim, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York 2014

Ziga Denis, Just-In-Time und Just-In-Sequence – moderne Fertigungsabläufe und Resilienz, in: Andreas H. Karsten/Stefan Vosschmidt (Hrsg.), Resilienz und kritische Infrastrukturen: Aufrechterhaltung von Versorgungsstrukturen im Krisenfall, Stuttgart 2019, S. 127 ff.

Zoller Elisabeth, Peacetime Unilateral Remedies: An Analysis of Countermeasures, New York 1984

Zwitter Andrej, The Rule of Law in Times of Crisis: A Legal Theory on the State of Emergency in Liberal Democracy, 98 Archives for Philosophy of Law and Social Philosophy 2012, S. 95 ff.

Materialienverzeichnis

Advisory Council on International Affairs, Cyber Warfare, No. 77, Advisory Committee on Issues of Public International Law, No. 22, Dezember 2011, abrufbar unter: <https://cyberwar.nl/d/20120426_cavv-advies-nr-22-digitale-oorlogsvoering-en.pdf> (zuletzt besucht: März 2023) (zit. Advisory Council on International Affairs 2011)

Bundesamt für Bevölkerungsschutz, Die kritischen Infrastrukturen, abrufbar unter: <https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html> (zuletzt besucht: Mai 2023) (zit. Bundesamt für Bevölkerungsschutz, kritische Infrastrukturen)

Bundesamt für Statistik, Internetnutzung, abrufbar unter: <https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/internetnutzung.html> (zuletzt besucht: März 2023) (zit. Bundesamt für Statistik, Internetnutzung 1997–2021)

Cartwright James E., Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories, Joint Terminology for Cyberspace Operations, November 2010, abrufbar unter <https://info.publicintelligence.net/DoD-JointCyberTerms.pdf> (zuletzt besucht: März 2023) (zit. U.S. Joint Chiefs of Staff, Terminology for Cyberspace 2010)

CCDCOE, Israeli Attack against Hamas Cyber Headquarters in Gaza (2019), Discussion, abrufbar unter: <https://cyberlaw.ccdcoe.org/wiki/Israeli_attack_against_Hamas_cyber_headquarters_in_Gaza_(2019)> (zuletzt besucht: März 2023) (zit. CCDCOE, Israeli Attack against Hamas Cyber Headquarters in Gaza 2019)

Clinton William J., Letter to Congressional Leaders Reporting on Military Action Against Terrorist Sites in Afghanistan and Sudan, 34 Weekly Compilation of Presidential Documents, 21.08.1998, S. 1650 f., abrufbar unter: <https://www.govinfo.gov/content/pkg/WCPD-1998-08-31/pdf/WCPD-1998-08-31-Pg1650-2.pdf> (zuletzt besucht: März 2023) (zit. Clinton, Letter to Congressional Leaders vom 21.08.1998)

Cybersecurity and Infrastructure Security Agency (CISA), Cyber Infrastructure, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, Alert TA17-293A, zuletzt revidiert: 15.03.2018, abrufbar unter: <https://www.us-cert.gov/ncas/alerts/TA17-293A> (zuletzt besucht: März 2023) (zit. CISA, Alert TA17-293A, 2017)

Cybersecurity and Infrastructure Security Agency (CISA), Cyber Infrastructure, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, Alert TA18-074A, zuletzt revidiert: 16.03.2018, abrufbar unter: <https://www.us-cert.gov/ncas/alerts/TA18-074A> (zuletzt besucht: März 2023) (zit. CISA, Alert TA18-074A, 2018)

Der Bundesrat, Bundesrat verabschiedet Botschaft zur Stärkung der Cyber-Defence der Armee, Medienmitteilung vom 01.09.2021, abrufbar unter: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84925.html> (zuletzt besucht: März 2023) (zit. Der Bundesrat, Medienmitteilung vom 01.09.2021)

Der Bundesrat, Die Sicherheitspolitik der Schweiz, Bericht des Bundesrates, Entwurf vom 14.04.2021, abrufbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/66420.pdf> (zuletzt besucht: März 2023) (zit. Der Bundesrat, Sicherheitspolitischer Bericht vom 14.04.2021)

Der Bundesrat, Kommando Cyber der Armee: Bundesrat fällt personelle Entscheide, Medienmitteilung vom 31.03.2021, abrufbar unter: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-82928.html> (zuletzt besucht: März 2023) (zit. Der Bundesrat, Medienmitteilung vom 31.03.2021)

Eidgenössisches Justiz- und Polizeidepartement, Bundesamt für Justiz (BJ) /Eidgenössisches Departement für auswärtige Angelegenheiten, Direktion für Völkerrecht (DV), Gutachten über Rechtsgrundlagen für Computernetzwerkoperationen durch Dienststellen des VBS, Gutachten vom 10.03.2009, S. 141 ff. (zit. BJ/DV, Gutachten vom 10.03.2009)

Europäischer Rat, Böswillige Cyberangriffe: EU-Sanktionen gegen zwei Personen und eine Einrichtung wegen Hackerangriff auf den Bundestag 2015, Pressemitteilung vom 22.10.2020, abrufbar unter: <https://www.consilium.europa.eu/de/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/> (zuletzt besucht: März 2023) (zit. Europäischer Rat, Pressemitteilung vom 22.10.2020)

Europäischer Rat, Cyberangriffe: Rat kann jetzt Sanktionen verhängen, Pressemitteilung vom 17.05.2019, abrufbar unter: <https://www.consilium.europa.eu/de/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/> (zuletzt besucht: März 2023) (zit. Europäischer Rat, Pressemitteilung vom 17.05.2019)

Europäischer Rat, Cybersicherheit: Wie die EU Cyberbedrohungen begegnet, Überblick, zuletzt überprüft: 04.01.2022, abrufbar unter <https://www.consilium.europa.eu/de/policies/cybersecurity/> (zuletzt besucht: März 2023) (zit. Europäischer Rat, Cybersicherheit 2022)

Europäischer Rat, EU verhängt erstmals Sanktionen als Reaktion auf Cyberangriffe, Pressemitteilung vom 30.07.2020, abrufbar unter: <https://www.consilium.europa.eu/de/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/> (zuletzt besucht: März 2023) (zit. Europäischer Rat, Pressemitteilung vom 30.07.2020)

European Union Agency for Cybersecurity (ENISA), Glossary, Zero-Day, abrufbar unter: <https://www.enisa.europa.eu/topics/incident-response/glossary/zero-day> (zuletzt besucht: März 2023) (zit. ENISA, Glossary, Zero-Day (Stand 2023))

Eurostat, Individuals Internet Use, abrufbar unter: <https://ec.europa.eu/eurostat/databrowser/view/tin00028/default/table?lang=en> (zuletzt besucht: März 2023) (zit. Eurostat, Individuals Internet Use 2023)

France et al., The Paris Call for Trust and Security in Cyberspace, 11.12.2018, abrufbar unter <https://pariscall.international/en/> (zuletzt besucht: März 2023) (zit. Paris Call 2018)

Institute de Droit Internationale, Present Problems of the Use of Armed Force in International Law, Santiago Session, 10th Commission, 27.10.2007, abrufbar unter: <https://www.idi-iil.org/app/uploads/2017/06/2007_san_02_en.pdf> (zuletzt besucht: März 2023) (zit. Institute de Droit Internationale, Resolution on Self-Defense 2007)

International Committee of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report, 32nd International Conference, 8–10 December 2015, abrufbar unter: <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts> (zuletzt besucht: März 2023) (zit. ICRC Report 2015)

International Law Association Study Group, Due Diligence in International Law, Second Report by Tim Stephens (Rapporteur) and Duncan French (Chair), 20 July 2016, abrufbar unter: <https://www.ila-hq.org/index.php/study-groups> (zuletzt besucht: März 2023) (zit. ILA Study Group on Due Diligence 2016)

International Law Commission, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities with Commentaries; angenommen von der Völkerrechtskommission (ILC) auf ihrer 53. Sitzung (2001), aufgenommen von der Generalversammlung der Vereinten Nationen auf ihrer 56. Tagung (2001) in Resolution 56/10 (zit. ILC, Draft Articles on Prevention of Transboundary Harm (2001))

Kaljulaid Kersti, Keynote Address by H.E. Kersti Kaljulaid, President of the Republic of Estonia, CyCon 2019 (zit. Kaljulaid, Eröffnungsrede CyCon 2019)

Nationales Zentrum für Cybersicherheit (NCSC), Glossar, 1×1 der digitalen Schädlinge und Cyberangriffe, abrufbar unter: <https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/bundesinterne-kampagnen/glossar-einmal-eins.html#736118159> (zuletzt besucht: März 2023) (zit. NCSC, Glossar)

Nationales Zentrum für Cybersicherheit (NCSC), Massnahmen zum Schutz vor DDoS-Angriffen, abrufbar unter: <https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html> (zuletzt besucht: März 2023) (zit. NCSC, Measures to Counter DDoS Attacks)

NATO, Wales Summit Declaration vom 05.09.2014, abrufbar unter: <https://www.nato.int/cps/en/natohq/official_texts_112964.htm> (zuletzt besucht: März 2023) (zit. NATO, Wales Summit Declaration vom 05.09.2014)

Office of the Director of National Intelligence, Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent US Elections, The Analytic Process and Cyber Incident Attribution vom 06.01.2017, abrufbar unter: <https://www.dni.gov/files/documents/ICA_2017_01.pdf> (zuletzt besucht: März 2023) (zit. Intelligence Community Assessment vom 06.01.2017)

Prime Minister Boris Johnson (PM), Oral Statement to the House on the Integrated Review vom 19.11.2020, abrufbar unter: <https://www.gov.uk/government/speeches/pm-statement-to-the-house-on-the-integrated-review-19-november-2020> (zuletzt besucht: März 2023) (zit. PM, Oral Statement to Parliament vom 19.11.2020)

Rodríguez Miguel, Representative of Cuba, Declaration at the Final session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, 23.06.2017, abrufbar unter: <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf> (zuletzt besucht: März 2023) (zit. Rodríguez, Deklaration vom 23.06.2017)

Shanghai Cooperation Organization, Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st Plenary Meeting vom 02.12.2008, abrufbar unter: <https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf> (zuletzt besucht: März 2023) (zit. SCO-Übereinkommen)

The White House, Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment, Statements and Releases vom 29.12.2016, abrufbar unter: <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and> (zuletzt besucht: März 2023) (zit. The White House, Statements and Releases vom 29.12.2016)

The White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government, Statements and Releases vom 15.04.2021, abrufbar unter: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> (zuletzt besucht: März 2023) (zit. The White House, Statements and Releases vom 15.04.2021)

The White House, Interim National Security Strategic Guidance, March 2021, abrufbar unter: <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf> (zuletzt besucht: März 2023) (zit. The White House, Interim National Security Strategic Guidance 2021)

The White House, National Cyber Strategy of the United States of America, September 2018, abrufbar unter: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (zuletzt besucht: März 2023) (zit. U.S. National Cyber Strategy 2018)

U.S. Congress, National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81, 31.12.2011, abrufbar unter: <https://www.congress.gov/112/plaws/publ81/PLAW-112publ81.pdf> (zuletzt besucht: März 2023) (zit. U.S. National Defense Authorization Act for Fiscal Year 2012)

U.S. Cyber Command Public Affairs, The Cutting Edge of Defense, News vom 10.09.2020, abrufbar unter: <https://www.cybercom.mil/Media/News/Article/2342894/the-cutting-edge-of-defense/> (zuletzt besucht: März 2023) (zit. U.S. Cyber Command Public Affairs, News vom 10.09.2020)

U.S. Department of Defense Strategy for Operating in Cyberspace, July 2011, abrufbar unter: <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf> (zuletzt besucht: März 2023) (zit. U.S. DoD Cyber Strategy 2011)

U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02 vom 08.11.2010; geändert am 15.02.2016, abrufbar unter: <https://irp.fas.org/doddir/dod/jp1_02.pdf> (zuletzt besucht: März 2023) (zit. U.S. DoD, Dictionary of Military and Associated Terms 2016)

U.S. Department of Defense, Dictionary of Military and Associated Terms, November 2021, abrufbar unter: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> (zuletzt besucht: März 2023) (zit. U.S. DoD, Dictionary of Military and Associated Terms 2021)

U.S. Department of Defense, Summary Department of Defense Cyber Strategy 2018, abrufbar unter: <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF> (zuletzt besucht: März 2023) (zit. U.S. DoD Cyber Strategy Summary 2018)

U.S. Department of Homeland Security, Topics, Cybersecurity, Homepage, zuletzt aktualisiert: 22.04.2022, abrufbar unter: <https://www.dhs.gov/topic/cybersecurity> (zuletzt besucht: Mai 2023) (zit. U.S. Homeland Security, Cybersecurity, Homepage)

U.S. Federal Register, Presidential Documents, Vol. 86, No. 73, Executive Order 14024 vom 15.04.2021, Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation, abrufbar unter: <https://home.treasury.gov/system/files/126/russian_harmful_for_act_eo.pdf> (zuletzt besucht: März 2023) (zit. Executive Order 14024 vom 15.04.2021)

U.S. International Strategy for Cyberspace 2011, Prosperity, Security, and Openness in a Networked World, May 2011, abrufbar unter: <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> (zuletzt besucht: März 2023) (zit. U.S. International Strategy for Cyberspace 2011)

U.S. Joint Chiefs of Staff, DoD Terminology Program, abrufbar unter: <https://www.jcs.mil/Doctrine/DOD-Terminology-Program/> (zuletzt besucht: März 2023) (zit. U.S. Joint Chiefs of Staff, DoD Terminology Program)

UK Ministry of Defence et al., Elite Force of UK Armed Forces Cyber Reserves Steps up to Join Fight Against Evolving Threats, News Story vom 27.06.2018, abrufbar unter: <https://www.gov.uk/government/news/elite-force-of-uk-armed-forces-cyber-reserves-steps-up-to-join-fight-against-evolving-threats> (zuletzt besucht: März 2023) (zit. UK Ministry of Defence et al., News Story vom 27.06.2018)

UK Ministry of Defence et al., National Cyber Force Transforms Country's Cyber Capabilities to Protect UK, News Story vom 19.11.2020, abrufbar unter: <https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk> (zuletzt besucht: März 2023) (zit. UK Ministry of Defence et al., News Story vom 19.11.2020)

UK National Cyber Strategy 2022, publiziert am 15.12.2021, abrufbar unter: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-5-countering-threats> (zuletzt besucht: März 2023) (zit. UK National Cyber Strategy 2022)

UN General Assembly, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Report of the First Committee, A/73/505; aufgenommen in A/RES/73/266, 73rd Sess., Agenda item 96, 22.12.2018 (zit. UN Doc. A/RES/73/266 (2018))

UN General Assembly, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, Sixth Committee, A/8082; aufgenommen in A/RES/2625 (XXV), 25th Sess., Annex, 24.10.1970 (zit. Declaration on Friendly Relations (UN Doc. A/RES/2625 (XXV)))

UN General Assembly, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, First Committee; aufgenommen in A/RES/36/103, 36th Sess., Agenda item 58 b, Annex, 09.12.1981 (zit. Declaration on the Inadmissibility of Intervention (UN Doc. A/RES/36/103 (1981))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee, A/53/576; aufgenommen in A/RES/53/70, 53rd Sess., Agenda item 63, 04.12.1998 (zit. UN Doc. A/RES/53/70 (1998))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, A/54/213, 54th Sess., Item 71 of the provisional agenda, 10.08.1999 (zit. UN Doc. A/54/213 (1999))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, A/56/164, 56th Sess., Item 81 of the preliminary list, 03.07.2001 (zit. UN Doc. A/56/164 (2001))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee, A/56/533; aufgenommen in A/RES/56/19, 56th Sess., Agenda item 69, 29.11.2001 (zit. UN Doc. A/RES/56/19 (2001))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee, A/57/505; aufgenommen in A/RES/57/53, 57th Sess., Agenda item 61, 22.11.2002 (zit. UN Doc. A/RES/57/53 (2002))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, A/58/373, 58th Sess., Item 69 of the provisional agenda, 17.09.2003 (zit. UN Doc. A/58/373 (2003))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, A/59/116, 59th Sess., Item 62 of the preliminary list, 23.06.2004 (zit. UN Doc. A/59/116 (2004))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee, A/58/457; aufgenommen in A/RES/58/32, 58th Sess., Agenda item 68, 18.12.2003 (zit. UN Doc. A/RES/58/32 (2003))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee, A/60/452; adopted in A/RES/60/45, 60th Sess., Agenda item 86, 08.12.2005 (zit. UN Doc. A/RES/60/45 (2005))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts; aufgenommen in A/65/201, 65th Sess., Item 94 of the provisional agenda, 30.07.2010 (zit. UN Doc. A/65/201 (2010))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, A/66/152, 66th Sess., Item 93 of the provisional agenda, 15.07.2011 (zit. UN Doc. A/66/152 (2011))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, A/68/156, 68th Sess., Item 94 of the preliminary list, 16.07.2013 (zit. UN Doc. A/68/156 (2013))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts, A/68/98; aufgenommen in A/RES/68/243, 68th Sess., Agenda item 94, 27.12.2013 (zit. UN Doc. A/RES/68/98 (2013))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts, A/RES/70/174; aufgenommen in A/RES/70/237, 70th Sess., Agenda item 92, 23.12.2015 (zit. UN Doc. A/RES/70/174 (2015))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee, A/73/505; aufgenommen in A/RES/73/27, 73rd Sess., Agenda item 96, 05.12.2018 (zit. UN Doc. A/RES/73/27 (2018))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts; aufgenommen in A/76/135, 76th Sess., Item 96 of the preliminary list, 14.07.2021 (zit. UN Doc. A/76/135 (2021))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Official Compendium of Voluntary National Contributions on the Subject of how International Law applies to the use of Information and Communications Technologies by States submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security; aufgenommen in A/76/136, 76th Sess., Item 96 of the preliminary list, 13.07.2021 (zit. UN Doc. A/76/136 (2021))

UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report of the Open-Ended Working Group, A/AC.290/2021/CRP.2, Conference Room Paper, 10.03.2021 (zit. OEWG, finaler Bericht vom 10.03.2021)

UN General Assembly, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, Role of Science and Technology in the Context of International Security,

Disarmament and other Related Fields; aufgenommen in A/C.1/53/3, First Committee, 53rd Sess., Annex, Agenda item 63, 30.09.1998 (zit. UN Doc. A/C.1/53/3 (1998))

UN General Assembly, Report of the International Law Commission on the Work of its 44th Sess. vom 04.05.–24.07.1992, A/47/10; General Assembly Official Records, 47th Sess., Supplement No. 10 (zit. UN Doc. A/47/10 (1992))

UN General Assembly, Report of the International Law Commission on the Work of its 45th Sess. vom 03.05.–23.07.1993, A/48/10; General Assembly Official Records, 48th Sess., Supplement No. 10 (zit. UN Doc. A/48/10 (1993))

UN General Assembly, Responsibility of States for Internationally Wrongful Acts, Report of the Sixth Committee, A/56/589 and Corr.1; aufgenommen in A/RES/56/83, 56th Sess., Annex, Agenda item 162, 12.12.2001, Corr. in A/56/49(Vol. I)/Corr.4 (2007) (zit. UN Doc. A/RES/56/83 (2001))

UN General Assembly, Responsibility of States for Internationally Wrongful Acts, Report of the Sixth Committee, A/59/505; aufgenommen in A/RES/59/35, 59th Sess., Agenda item 139, 02.12.2004 (zit. UN Doc. A/RES/59/35 (2004))

UN General Assembly, Responsibility of States for Internationally Wrongful Acts Compilation of Decisions of International Courts, Tribunals and Other Bodies, Report of the Secretary-General, Sixth Committee, 62nd Sess., Agenda item 78, A/62/62, 01.02.2007 (zit. UN Doc. A/62/62 (2007))

UN General Assembly, Thematic Discussion on item Subjects and Introduction and Consideration of all Draft Resolutions Submitted under all Disarmament and International Security Agenda items, First Committee, 13th Meeting; aufgenommen in A/C.1/60/PV.13, General Assembly Official Records, 60th Sess., Agenda item 85 to 105, 17.10.2005 (zit. UN Doc. A/C.1/60/PV.13 (2005))

UN General Assembly, Transmittal letter dated 1 December 2004 from the Chair of the High-level Panel on Threats, Challenges and Change addressed to the Secretary-General, 59th Sess., Agenda item 55, A/59/565, 02.12.2004 (zit. UN Doc. A/59/565 (2004))

UN Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security, Homepage, abrufbar unter: <https://www.un.org/disarmament/ict-security/> (zuletzt besucht: März 2023) (zit. UNODA, Information and Telecommunications, Homepage)

UN Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security, Fact Sheet, abrufbar unter: <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf> (zuletzt besucht: März 2023) (zit. UNODA, Information and Telecommunications, Fact Sheet)

UN Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security, Open-ended Working Group, abrufbar unter abrufbar unter: <https://www.un.org/disarmament/open-ended-working-group/> (zuletzt besucht: März 2023) (zit. UNODA, Information and Telecommunications, Open-ended Working Group)

UN Security Council, Provisional, 5493. Meeting vom 21.07.2006 (zit. UN Doc. S/PV 5493 (2006))

UN Security Council, Provisional, 5511. Meeting vom 11.08.2006 (zit. UN Doc. S/PV 5511 (2006))

UN Security Council, Resolution 1368 (2001), aufgenommen durch den Sicherheitsrat an seinem 4370. Meeting vom 12.09.2001 (zit. UN Doc. S/RES/1368 (2001))

UN Security Council, Resolution 1373 (2001), aufgenommen durch den Sicherheitsrat an seinem 4385. Meeting vom 28.09.2001 (zit. UN Doc. S/RES/1373 (2001))

Wright Jeremy, Attorney General's Office, Cyber and International Law in the 21st Century, Rede vom 23.05.2018, abrufbar unter: <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> (zuletzt besucht: März 2023) (zit. Wright, Rede vom 23.05.2018)

I. Einleitung

Die Digitalisierung und die damit verbundenen, globalen Interdependenzen prägen unsere internationale Landschaft wie nie zuvor. Täglich werden im Sekundentakt ungeachtet territorialer Grenzen bis zu 140 Mio. Cyberangriffe auf Computerinfrastrukturen weltweit ausgeübt.[8] Solche digitalen Vorfälle füllen dabei regelmässig die Schlagzeilen, und die Frage nach staatlichen Gegenmassnahmen hält die internationale Staatengemeinschaft regelrecht auf Trab.[9] Cyberangriffe gelten mittlerweile als eine der prioritären Angelegenheiten für die nationale und internationale Sicherheit.[10] Begrifflich wird unter Cyberangriffen in der Rechtswissenschaft überwiegend ein defensives oder offensives elektronisches Einwirken auf fremde Computersysteme verstanden, das (direkte oder indirekte) Schäden nach sich zieht oder ziehen kann.[11] Neben täglichen »kleineren« Angriffen gibt es auch schwerwiegende Angriffe. So können die Kumulierung mehrerer Angriffe und/oder gezielte Angriffe auf Kontrollsysteme wichtiger Infrastrukturen massive ökonomische, soziale oder politische Folgen nach sich ziehen.

Weltweit Aufmerksamkeit erlangten erstmals u.a. die Angriffe auf Estland am 27. April 2007, auf Georgien am 8. August 2008 und auf den Iran (entdeckt im Juni[12]) 2010.[13] Estland z.B. wurde das Ziel folgenschwerer Cyberangriffe, die hunderte von zentralen staatlichen und privaten Servern ausser Gefecht setzten und dadurch »nationale Relevanz« erlangten.[14] Die gesamte Nation wurde

---

8 Weltweite Cyberangriffe sind live nachzuverfolgen unter: Checkpoint, Live Cyber Attack Threat Map: <https://threatmap.checkpoint.com/ThreatPortal/livemap.html> (zuletzt besucht: März 2023).

9 Siehe u.a.: Langer, NZZ vom 12.02.2021; Mäder, NZZ vom 28.03.2021; Nakashima, Washington Post vom 14.10.2021; Nakashima, Washington Post vom 28.10.2021; Sanger/Perlroth, New York Times vom 08.12.2020.

10 Der Bundesrat, Sicherheitspolitischer Bericht vom 14.04.2021; The White House, Interim National Security Strategic Guidance 2021. Die Biden-Administration z.B. hat die Cybersicherheit als Priorität auf *allen* Verwaltungs-Ebenen erklärt. Siehe: U.S. Homeland Security, Cybersecurity, Homepage.

11 Tallinn Manual 2.0, S. 415, R92. Siehe u.a. Diggelmann/Hadorn, S. 256; Hathaway et al, S. 817 ff. Zu weiteren Definitionsansätzen nachfolgend unter: III.A. Zum Begriff der Computersysteme und -netzwerke siehe nachfolgend unter II.B.1.a) Fn. 83 f.

12 Nicoll, S. 1.

13 Ausführlich zu den Angriffen: Tikk/Kaska/Vihul, S. 14 ff. Zu Stuxnet: Baezner/Robin, Stuxnet, S. 4 ff.

14 Tikk-Ringas, S. 7.

über mehrere Wochen von zehntausenden von sog. Distributed Denial-of-Service (DDoS)-Angriffen überflutet. Das Ziel von DDoS-Angriffen ist es, simultan eine Vielzahl von Computern mittels externer Kommunikationsanforderungen zu überlasten.[15] Anders als typische DDoS-Angriffe, die einige Tage andauern, haben die Angriffe auf Estland innert Kürze in automatisierter Weise über eine Million Computer infiziert und das Internet praktisch landesweit ausser Betrieb gesetzt, was signifikante Auswirkungen auf die estländische Wirtschaft nach sich zog.[16] Estland ist eine der digitalisiertesten Gesellschaften der Welt, in der fast alle (Wirtschafts-, Zivil- und Regierungs-) Prozesse digitalisiert und i.d.R. auch an das Internet gekoppelt sind, womit die beschriebenen Angriffe den Staat besonders hart trafen.[17] Im Falle Georgiens wurden innerhalb eines bereits laufenden Konflikts mit Russland ebenfalls DDoS-Angriffe lanciert sowie offizielle, nationale Webseiten manipuliert.[18] Es wurden nicht nur relevante Kommunikationssysteme blockiert, sondern – anders als bei Estland – auch Inhalte verändert und verfälscht, um auf die politische Meinungsbildung Einfluss zu nehmen.[19] Im Beispiel der Angriffe auf den Iran hingegen wurde ein sehr spezifischer Computerwurm (»Stuxnet«) entwickelt, der konkret auf das zentrale Steuerungssystem der Atomanreicherungsanlagen von Natanz abzielte.[20] Dort angelangt, änderte Stuxnet die Programmierung der Geschwindigkeit der Zentrifugen, indem er die Kontrollsoftware umschrieb. Diese Änderung führte dazu, dass die Zentrifugen so schnell zu schleudern begannen, bis sie zersprangen. Dadurch wurde ein substanzieller Teil des iranischen Atomprogrammes zerstört. Dies – und das ist für die vorliegende Abhandlung wichtig – stellte eine erstmals dokumentierte, *physische* Zerstörung von Infrastrukturen durch einen Cyberangriff dar.[21] Zudem wurden iranische Atomwissenschaftler gezwungen den Anreicherungsprozess auszuschalten, bis man den Ursprung der Schädigungen eruieren konnte.[22] Stuxnet befand sich über ein Jahr lang unbemerkt im Computernetzwerk von Natanz,

15 Schweizerische Eidgenossenschaft, Cyberkriminalitäts-Phänomene, DoS/DDoS Kurzbeschrieb. Eingehender zu DDoS-Angriffen siehe nachfolgend unter III.A.3.a).

16 Springer, Cyber Warfare, S. 35.

17 Harrison Dinniss, S. 38 f.

18 Ausführlicher dazu u.a. Tikk/Kaska/Vihul, S. 69 ff.; Swanson, S. 303 ff.

19 Woltag, S. 45.

20 Brenner, S. 102 ff.; Springer, Cyber Warfare, S. 30.

21 Sanger, S. 200; Finkelstein/Govern, S. ix.

22 Springer, Cyber Warfare, S. 30. Vgl. Poroshyn, S. 48 ff.; Rosenzweig, S. 2 ff.

und auch nach dem Eintreffen der Schädigungen wussten die Verantwortlichen der Atomanlage nicht, dass sie Opfer eines Cyberangriffs geworden waren, sondern gingen lange von vereinzelten Softwarefehlern aus.[23]

Hinter den Angriffen auf Georgien und Estland werden, trotz Schwierigkeiten des technischen Nachweises, Russland[24] und beim Angriff auf den Iran die USA und Israel vermutet.[25] Neben privaten Akteuren – und dies ist ein wichtiger Punkt für die vorliegende Dissertation – werden Cyberangriffe also auch von *Staaten* eingesetzt, um strategische, geopolitische und militärische Ziele zu verfolgen.[26] Die Beispiele zeigen zudem, dass die Konsequenzen solcher Angriffe für die betroffenen Staaten gravierend sein können – etwa bei Cyberangriffen auf Kontrollsysteme kritischer Infrastrukturen wie z.B. Atomanreicherungsanlagen, Elektrizitätswerke oder Spitäler, auf deren Funktionieren die Zivilbevölkerung und staatliche Einrichtungen zunehmend angewiesen sind.[27] Indem moderne Staaten zunehmend vernetzt und von Computersystemen abhängig sind, werden sie insgesamt also verletzlicher für Angriffe.[28] Oder in Roscini's Worten: »*If computer networks become the society's ›nerve system‹, incapacitating them may mean paralysing the country.*«[29] Daher sind verschiedene Arten politischer, ökonomischer sowie physischer Folgen und/oder die Herbeiführung von Todesopfern realistische Szenarien im Diskurs um Cyberangriffe.

Diese dem wachsenden technologischen Fortschritt geschuldeten Entwicklungen stellen die Staatengemeinschaft vor schwierige Herausforderungen. Insb. stellt sich aus völkerrechtlicher Sicht die Frage, welche internationalen Normen durch transnationale Cyberangriffe verletzt werden und wie Staaten

23 Ausführlicher zu Stuxnet: Singer/Friedman, S. 115 ff.; Langner, S. 3 ff.

24 Tikk/Kaska/Vihul, S. 15 ff., 74 ff.

25 Siehe dazu u.a. Harrison Dinniss, S. 37 m.w.V.; Greenberg, Sandworm, S. 96 ff.; Sanger, S. 188 ff.; Schulze, S. 16 m.w.V; Singer/Friedman, S. 117.

26 Siehe dazu u.a. die Analyse von Dewar, Contextualizing, S. 3 ff., insb. S. 8; Sanger/Perlroth, New York Times vom 08.12.2020.

27 Zu Sektoren kritischer Infrastrukturen in der Schweiz siehe auf der Homepage: Bundesamt für Bevölkerungsschutz, kritische Infrastrukturen. Die USA haben bereits am 20.10.2017 ein erstes Warnmeldesystem entwickelt, um auf kritische Infrastrukturen abzielende Gefahrenaktivitäten zu messen. Dazu u.a.: Litan, Gartner Blog Network vom 02.11.2017. Zum Warnmeldesystem siehe: CISA, Alert TA17-293A, 2017. Dieses Meldesystem wurde ersetzt durch CISA, Alert TA18-074A, 2018 und jüngere Programme. Näheres zu solchen Gefahren: Singer/Friedman, S. 55 ff.

28 Singer/Friedman, Cybersecurity, S. 152.

29 Roscini, Cyber Operations, S. 1.

darauf reagieren dürfen. Grundsätzlich besteht Einigkeit darüber, dass diese Fragen vor dem Hintergrund des traditionellen Völkerrechts beantwortet werden müssen.[30] Es besteht demzufolge Klärungsbedarf, *wie* staatliches oder dem Staat zurechenbares Verhalten im Cyberraum[31] völkerrechtlich erfasst werden soll und welches die zulässigen Reaktionsmöglichkeiten darauf sind. Mit dem Aufkommen von Cyberangriffen trifft somit ein neues, transnationales Phänomen von sicherheitspolitischer Relevanz auf traditionelle Rechtsstrukturen, die auf Konflikte jenseits des Cyberkontexts ausgerichtet sind.

Im dezentralen System des Völkerrechts erfolgen Reaktionsmechanismen grundsätzlich auf dem Weg der Selbsthilfe.[32] Dabei werden, vereinfacht gesprochen, einerseits die allgemeine Form nicht-militärischer Gegenmassnahmen (»*countermeasures*«) und andererseits der Ausnahmefall einer militärischen Selbstverteidigung nach Art. 51 UN-Charta unterschieden. Da aufgrund des durch die Staatengemeinschaft anerkannten Gewaltverbots gewaltsame Selbsthilfe grundsätzlich nicht erlaubt ist,[33] darf die militärische Selbstverteidigung lediglich in einem eng definierten Ausnahmefall erfolgen, in dem alle Voraussetzungen von Art. 51 UN-Charta erfüllt sind. Nicht-militärische Gegenmassnahmen hingegen müssen dem grösstenteils als Gewohnheitsrecht anerkannten Artikelentwurf für die Verantwortlichkeit von Staaten für völkerrechtswidriges Handeln (ARSIWA)[34] standhalten.[35] Damit Selbsthilfe zulässig

30 Siehe nachfolgend unter II.A.2.

31 Der Cyberraum wird oft als ein globales, interdependentes Netzwerk verstanden, das digitale Infrastrukturen, Daten und diverse Computernetzwerke und -systeme (durch das Internet) verbindet. Siehe z.B.: SCHULZE, S. 110 m.w.H. Das Internet ist einer solchen Lesart zufolge als ein wesentlicher Bestandteil, jedoch nicht als Synonym für den Cyberraum zu verstehen.

32 DIGGELMANN, Völkerrecht, S. 158.

33 DIGGELMANN, Völkerrecht, S. 158.

34 Aufgrund der hohen Autorität der internationalen Völkerrechtskommission (ILC) sowie des Einbezugs der Staaten bei der Ausarbeitung des ARSIWA-Entwurfs entwickelten sich diese über Zeit zu einer wichtigen Völkerrechtsquelle. Der Entwurf wurde nicht in eine Konvention überführt, sondern in einer Resolution der UN-Generalversammlung inkludiert und dadurch bestätigt. Siehe: Annex in UN Doc. A/RES/56/83 (2001), korrigiert durch A/56/49(Vol. I)/Corr.4, bestätigt in UN Doc. A/ A/RES/59/35 (2004). Von der Bedeutung und Rechtswirksamkeit der ARSIWA als Völkerrechtsquelle zeugt ausserdem, dass sich die internationale Gerichts- und Staatenpraxis explizit darauf stützt: Der UN-Bericht (UN Doc. A/62/62 (2007)) listet 129 Fälle auf, in denen internationale Gerichte und weitere Gremien sich auf die ARSIWA beziehen. So z.B. IGH, Gabčíkovo-Nagymaros-Urteil, §79. Siehe dazu u.a.: CRAWFORD, MPEPIL 2006, §65 ff.; DAHM/DELBRÜCK/WOLFRUM, Bd. I/3, S. 866; WOLTAG, S. 86.

35 Zu nicht-militärischen Gegenmassnahmen siehe Art. 49 ff. ARSIWA.

ist, muss für beide Formen der Selbsthilfe u.a. das Erfordernis der Verhältnismässigkeit erfüllt sein. Dieses völkerrechtlich anerkannte Prinzip soll im Grunde dem Zweck dienen, *übermässige Sanktionierung* zu verhindern.[36]

Die vorliegende Dissertation soll einen Beitrag zur Klärung völkerrechtlicher Selbsthilfemöglichkeiten von Staaten bei Cyberangriffen leisten. Die leitenden Forschungsfragen dazu sind: Wann dürfen Staaten aus völkerrechtlicher Sicht auf Cyberangriffe reagieren? Welche unilateralen Verteidigungs- und Gegenmassnahmen sind dabei verhältnismässig? Insgesamt soll im Rahmen der vorliegenden Analyse der Gedanke zentral sein, internationale Stabilität und verantwortungsvolles, verhältnismässiges Verhalten der Staaten im Cyberraum zu fördern. Dabei wird die Ansicht vertreten, dass für die Regulierung staatlichen Verhaltens im Cyberraum grundsätzlich am über Jahrzehnte durch Rechtsüberzeugung (*opinio iuris*), durch IGH-Rechtsprechung, Staatenpraxis und Lehrmeinungen etablierten und bereits bestehenden Rahmen des traditionellen Völkerrechts anzuknüpfen ist, um internationale Stabilität und die Voraussehbarkeit staatlichen Handelns zu fördern.

Für die Erarbeitung der Leitfragen wird einerseits die Debatte um das völkerrechtliche Recht auf Selbstverteidigung gem. Art. 51 UN-Charta bei Cyberangriffen kritisch aufgegriffen. Andererseits werden die Grundideen des völkerrechtlichen Gegenmassnahmenrechts gem. ARSIWA näher beleuchtet. Angesichts der hohen Dichte an staatlichen Stellungnahmen zur Cybersicherheit innerhalb der UNO sowie die jeweils hinzukommenden nationalen Cyber-Strategien kann nur eine limitierte Auswahl der für die Erarbeitung der vorliegenden These relevanten Staatenansichten aufgegriffen werden. Aufgrund ihres Einflusses auf das Völkerrecht fliessen allerdings insb. Positionen von Staaten wie den USA oder Grossbritanniens in die vorliegende Abhandlung ein. Die Perspektive dieser Untersuchung bleibt jedoch in ihren Grundzügen eine schweizerische.

Die Untersuchung ist wie folgt gegliedert: In einem nächsten Schritt (Teil II.) sollen der Diskurs um das neuartige Phänomen von Cyberangriffen eingeordnet und die offenen Fragen herausgearbeitet werden. Um eine Grundlage für die nachfolgende Anwendung traditioneller Völkerrechtsnormen auf Cyberangriffe zu schaffen, erfolgt ein kurzer historischer Abriss zum Aufkommen des Diskurses sowie zu den ersten Regulierungsansätzen. Daraufhin wird die Bedeutung des Verhältnismässigkeitsprinzips für den Diskurs aufgegriffen sowie der erwartete Erkenntnisgewinn der vorliegenden Dissertation definiert.

[36] DIGGELMANN, Völkerrecht, S. 158.

Im Teil III. werden verschiedene Definitionen und technische Kategorien von Cyberangriffen angeführt, um eine für die vorliegend rechtliche Analyse einschlägige Definition des Untersuchungsgegenstands »Cyberangriffe« zu erarbeiten. Anschliessend folgt die völkerrechtliche Einordnung und Erfassung dieser Definition. Insbesondere soll die Anwendbarkeit der Konzepte eines bewaffneten Angriffs nach Art. 51 UN-Charta (*ius ad bellum*), des für die völkerrechtliche Staatenverantwortlichkeit relevanten Interventionsverbots und der völkerrechtlichen Sorgfaltspflicht (Due Diligence) Erwähnung finden. Darauf folgt im Teil IV. eine nähere Betrachtung der Bedeutung des Verhältnismässigkeitsprinzips i.S.v. Art. 51 UN-Charta sowie i.S. des Gegenmassnahmenrechts im Cyberkontext. Die gewonnenen Erkenntnisse erlauben in einem Schlussteil die Beantwortung der Frage, welche Reaktionsmöglichkeiten bei Cyberangriffen verhältnismässig und somit der vorliegenden, völkerrechtlichen Betrachtung nach (un-)zulässig sind. Die Untersuchung endet schliesslich mit ausblickenden Folgerungen.

II. Diskurseinordnung

A. Aufkommen des Diskurses

1. Erste internationale Regulierungsversuche

Der wissenschaftliche Diskurs über die Regulierung des Cyberraums kam grundsätzlich ab Mitte der 1990er Jahre auf.[37] Erste internationale Regulierungsansätze gehen auf eine Initiative Russlands im Jahr 1998 zurück. Der damalige russische Aussenminister Igor Iwanow wandte sich am 23. September 1998 mit dem Resolutionsentwurf »*Developments in the field of information and telecommunications in the context of international security*« an den UN-Ausschuss für Abrüstung und internationale Sicherheit (Erstes Komitee[38]).[39] Darin äusserte er die Besorgnis, dass Informationstechnologien (als Äquivalent zu Cybertechnologien zu verstehen) potenziell zu Zwecken eingesetzt würden, die mit der Gewährleistung der internationalen Stabilität und der Beachtung des Gewalt- und Interventionsverbots sowie mit den Menschenrechten unvereinbar sein könnten. Eine breite internationale Zusammenarbeit werde des Weiteren unerlässlich, da die (militärische) Nutzung von Informationstechnologien mit Massenvernichtungswaffen vergleichbar sei. Zwar wurden das Gewalt- und das Interventionsverbot erwähnt, eine wesentliche Angst lag jedoch auch spürbar beim unter Umständen »desaströsen« Missbrauch von Informationstechnologien durch Terroristen oder Kriminelle.[40] Die internationale Staatengemeinschaft wurde durch den Resolutionsentwurf 1998 insgesamt erstmals aufgefordert, sich zur staatlichen Verwendung von Informationstechnologien und zu einem Entwicklungs-, Produktions- und Nutzungsverbot besonders gefährlicher Technologien zu äussern.[41] Ebenso sollten die Staaten ihre Meinung zur Errichtung eines zentralisierten, internationalen Systems zur Erkennung von Gefahren für die Sicherheit globaler Informati-

---

37 Siehe u.a. ARQUILLA/RONFELDT, S. 141 ff.; BERKOWITZ, S. 59 ff.; BLANK STEPHEN, S. 17 ff.; HUNDLEY/ANDERSON, S. 19 ff.; JOHNSON/POST, S. 1367 ff.; MEFFORD, S. 211 ff.; SHARP. So auch: O'CONNELL, Cyber Security, S. 187. Dazu auch: KERSCHISCHNIG, S. 59 ff.

38 Zum Ersten Komitee siehe <https://www.un.org/en/ga/first/index.shtml> (zuletzt besucht: März 2023).

39 UN Doc. A/C.1/53/3 (1998); TIKK-RINGAS, S. 3; MAURER, S. 20 ff.; SCHULZE, S. 170.

40 Heute werden Cybersicherheitsthemen je nach dahinterstehender Akteursgruppe generell in vier verschiedene Kategorien unterteilt: In die Cyberkriminalität, den Cyberterrorismus, die Cyberspionage und den bewaffneten Konflikt. Siehe: NCS-II, S. 4 f.

41 SCHULZE, S. 170.

onssysteme darlegen.[42] Dabei verfingen weder ein Verbot besonders gefährlicher Informationstechnologien noch die Idee eines Erkennungssystems.[43] In der schliesslich per Konsens durch die UN-Generalversammlung angenommenen Resolution vom 4. Dezember 1998 wurde vielmehr allgemein zur Verbesserung der Informationssicherheit aufgerufen.[44] Es wurde festgehalten, dass Informationstechnologien potenziell zu zivilen *und* militärischen Zwecken missbraucht werden könnten. Die UN-Resolution 53/70 diente in der Folge als Basis für weitergehende UNO-Debatten zu völkerrechtlichen Regelwerken im Cyberkontext.[45] Ab 2006 folgten zudem jährliche Stellungnahmen der Staaten zur Informationssicherheit.[46] Die Haltungen der Staaten divergierten dabei nicht nur bezüglich der Regulierung der Informationssicherheit, sondern auch im Hinblick auf die damit zusammenhängende Bedeutung des Ersten Komitees[47] sowie bezüglich der Schlüsseldefinitionen.[48] Zudem bestanden lange inhaltliche Meinungsdifferenzen in Bezug auf die Notwendigkeit eines separaten, internationalen Vertrags.[49]

Am 29. November 2001 schlug Russland die Errichtung einer UN-Expertengruppe (UN GGE) vor, die sich im Rahmen der UNO mit der Thematik auseinandersetzen und die Entwicklungen kooperativer Massnahmen unterstützen sollte.[50] Im Juni 2004 fand die erste UN GGE mit Experten aus 15 Staaten

42 UN Doc. A/C.1/53/3 (1998).

43 SCHULZE, S. 171.

44 UN Doc. A/RES/53/70 (1998).

45 RALTCHEV, S. 85 m.w.V.

46 RALTCHEV, S. 87 m.w.V.; SCHULZE, S. 171 m.w.V. Zu einer Übersicht staatlicher Stellungnahmen sowie weiterer damit zusammenhängenden Entwicklungen: UNODA, Information and Telecommunications, Homepage.

47 Russland, Kuba und China z.B. sahen die UNO und das Erste Komitee als adäquates Forum für die Aufarbeitung militärischer, terroristischer und krimineller Cyberfragen (Kuba in UN Doc. A/54/213 (1999), S. 3 ff., China in UN Doc. A/59/116 (2004), S. 4), während die USA, Australien und die EU-Länder sich für eine limitiertere Rolle des Ersten Komitees aussprachen (Australien und die USA in UN Doc. A/54/213 (1999), S. 2 ff., S. 11 ff., Schweden in UN Doc. A/56/164 (2001), S. 4 im Namen der EU-Staaten).

48 Ausführlicher zu den Haltungen sowie zu den nationalen Stellungnahmen zwischen 1998–2011: TIKK-RINGAS, S. 4 ff.

49 So z.B. Russland in UN Doc. A/54/213 (1999), S. 8. Anderer Ansicht: USA in UN Doc. A/54/213 (1999), 12 f.; USA in UN Doc. A/59/116/Add.1 (2004), S. 4; UK in UN Doc. A/59/116 (2004), S. 11. Dazu u.a.: RALTCHEV, S. 93; MARKOFF/KRAMER, New York Times vom 27.06.2009.

50 Russland in UN Doc. A/58/373 (2003), S. 9. Dazu: TIKK-RINGAS, S. 6. Dieser Vorschlag wurde von der UN-Generalversammlung aufgenommen in UN Doc. A/RES/56/19 (2001) und UN Doc. A/RES/57/53 (2002).

zusammen.[51] Die Meinungen innerhalb der UN GGE divergierten allerdings so stark, dass kein Konsens gefunden wurde.[52] Der russische Diplomat Andrei Krutskikh umschrieb die Herausforderungen dahingehend, dass innerhalb eines kurzen Zeitraumes eine ganze Bandbreite an »fundamental neuen« und »heiklen« Problemen adressiert werden musste.[53] Die Experten hätten in Bezug auf die zentralen Probleme der internationalen Informationssicherheit, trotz Übersetzung, »verschiedene Sprachen« gesprochen.[54] Zudem variierten sowohl die nationalen Regulierungsansätze als auch die Verständnisse der Anwendung des Völkerrechts im Bereich der internationalen Informationssicherheit fundamental.[55]

Die zweite UN GGE fand zwischen 2009 und 2010 statt, also *nach* den Cyberangriffen auf Estland und Georgien.[56] Dementsprechend bestanden während den Verhandlungen beträchtliche politische Spannungen zwischen den Opferstaaten und Russland, das hinter den Angriffen vermutet wurde.[57] Im Bericht festgehalten wurde, dass die Gefahren im Bereich der Informationssicherheit zu den »ernstesten Herausforderungen des 21. Jahrhunderts zählen.«[58] Die allgemeine Besorgnis, dass Staaten Technologien als Instrumente für Krieg und politische Zwecke verwenden würden, war sichtlich gestiegen.[59] Die Hauptergebnisse der zweiten UN GGE gingen insofern weiter als im Jahr 2004, als dass man sich darauf einigte, die nationalen Ansichten zu möglichen Regulierungen von Cybertechnologien weiterhin zu diskutieren, und, dass kollektive Risiken reduziert und nationale und internationale Infrastrukturen besser geschützt werden müssen. Es wurden u.a. Risikoverringerungs- und vertrauensbildende Massnahmen vorgeschlagen.[60]

Neben den Regulierungsversuchen auf Ebene der UNO gab und gibt es weitere internationale und regionale Anstrengungen auf dem Gebiet der Cybersicherheit. Nennenswert sind u.a. die Entwicklungen im Zusammenhang mit der

---

51 Basierend auf UN Doc. A/RES/58/32 (2003). Ausführlicher dazu: Tikk-Ringas, S. 6, (zur Zusammensetzung der UN GGE zwischen 2004–2012) S. 12.

52 Tikk-Ringas, S. 7.

53 UN Doc. A/C.1/60/PV.13 (2005), S. 5.

54 UN Doc. A/C.1/60/PV.13 (2005), S. 5.

55 UN Doc. A/C.1/60/PV.13 (2005), S. 5; Tikk-Ringas, S. 7.

56 Angefordert wurde die Errichtung einer weiteren UN GGE in UN Doc. A/RES/60/45 (2005), S. 3. Die Sessionen mündeten sodann in UN Doc. A/65/201 (2010).

57 Tikk-Ringas, S. 7.

58 UN Doc. A/65/201 (2010), S. 2.

59 Siehe in: UN Doc. A/65/201 (2010), S. 7.

60 UN Doc. A/65/201 (2010); Tikk-Ringas, S. 7.

Internationalen Fernmeldeunion (ITU), der NATO, der OSZE, dem Europarat, der Shanghaier Organisation für Zusammenarbeit (SCO), mit dem Regionalforum des Verbands Südostasiatischer Nationen (ASEAN), die Errichtung der Budapest Konvention sowie weitere Entwicklungen innerhalb der EU[61].[62] Diese Bemühungen gehen allerdings in Bezug auf völkerrechtliche Fragen grundsätzlich nicht über die im Rahmen der UNO erzielten Ergebnisse hinaus bzw. wurden die Ergebnisse der UNO teilweise sogar übernommen.[63] Daher sind für die vorliegende Abhandlung primär die innerhalb der UNO-Prozesse erzielten Konsense relevant.

2. Anwendbarkeit des traditionellen Völkerrechts

Nach den DDoS-Angriffen auf Estland im Jahr 2007 gab es in Lehre und Öffentlichkeit eine Verlagerung auf die Thematik um *staatlich* geführten »Cyberkrieg«.[64] Die Angriffe auf Estland wurden wiederholt als erstmals dokumentierte »*acts of genuine cyberwar*« bezeichnet.[65] Auch der 2010 entdeckte Computerwurm Stuxnet stellte einen sicherheitspolitischen Umbruch dar, der intensive Debatten zu dessen rechtlicher Erfassung auslöste.[66] Weil sowohl hinter den Angriffen auf Estland als auch hinter Stuxnet staatliche Interessen vermutet wurden,[67] rückten in der Folge zunehmend Staaten als Akteure hinter Cyberangriffen in den regulatorischen Fokus.

---

61 Zu einer Übersicht der Entwicklungen innerhalb der EU: Europäischer Rat, Cybersicherheit 2022.

62 Ausführlicher zu regionalen Bemühungen: Schulze, S. 179 ff. Ebenso zu einer Abhandlung verschiedener regionaler und globaler Prozesse, Agenden und Instrumente: Weekes/Tikk-Ringas.

63 Lehto, S. 32; Schulze, S. 182.

64 Als zweite »Cyberkriegs-Hysterie« umschreibend: Raltchev, S. 114. Zum Aufkommen des Diskurses um Cyberkrieg auch: Dunn Cavelty, ETH Zukunftsblog vom 15.06.2018; Dunn Cavelty, Computerworld vom 17.05.2013.

65 Brenner, S. 127 ff.; Clarke/Knake, Cyber War, S. 11 ff.; Lucas, S. 64. Andere Autoren sehen die Angriffe auf Georgien als »ersten« Cyberkrieg: Stiennon, S. 95 ff. Dennoch wurde in der im Nachgang an die Vorfälle in Estland und Georgien folgenden UN GGE im Jahr 2009 kein Konsens bezüglich staatlich lancierten Cyberangriffen gefunden.

66 Broad/Markoff/Sanger, New York Times vom 15.01.2011; Dunn Cavelty, Computerworld vom 17.05.2013; Finkelstein/Govern, S. ix; Sanger, S. 200.

67 Siehe vorangehend unter Fn. 25.

Im Jahr 2013 fand die dritte UN-Expertengruppe (UN GGE) erstmals einen internationalen Konsens, wonach das Völkerrecht und insb. die UN-Charta auf den Cyberraum anwendbar sind.[68] Das Völkerrecht soll dazu beitragen, ein offenes, sicheres, zugängliches und friedliches Cyberumfeld zu schaffen und als Rahmen im Umgang mit Cybertechnologien gelten.[69] Im selben Jahr wurde auf Initiative des NATO Cooperative Cyber Defence Center das sog. Tallinn Projekt in Tallinn, Estland gestartet. Daraus resultierte 2013 das Tallinn Manual 1.0 »zur Anwendung des Völkerrechts auf den Cyberkrieg«. Das Manual ist ein durch internationale Experten erarbeiteter, nicht-bindender Leitfaden zu Auslegungsfragen des Völkerrechts im Cyberkontext.[70] Das Projekt war damit ein erster Versuch, die staatliche Verwendung von Informationstechnologien völkerrechtlich zu erfassen. Die Anwendbarkeit des Völkerrechts wurde im Jahr 2015 von der vierten UN GGE bestätigt, doch im Grunde nicht substanziell konkretisiert.[71] Im Jahr 2017 folgte das Tallinn Manual 2.0, das sich, ergänzend zum Tallinn Manual 1.0, mit dem anwendbaren Völkerrecht auf Cyberoperationen zu Friedenszeiten befasst.[72] Damit bieten die Beiträge der Experten im Tallinn Manual 1.0 und 2.0 erste Orientierungshilfen bei der Frage nach der Anwendung von Völkerrecht im Cyberkontext. Diese sollen auch als Quelle für die vorliegende Analyse herangezogen werden.

Im Juni 2017 sollte die fünfte UN GGE die inhaltliche Frage adressieren, wie das Völkerrecht – mitunter das Selbstverteidigungs- und das Gegenmassnahmenrecht – auf Cyberangriffe anzuwenden ist.[73] Allerdings scheiterte ein derartiger politischer Konsens zwischen den damals 25 Mitgliedern der UN GGE.[74] Im Rahmen der UNO kam somit in den folgenden Jahren keine weitergehende Einigung zustande zur Frage, *wie* Völkerrechtsnormen anzuwenden sind.[75] Im Dezember 2018 gründete die UN-Generalversammlung sodann mit einer neuen UN GGE[76] sowie einer für alle UN-Mitgliedstaaten offenen[77]

68 UN Doc. A/RES/68/98 (2013).

69 UN Doc. A/RES/68/98 (2013).

70 Tallinn Manual 1.0, S. 1.

71 UN Doc. A/RES/70/174 (2015).

72 Tallinn Manual 2.0, S. 3.

73 Schmitt/Vihul, Just Security vom 30.06.2017.

74 Siehe: UNODA, Information and Telecommunications, Fact Sheet.

75 Roguski, S. 2.

76 Siehe: UN Doc. A/RES/73/266 (2018).

77 Siehe: UN Doc. A/RES/73/27 (2018), S. 4. Ausführlichere Informationen zu den Sitzungen: UNODA, Information and Telecommunications, Open-ended Working Group.

Open-ended Working Group (OEWG)[78] neue Mandate, die sich während den Jahren 2019 – 2021 eingehender mit der Frage nach der Anwendbarkeit von Völkerrechtsnormen auf Cyberangriffe befassten.[79]

Rückblickend kann gesagt werden, dass die Fragen zur Anwendung des Völkerrechts auf den Cyberraum Politiker, Juristen und weitere Experten bereits seit rund drei Jahrzehnten beschäftigen. Die Verhandlungsprozesse haben dabei allerdings erst zu relativ rudimentären Lösungsansätzen geführt. Bis zur dritten UN GGE im Jahr 2013 konzentrierten sich die verschiedenen nationalen und internationalen Regelungsversuche überwiegend auf Fragen von Cyberkriminalität und -terrorismus.[80] Die Ergebnisse der UN GGE in den Jahren 2013 und 2015 sowie des finalen Berichts der OEWG vom 10. März 2021 sind für den gegenwärtigen internationalen Diskurs um staatliche Cybersicherheitsaspekte insofern massgebend, als dass diese im Grunde die Anwendbarkeit von Völkerrecht bestätigt haben. Damit war die Debatte um dessen Interpretation im Cyberkontext lanciert.

Insgesamt bestehen im Hinblick auf die Regulierung von Cyberangriffen immer noch sehr unterschiedliche internationale Auffassungen. Die Vielzahl an Verhandlungen sowie die schleppenden Fortschritte in der Konsensfindung manifestieren einerseits die Herausforderungen bei der Anwendung und Interpretation traditioneller Normen. Die technischen Eigenheiten von Cyberangriffen und die international divergierenden Ansichten machen die Thematik besonders anspruchsvoll. Andererseits scheint die Schwierigkeit, internationale Konsense zu finden, auch zu manifestieren, dass die Diskussion nicht nur eine rechtliche, sondern auch eine strategische und politische ist, bei der unvermeidbar ideologische Differenzen mitschwingen.[81] Völkerrechtliche Regulierungen bedeuten nämlich jeweils auch Einbussen des (eigenen) staatlichen Handlungsspielraums. Staatliche Ansichten sind für den Diskurs dennoch sehr wichtig, da sie das Völkerrecht durch Staatenpraxis und *opinio iuris* mitkonstituieren.[82]

78 Siehe: UN Doc. A/RES/73/27 (2018).

79 UNODA, Information and Telecommunications, Homepage; ROGUSKI, S. 2. Zu wichtigen Konsensen und offenen Fragen sogleich ausführlicher unter II.B.2. Eingehender zu den UN GGE und den damit verbundenen Normentwicklungen: LEHTO, S. 32 ff.

80 RALTCHEV, S. 114.

81 HENRIKSEN, S. 1.

82 KANUCK, S. 1582.

B. Forschungsstand und offene Fragen

1. Forschungsstand zum Untersuchungsgegenstand »Cyberangriffe«

a. Neue Dimension globaler Interkonnektivität und Schädigungsradien

Computersysteme[83] und -netzwerke[84] sind mittlerweile allgegenwärtige Bestandteile des gesellschaftlichen Alltags. Sie sind (teilweise unbemerkt) für praktisch alle ökonomisch, sozial und öffentlich relevanten Vorgänge unverzichtbar geworden.[85] Durch das Internet werden all diese Computer, Computersysteme und -netzwerke und deren technischen Sicherheitslücken weltweit vernetzt,[86] was Staaten insgesamt extrem angreifbar macht.[87] »Je mehr Vernetzung, desto mehr potenzielle Ziele« existieren.[88] Bereits 2002 wurde angenommen, dass »alle Computer der Welt« miteinander verbunden seien, indem durch den Zugang eines Computers zum Internet dieser global mit allen anderen Computern verknüpft wird, die zu die diesem Zeitpunkt online sind.[89]

---

83 Im Tallinn Manual wird ein Computer umschrieben als »*[a] device that processes data*«, ein Computersystem als »*one or more interconnected computers with associated software and peripheral devices*«: Tallinn Manual 1.0, S. 258.

84 Ein Computernetzwerk verbindet zwei oder mehrere Computer oder Computersysteme (auch verstanden als »Netzwerkknoten«), um mittels Internet Daten auszutauschen: Roscini, Cyber Operations, S. 1 Fn. 1.

85 Schulze, S. 2. Zu Ausführungen einer zunehmenden Digitalisierung des öffentlichen Bereichs siehe »*State and eGovernment*«: Woltag, S. 17 ff. Gemäss Bundesamt für Statistik wuchs der Anteil der regelmässigen Internetnutzer/-innen in den letzten Jahren rasant und bewegt sich in gewissen Alterskategorien mittlerweile bei 100%. Die Internetnutzung in der Schweiz lag bereits im März 2018 bei einem Durchschnittswert von 85.7% und 2021 bei 96%. Dies zeigt, dass das Internet ein alltägliches Medium geworden ist. Siehe Bundesamt für Statistik, Internetnutzung 1997–2021. Ähnlich liegt gem. Eurostat der Durchnittswert für die EU-Länder im Jahr 2020 bei rund 89% und 2022 bei rund 91%. Siehe Eurostat, Individuals Internet Use 2023.

86 Ausführlicher dazu: Woltag, S. 9 ff.

87 Schulze, S. 2.; ähnlich Joyner/Lotrionte, S. 830; Schmitt, Computer Network Attack, S. 887; Woltag, S. 13 ff.

88 Dunn Cavelty, ETH Zukunftsblog vom 18.01.2018.

89 Barnett, S. 21.

Dazu kommt, dass sich an das Internet angeschlossene Alltagsgeräte, sog. internet of things-Geräte, zunehmend in der Gesellschaft verbreiten, ohne dass die Sicherheit der Geräte und deren Software Schritt hält.[90] Teilweise sind auch kritische staatliche Infrastrukturen[91], die wichtige Funktionen für die Gesellschaft übernehmen, an das Internet angeschlossen und weisen oftmals erhebliche Sicherheitslücken auf.[92] Durch die zunehmende Digitalisierung moderner Staaten werden sich die globalen Angriffsflächen wohl weiterhin vergrössern.[93] Oder gem. Dewar: »*The wired world may be moving from a position of hyper connectivity to one of hyper vulnerability.*«[94]

Technische Sicherheitslücken sind Zugriffspfade zu einem Computer, durch die Hacker oder automatisierte Schadprogramme unbefugt eindringen können. Sicherheitslücken entstehen i.d.R. durch Misskonfigurationen von Applikationen, durch Software- oder menschliche Fehler.[95] Umgekehrt wird unter Hacking im Grunde eine Technik verstanden, mittels derer Sicherheitslücken von Systemen ausgenutzt werden können.[96] Im technischen Jargon ist mit dem Eindringen in einen Computer i.d.R. die unbefugte Manipulation der sog. »Vertraulichkeit«, »Integrität« und »Verfügbarkeit« von Computersystemen und -netzwerken gemeint (»*confidentiality*«, »*integrity*«, »*availability*«).[97] Dabei ist es im technischen Sinne irrelevant, ob die unbefugte Manipulation der Vertraulichkeit, der Integrität oder der Verfügbarkeit via Hacking oder via Schadprogrammen erfolgt, und von welchen Akteuren (oder technischen Fehlern) eine solche Manipulation ausgeht. Sobald unbefugter Zugang zu einem System erlangt wird (was eine Beeinträchtigung der Vertraulichkeit desselben bedeutet), können darin verschiedene Funktionen ausgeführt werden. So können bspw. Daten zerstört, kopiert, abgehört (Vertraulichkeits- und Integritätsbeeinträchtigung) oder blockiert und unzugänglich (Verfügbarkeits-

90 Dewar, Contextualizing, S. 7. Dazu auch: Clarke/Knake, Fifth Domain, S. 265 ff.

91 Zu kritischen Infrastrukturen siehe vorangehend unter Fn. 27.

92 Dewar, Contextualizing, S. 7. Das deutsche Bundesamt für Sicherheit in der Informationstechnik hat bspw. auf erhebliche Sicherheitslücken in der Steuerungssoftware von Kraftwerken hingewiesen: Agenturmeldung reu, NZZ vom 05.01.2020.

93 Vgl. Woltag, S. 13 ff.

94 Dewar, Contextualizing, S. 7 m.V.a. Newman, Wired vom 18.01.2018; Johnson et al., Mandiant vom 14.12.2017.

95 Singer/Friedman, S. 40 ff.

96 Burkart/McCourt, S. 1.

97 Burkart/McCourt, S. 1; Herrmann/Pridöhl, S. 13. Dazu nachfolgend ausführlicher unter III.A.3.

beinträchtigung) werden.[98] Von einer einzigen Sicherheitslücke gehen somit eine Vielzahl von Risiken aus, indem unterschiedlich motivierte Hacker (z.B. zu terroristischen, kriminellen oder politischen Zwecken)[99] oder aber (automatisierte) Schadprogramme eindringen können. Die globale Angriffsfläche ist gesamtgesellschaftlich gesehen riesig. Als Daumenregel gilt, dass es in technischen Geräten jeweils pro 2'500 Codelinien einen Fehler gibt.[100] Ein Android Mobiltelefon enthält um die 12 Mio. Codelinien, d.h. es gibt pro Gerät etwa 5'000 potenzielle technische Sicherheitslücken. Hochgerechnet auf die gesamte Gesellschaft ergeben sich folglich eine enorme Anzahl technischer Sicherheitslücken. Dabei handelt es sich auch um durch die Hersteller nicht vorausgesehene oder unbekannte Fehler oder Systemschwächen.[101] Sicherheitslücken können i.d.R. so lange ausgenutzt werden bis man diese identifiziert hat, Software-Entwickler diese Lücke schliessen können und Endnutzer einer Software oder eines Geräts das verbesserte Programm auch effektiv installieren.[102] Den Herstellern und Nutzern unbekannte Sicherheitslücken in Programmen oder Netzwerken – sog. »Zero-Day-Lücken« – sind deshalb besonders gefährlich.[103] Indem Hersteller und Nutzer keine Vorlaufzeit, also null Tage haben (daher der Name »Zero-Days«), um den Fehler zu beheben[104], bleibt das System nämlich so lange angreifbar, bis die Lücke entdeckt und effektiv (mittels Installation durch den Endnutzer) geschlossen wird.

Grundsätzlich gibt es verschiedene Wege, um Sicherheitslücken auszunutzen und damit in ein System einzudringen.[105] Ist das betreffende System an das Internet geschlossen, kann diese Sicherheitslücke grundsätzlich von überall auf der Welt erreicht und ausgenutzt werden. Das einleitend angeführte Beispiel des Computerwurms Stuxnet, mit dem 2010 die iranische Atomanlage beschädigt wurde, hat ferner gezeigt, dass das Internet nur einer von meh-

98 Burkart/McCourt, S. 3.

99 Singer/Friedman, S. 37.

100 Zegart, TED vom 29.06.2015.

101 Zegart, TED vom 29.06.2015. Zu Beispielen von gefährlichen (und ausgenutzten) Sicherheitslücken im Jahr 2022: Tavares, Infosec vom 17.08.2022.

102 Dewar, Contextualizing, S. 6.

103 Burkart/McCourt, S. 3; Dewar, Contextualizing, S. 6; Greenberg, Sandworm, S. 5 ff. Zu einer Definition von Zero-Day-Lücken siehe unter: ENISA, Glossary, Zero-Day (Stand 2023). Zu einer eingehenden Abhandlung zu Zero-Day-Lücken und deren Ausnutzungsprogrammen: Ablon/Bogart.

104 Greenberg, Sandworm, S. 5.

105 Burkart/McCourt, S. 3 nennt bspw. Drucker, Router, USB-Speicherstifte, E-Mail Anhänge oder infizierte Webseiten.

reren möglichen Angriffspfaden ist. Der Iran hatte das Nuklearprogramm von Natanz nämlich bewusst nicht an das Internet geschlossen.[106] Der Computerwurm konnte dennoch mittels USB-Speicherstift oder der Programmierung durch einen Menschen vor Ort eingeführt werden und ist von da aus selbständig über die intern vernetzten Systeme zum Kontrollsystem vorgedrungen.[107] Das heisst, es gehen immer auch Risiken von menschlichen Akteuren aus, die ohne Internet direkt in ein Computersystem eindringen können.

Der Radius potenzieller Schädigungen wird zusätzlich erweitert, indem zunehmend vorprogrammierte Schadprogramme zur Verfügung gestellt und eingesetzt werden, die in automatisierter Weise auf Sicherheitslücken abzielen.[108] Gemäss LENDERS gibt es zudem Risiken und Angriffsflächen in der Cybersicherheit, die wir noch gar nicht kennen.[109] Dies könne z.B. bei kritischen Infrastrukturen, bei denen unübersichtliche Abhängigkeiten bestehen, der Fall sein. Als Beispiel nennt er die als dezentrale Infrastruktur ausgestaltete Stromversorgung, bei der viele beteiligte Zulieferer zusammenarbeiten. Es bestehe hier die Möglichkeit von Risiken und Schädigungsmöglichkeiten, die sich nicht einfach erkennen lassen.[110] Beispielsweise kann mittels eines simplen Hackerangriffs ein Türschloss gesperrt werden. Wenn jenes Türschloss allerdings zu einem Gebäude einer kritischen Infrastruktur führt, kann dies schwere Folgen haben.[111] Mit der fortschreitenden Digitalisierung lassen sich Abhängigkeiten von Computersystemen und -netzwerken somit kaum mehr überblicken. Technische Lücken bleiben als solche oftmals unerkannt und sind dadurch sehr schwierig zu schützen.[112] Insgesamt bedeuten diese Entwicklungen für unsere global vernetzte Welt somit eine neue Dimension sicherheitspolitisch relevanter Risiken, die man adressieren muss.

106 SPRINGER, Cyber Warfare, S. 31.

107 SPRINGER, Cyber Warfare, S. 31.

108 DEWAR, Contextualizing, S. 4, S. 7 Tabelle 1 ("*attacker is an algorithm*"); DEWAR, Cyberweapons, S. 12 f.; PATTERSON, Tech Republic vom 01.06.2017.

109 BETSCHON, Interview mit Lenders, NZZ vom 05.12.2019.

110 BETSCHON, Interview mit Lenders, NZZ vom 05.12.2019. Zum ungenügenden Schutz des Schweizer Stromnetzes gegen Cyberangriffe siehe auch: MÄDER, NZZ vom 02.07.2021.

111 BETSCHON, Interview mit Lenders, NZZ vom 05.12.2019.

112 BETSCHON, Interview mit Lenders, NZZ vom 05.12.2019.

b. Unübersichtliche, hybride Akteurskonstellationen

Statistiken zufolge geht der Grossteil von Cyberangriffen durch von Staaten völlig oder teilweise unabhängigen privaten Akteuren aus.[113] Man geht allerdings davon aus, dass Cyberangriffe auch von staatlichen Akteuren ausgeübt werden.[114] Es ist dabei jedoch schwierig, einem Staat nachzuweisen, dass er hinter einem Angriff steht, da Angriffsursprünge technisch schwer zurückzuverfolgen sind. Durch sog. »IP-Spoofing« können sich Angreifer in andere Computer oder Computernetzwerke bzw. in deren IP-Adressen[115] hacken und diese zweckentfremden.[116] Dies macht es extrem schwierig zu eruieren, von *wem* ein Angriff tatsächlich initiiert wurde. Aufgrund dieser weitgehenden Anonymität hinter Angriffen müssen Statistiken zu Akteursgruppen daher jeweils relativiert werden. Man muss davon ausgehen, dass eine unklare Anzahl staatlicher Angriffe mangels technischer Beweise in die statistisch erfasste Kategorie privater Angriffe fallen könnten. Man sollte deshalb bei staatlich lancierten Cyberangriffen von einer Dunkelziffer ausgehen.[117] Hinzu kommt, dass die Akteursfrage nicht nur in quantitativer Hinsicht relativ unklar, sondern auch inhaltlich komplex ist. Es besteht (u.a. aufgrund der mangelnden technischen Zurückverfolgung) ein unklares Verhältnis von staatlichen und nichtstaatlichen Akteuren sowie ein kreuzweises Zusammenkommen politischer, krimineller, terroristischer und ideologischer Motive. Es findet also – und dies macht die Thematik so anspruchsvoll – eine kontinuierliche und wechselseitige Cyberaktivität zwischen verschiedenen Akteuren und Zielen statt.[118] Analysen verschiedener Cybervorfälle zeigen, dass private Akteure gewillt und

113 Zu übersichtlichen Statistiken hierzu siehe Passeri, Hackmageddon vom 16.02.23.

114 Dewar, Contextualizing, S. 4.

115 Im Glossar des Tallinn Manuals 2.0 auf S. 566 wird die Internet-Protokoll (IP-) Addresse wie folgt umschrieben: »A *unique identifier for a device on an IP network, including the Internet*.« Dazu wird auf den Begriff der Internet Assigned Numbers Authority (iana) verwiesen. Zu »spoofing« siehe S. 567 sowie S. 91 R15 C15.

116 Zu einem fundierten Bericht: Lipson, insb. S. 14. Ferner: Banks, S. 165; Brenner, S. 32; Singer/Friedman, Cybersecurity, S. 33: »A *sophisticated user can easily hide or disguise her IP address by routing her activities through another point on the Internet, making it appear that that node was responsible for the original traffic*«; Dunn Cavelty, ETH Zukunftsblog vom 18.01.2018; Schulze, S. 45; Woltag, S. 29 m.w.H.

117 Auch gem. Dewar ist die Erstellung einer kompletten Abbildung internationaler Cybervorfälle eine Herausforderung, da viele Cybervorfälle im privaten und staatlichen Sektor u.a. aufgrund möglicher Reputationsschäden ungemeldet bleiben: Dewar, Contextualizing, S. 3.

118 Dewar, Contextualizing, S. 13.

in der Lage waren, durch Cyberkampagnen staatliche Prozesse zu beeinflussen, indem eine oder die andere Seite eines Konflikts unterstützt wurde.[119] So könnten sowohl Private (oder hinter Privaten versteckte Staaten) als auch Staaten (weitgehend anonym) Cyberangriffe lancieren, die das Vertrauen in eine nationale Regierung untergraben oder gar Regimewechsel anstossen.[120] Einerseits können daher nichtstaatliche Akteure zunehmend mittels Cyberangriffen auf staatliche Angelegenheiten einwirken.[121] Andererseits können auch Staaten vermehrt in einem Zusammenhang mit nichtstaatlichen Cyberangriffen stehen.[122] Dies zeigt, dass sich die Grenzen zwischen privaten und staatlichen Cyberhandlungen sowie die privaten und staatlichen Einflussnahmemöglichkeiten in Bereichen nationaler Relevanz zunehmend verwischen und folglich beträchtliche Asymmetrien bestehen.[123]

Die Komplexität der Thematik wird zusätzlich dadurch erhöht, dass Cybertechnologien sowie das Internet für die allgemeine Öffentlichkeit frei zugänglich sind.[124] Grundsätzlich kann sich jedes Individuum mit genügend hohem Aufwand in ein anderes System hacken.[125] Hinzu kommt, dass schädigende, teilweise bereits auf die automatisierte Ausnutzung (konkreter) technischer Verletzlichkeiten vorprogrammiere Computerprogramme einfach und relativ günstig für die Öffentlichkeit zugänglich sind.[126] Dies ermöglicht es auch weniger talentierten Hackern, relativ grosse Angriffe zu tätigen. Zudem kann (aus der Ferne) mit einem öffentlichen zur Verfügungstellen von Schadprogrammen auch simultan eine hohe Anzahl ziviler Personen mobilisiert werden, um Cyberangriffe auszuführen. Im Zusammenhang mit den Angriffen auf Georgien z.B. konnte man auf öffentlich zugänglichen Webseiten vorprogrammierte DDoS-Angriffe runterladen. Die Webseite <www.stopgeorgia.ru> bspw. war explizit darauf ausgerichtet, einer breiten Öffentlichkeit, und damit auch technologisch unerfahrenen Personen, Angriffe auf georgische Regierungs-

119 Dewar, Contextualizing, S. 6, (siehe seine Tabelle von Cybervorfällen in den fünf analysierten Konflikten) S. 15 f.

120 Dewar, Contextualizing, S. 12.

121 Dewar, Contextualizing, S. 6. Siehe auch: Bussolati, S. 102 ff., S. 104 ff.

122 Dewar, Contextualizing, S. 6.

123 Dewar, Contextualizing, S. 6.

124 Eriksson/Giacomello, S. 222.

125 Joyner/Lotrionte, S. 832; Schmitt, Computer Network Attack, S. 897; Schulze, S. 23; siehe Bodungen et al., die erklären, wie durch Viren (wie z.B. Stuxnet) technische Sicherheitslücken und Angriffskanäle ausgenutzt und kritische Prozesse gestört werden können.

126 Singer/Friedman, S. 43.

webseiten zu ermöglichen.[127] Dies bedeutet einerseits eine global zunehmende Anzahl cyber-kompetenter Akteure (mitunter auch finanzschwache Länder und weitere nichtstaatliche Akteure).[128] Andererseits steigt dadurch wohl auch künftig die Unübersichtlichkeit staatlich-privater Cyberaktivitäten erheblich.

Insgesamt erhöhen die hybriden Akteurskonstellationen, die zunehmend vernetzten Sicherheitslücken und die unübersichtlichen Abhängigkeiten von digitalen Infrastrukturen die Komplexität von sicherheitspolitischen Risiken.[129] Die Angreifer (»wer«), die technischen Mittel (»was«) sowie die ausnutzbaren Systemschwächen (»wie«) haben allesamt in qualitativer und quantitativer Hinsicht zugenommen[130] – und werden dies wohl weiterhin tun. In modernen Gesellschaften müssen Risiken für einen Staat aufgrund des Internets nicht mehr von einem spezifischen Territorium ausgehen. Vielmehr bestehen sie gerade darin, dass die ganze Welt zunehmend vernetzt ist.

2. Anhaltende Unklarheiten bezüglich der Anwendung von Völkerrecht

Innerhalb der internationalen Gemeinschaft besteht mittlerweile der grundsätzliche Konsens, dass Völkerrecht auf staatliches Verhalten im Cyberraum anwendbar ist. Dennoch divergieren die Haltungen der Staaten und der Lehre bezüglich der konkreten Auslegung der einzelnen Normen und teilweise auch bezüglich der Notwendigkeit weiterer Regelungsgrundlagen.[131] Aus dem am 10. März 2021 veröffentlichten finalen Bericht der OEWG sowie den staatlichen Positionen im Rahmen der jüngsten UN GGE 2021 wird ersichtlich, dass innerhalb der Staatengemeinschaft weiterhin ein Interesse besteht, die Anwend-

127 Woltag, S. 45.

128 Dazu, dass die Anzahl Akteure quantitativ (und qualitativ) zunimmt, die Zugang zu technischen Instrumenten haben: Dewar, Contextualizing, S. 4.

129 Dewar, Contextualizing, S. 4.

130 Dewar, Contextualizing, S. 4.

131 Russland und China z.B. sprachen sich lange Zeit für eine separate vertragliche Regulierung staatlichen Verhaltens bzw. für einen Code of Conduct aus, während die USA, GB, die Schweiz und weitere Staaten für die Anwendung geltender Völkerrechtsnormen plädierten: siehe z.B. in UN Doc. A/68/156 (2013), S. 18 f.; Raltchev, S. 82. Die UN GGE 2015 hat den Vorschlag eines Code of Conducts für Informationssicherheit zwar erwähnt. Allerdings hat sich die UN-Expertengruppe in ihrem Konsensbericht (UN Doc. A/RES/70/174 (2015)) auf die Anwendbarkeit des traditionellen Völkerrechts geeinigt, woduch ein separater Code of Conduct nicht weiter verfolgt wurde. Siehe dazu: Rõigas/Minárik, CCDCOE Incyder News vom 31.08.2015.

barkeit von Völkerrecht auf Cyberangriffe zu klären.[132] *Bis dato* besteht des Weiteren noch keine klare Staatenpraxis zu staatlich provozierten Cyberangriffen. Unlängst gab es zwar vereinzelte staatliche Reaktionen auf Cyberangriffe: Namentlich die kinetische Reaktion Israels auf (vermeintlich) palestinänsische Cyberangriffe[133], die Sanktionen der Biden-Administration gegen Russland mitunter als Reaktion auf die SolarWinds-Cyberangriffe[134] sowie die EU-Cyber-Sanktionen gegen juristische und natürliche Personen, die im Zusammenhang mit schädigenden Cyberangriffen gesehen werden.[135] Diese Reaktionen bieten zwar Anhaltspunkte, wie Völkerrecht seitens dieser Staaten angewendet werden könnte. Angesichts der anhaltenden Konsensfindungsschwierigkeiten zwischen den Staaten im Rahmen der multilateralen UN-Prozesse ist es aus vorliegender Sicht allerdings fraglich, ob diese überwiegend unilateral ergriffenen Massnahmen als sich etablierende Staatenpraxis gewertet werden können und sollen. Deshalb können gerade auch Beiträge aus der Wissenschaft und weiterer unabhängiger Betrachter hilfreich sein. Des Weiteren wurden bisher sicherheitspolitisch relevante Cyberangriffe von Opferstaaten noch nicht dem UN-Sicherheitsrat vorgelegt[136] und haben

132 OEWG, finaler Bericht vom 10.03.2021, §40. Während im Rahmen der UN GGE 2021 staatliche Positionen zwar die Anwendbarkeit spezifischer Völkerrechtsnormen bejahen, bleiben die Auslegungsfragen derselben im Einzelnen immer noch eher vage. Siehe: UN Doc. A/76/135 (2021) und UN Doc. A/76/136 (2021).

133 Doffman, Forbes vom 06.05.2019; Borghard/Schneider, Washington Post vom 09.05.2019. Eingehender und m.w.V. siehe die Homepage: CCDCOE, Israeli Attack against Hamas Cyber Headquarters in Gaza 2019. Zu späteren Entwicklungen i.Z.m. Israel: Mimran/Shany, Lawfare vom 30.12.2020.

134 Siehe: The White House, Statements and Releases vom 15.04.2021; Executive Order 14024 vom 15.04.2021.

135 Am 30. Juli 2020 hat der Europarat erstmals Sanktionen als Reaktion auf Cyberangriffe lanciert. Diese sind Teil der sog. EU "Cyber Diplomacy Toolbox". Siehe: Europäischer Rat, Pressemitteilung vom 30.07.2020. Weitere Sanktionen wurden i.Z.m. den Angriffen auf den Bundestag von 2015 lanciert: Europäischer Rat, Pressemitteilung vom 22.10.2020. Dazu nachfolgend näher unter IV.B.2.e).

136 Raltchev, S. 82. Dies bleibt der Stand im Mai 2022.

zu keinen international-rechtlichen Gerichtsurteilen[137] geführt, weshalb sich auch noch keine völkerrechtliche Rechtsprechung zu Cyberangriffen etabliert hat.[138] Somit bestehen im Hinblick auf die Anwendung von Völkerrechtsnormen insgesamt weiterhin Unklarheiten und Klärungsbedarf. Für die internationale Stabilität bleibt es daher wichtig, den Dialog zwischen den Staaten aufrechtzuhalten, auch wenn nur schleppende inhaltliche Erfolge erzielt werden.[139]

Neben dem zunehmenden, internationalen Bewusstsein, dass sich eine klare Regulierung des Cyberraums aufdrängt, werden vermehrt auch nationale Cyberstrategien entwickelt.[140] Dabei hängen die staatlichen Positionen im Rahmen der UNO oftmals eng mit den betreffenden nationalen Cyberstrategien zusammen. In Bezug auf eine fundierte Auslegung von Völkerrecht gehen die Strategien allerdings nicht fundamental über den allgemeinen Konsens der Staatengemeinschaft oder über die staatlichen Positionen hinaus, dass bestimmte Völkerrechtsnormen anwendbar sind.[141] Insoweit fördern sie zwar in massgeblicher Weise die Transparenz und Offenlegung staatlicher Ansichten, aber tragen zur abschliessenden Klärung des »Wie« der völkerrechtlichen Anwendung nur marginal bei. Bemerkenswert ist dennoch, dass prominente Cyberstrategien wie die der USA oder Grossbritanniens (obschon zum grundsätzlichen Zwecke der Verteidigung) zunehmend offensiv ausgerichtet sind. Die USA manifestieren dabei seit 2011 die grundsätzliche Bereitschaft auf digitale und kinetische militärische Massnahmen zurückzugreifen, um sich gegen

137 Mikanagi/Mačák, S. 56 allerdings m.V.a. das am IGH hängige Urteil "Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination" (Ukraine v Russian Federation), CR 2017/1 vom 06.03.2017. Darin wurde Russland auf S. 22 §5 beschuldigt, u.a. in Cyberangriffe gegen die Ukraine involviert gewesen zu sein. Der IGH hat in seinem diesbezüglichen Urteil vom 08.11.2019 seine Zuständigkeit in der Sache erklärt und die Fristen zur Einreichung weiterer Stellungnahmen durch die Verordnung vom 08.10.2021 bis Dezember 2022 verlängert.

138 Raltchev, S. 83. Dies bleibt der Stand im Mai 2022.

139 Siehe dazu: Lauber/Eberli, S. 2 ff.

140 Die Schweiz hat mit der NCS-II ihre Nationale Cyber Strategie für die Jahre 2018-2022 veröffentlicht. Zu weiteren nationalen Cyberstrategien: Baezner/Cordey.

141 Vgl. seitens der Schweiz: NCS-II, S. 25; seitens USA: U.S. National Cyber Strategy 2018, S. 20 ff.

Cyberangriffe zu verteidigen.[142] Obschon also der regulatorische internationale Rahmen im Zusammenhang mit Cyberangriffen (insb. auf dem multilateralem Weg) noch klärungsbedürftig ist, lassen jüngere Entwicklungen in vielen Staaten eine massive Aufstockung digitaler Verteidigungskapazitäten beobachten.[143] Einige Staaten setzen dabei auch vermehrt auf sog. »aktive Cyberverteidigung«, das heisst auf offensive digitale (Verteidigungs-)Kapazitäten.[144] Diese sollen, grob zusammengefasst, als Reaktion auf einen Cyberangriff lanciert werden können, der staatliche Interessen beeinträchtigt.[145]

Unter »aktiver Cyberverteidigung« werden generell über passive digitale Schutzmassnahmen hinausgehende Massnahmen verstanden.[146] Passive Massnahmen umfassen namentlich Firewalls, Patches, Antiviren-Software oder digitale Mittel zu technischen Investigationszwecken von Angriffen.[147] Passive Massnahmen beschränken sich grundsätzlich darauf, Cyberangriffe zu erkennen oder zu neutralisieren, ohne dabei einen offensiven Gegenangriff gegen eine Angriffsquelle zu starten.[148] Das heisst, passive Mittel verlassen das vom Angriff betroffene Computersystem grundsätzlich nicht, womit sie i.d.R. keine

142 Siehe die U.S. International Strategy for Cyberspace 2011 unter der Obama-Administration, S. 14. Der US-Kongress billigte den Einsatz von offensiven digitalen Gegenmassnahmen des Militärs zu Verteidigungszwecken im U.S. National Defense Authorization Act for Fiscal Year 2012 unter Abschnitt F, 125 Stat. 1551, Sektion 954.

143 So setzen insb. die USA und Grossbritannien verstärkt auf aktive Cyber-Verteidigung. Siehe die Tabelle zur Cyber-Verteidigungspolitik nach Ländern von Dewar, Active Cyber Defense, S. 14. Zur nationalen Cyberpolitik Russlands: Soldatov/Borogan, S. 15 ff.

144 Zum zunehmend offensiven Ansatz Grossbritanniens: PM, Oral Statement to Parliament vom 19.11.2020 sowie insb. Teil fünf der nationalen Strategie: UK National Cyber Strategy 2022. Diese Entwicklungen kommentierend u.a.: Corera, BBC News vom 20.11.2020; Sabbagh, The Guardian vom 19.11.2020; Warell, Financial Times vom 19.11.2020. Seit der Veröffentlichung der U.S. Cyber Strategie im September 2018 unter der Trump-Administration verfolgen auch die USA eine offensive Strategie. Siehe: U.S. National Cyber Strategy 2018. Siehe ferner die Verteidigungsstrategien: U.S. DoD Cyber Strategy 2011 und U.S. DoD Cyber Strategy Summary 2018. Auch die Ansätze der Biden-Administration sind *bis dato* ähnlich ausgelegt. Siehe: The White House, Interim National Security Strategic Guidance 2021. Zu diesen Entwicklungen auch: Lahmann, S. 125 m.w.V.

145 Lahmann, S. 125 m.V.a. Hathaway et al., S. 858; Sklerov, S. 10 ff. Ähnlich: Roscini, World Wide Warfare, S. 113 f. (allerdings mit Verweis auf das Verhältnismässigkeitserfordernis).

146 Lahmann, S. 125.

147 Zu verschiedenen Möglichkeiten defensiver Massnahmen: Denning, Information Warfare, S. 285 ff., S. 345 ff. (zum Begriff der Firewall) S. 353. Zu weiteren Massnahmen wie Antiviren-Software: Herrmann/Pridöhl, S. 27 f.

148 Lahmann, S. 125; Tallinn Manual 2.0, Glossar, S. 566.

Rechte Dritter (im In- und Ausland) beeinträchtigen und nicht völkerrechtlich gerechtfertigt sein müssen.[149] Einigen Ansichten zufolge reichen passive Massnahmen allerdings nicht aus, um betroffene Systeme vor digitalen Beeinträchtigungen zu schützen.[150] So seien diese zwar sinnvoll und auf allen Computersystemen erforderlich, würden jedoch nur einen begrenzten Schutz bieten[151] – insb., wenn heikle Systeme kritischer Infrastrukturen betroffen seien.[152] Demzufolge müsse – zumindest einer vor allem in den USA verbreiteten Ansicht zufolge – eine aktive digitale Verteidigung möglich sein, um Angreifer »abzuschrecken und zu bestrafen«.[153] Zugleich hat sich – und dies ist für den vorliegenden Kontext relevant – noch keine einheitliche Definition oder ein gemeinsames Verständnis darüber etabliert, was das Konzept aktiver Cyberverteidigung überhaupt konkret umfasst.[154] Grob zusammengefasst geht es, wie gesagt, überwiegend um Massnahmen, die über passive Massnahmen hinausgehen. Damit sind sie grundsätzlich gegen ein (Ursprungs- oder auch gegen ein durch IP-Spoofing missbrauchtes) Angriffssystem gerichtet. Daher bewegt man sich mit aktiven Massnahmen grundsätzlich ausserhalb der eigenen Cyberinfrastrukturen.[155] Dabei können auf oder mittels des betreffenden fremden Systems potenzielle (Folge-)Schädigungen ausgelöst werden, was für die völkerrechtliche Würdigung relevant sein kann.

Nationale Cyberstrategien ersetzen, wie bereits angedeutet, einen für Anwendungsfragen von Völkerrecht erforderlichen internationalen Konsens nicht. Dennoch haben Schätzungen zufolge trotz der anhaltenden Unklarheiten in Bezug auf das technische Konzept aktiver Cyberverteidigung sowie in Bezug auf seine grundsätzliche Legalität[156] um die 60 Länder bereits offensive digitale Kapazitäten entwickelt.[157] Einige Staaten etablieren in dieser Hinsicht

149 Lahmann, S. 125.

150 Sklerov, S. 8, S. 26.

151 Jensen, Critical National Infrastructure, S. 239 f. Ähnlich: Kesan/Hayes, S. 474 f. Ausführlicher dazu, dass passive und aktive digitale Verteidigungsmassnahmen gemeinsam eingesetzt werden sollten, um effektiv zu sein: Dewar, Active Cyber Defense, S. 16.

152 Colarik, S. 10; Lahmann, S. 125; Lehtinen/Russell/Gangemi; Sklerov, S. 8.

153 Jensen, Critical National Infrastructure, S. 239 f.

154 Dewar, Active Cyber Defense, S. 7; Giles/Hartmann, S. 23; Lahmann, S. 125.

155 Lahmann, S. 126; Tallinn Manual 2.0, Glossar, S. 563.

156 Vgl. Kesan/Hayes, S. 475.

157 Sabbagh, The Guardian vom 19.11.2020. Ähnlich: Halberstam, S. 204 m.V. in Fn. 35. Dazu auch: Kerschischnig, S. 90 ff. insb. unter Erwähnung der USA, China, Russland, der EU und der NATO.

sogar eigene militärische Cyber-Kommandos[158], die zunehmend und explizit auch auf offensive Cyberkapazitäten setzen, die Gegner aktiv beeinträchtigen (»*disrupt*«) können sollen.[159] Dabei ist gerade in den USA eine Tendenz zu erkennen, sich für die Legalität aktiver Cyberverteidigung von Staaten auszusprechen.[160] Auch der Schweizer Bundesrat hat am 31. März 2021 entschieden, dass die Führungsunterstützungsbasis der Armee bis Anfang 2024 in ein Kommando Cyber weiterentwickelt werden soll.[161] Obwohl die Schweiz einen primären Fokus auf Resilienz und auf den (passiven) Schutz ihrer militärischen Netzwerkinfrastrukturen hat, sind aktive Verteidigungsmassnahmen in ausländischen Computernetzwerken seit dem Inkrafttreten des revidierten Nachrichtendienstgesetzes am 1. September 2017 punktuell erlaubt. Mit bundesrätlicher Genehmigung kann der Nachrichtendienst gem. Art. 37 Abs. 1 NDG in sich im Ausland befindliche Computersysteme und -netzwerke eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen, wenn diese Computersysteme und -netzwerke für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet wurden.[162]

Nationale Entscheidungen, mit (militärischen) Massnahmen auf transnationale Cyberangriffe zu reagieren, können durch die Etablierung von Staatenpraxis die Auslegung des Völkerrechts beeinflussen. Zugleich müssen sie dem bestehenden internationalen Völkerrechtsrahmen jedoch standhalten, wenn sie einen anderen Staat tangieren. Wie erwähnt, ist es im Einzelnen *bis dato* umstritten, wie die völkerrechtliche Selbstverteidigung im Cyberkontext konkret anzuwenden ist. Dies gilt daher auch für die Völkerrechtskonformität aktiver digitaler und kinetischer Verteidigung.[163] Somit ist es insb. im Hinblick auf das militärische Verhalten von Staaten wichtig zu klären, wann (und ob) ak-

158 Mit Beispielen verschiedener Staaten u.a.: Clarke/Knake, Cyber War, S. 33 ff.; Schulze, S. 3, S. 14 f. Siehe z.B. das U.S. Cyber-Kommando unter <https://www.cybercom.mil> (zuletzt besucht: März 2023); Nakashima, Washington Post vom 27.01.2013. Zur Nationalen Cyberstreitkraft Grossbritanniens siehe <https://www.gov.uk/government/organisations/national-cyber-force> (zuletzt besucht: März 2023); UK Ministry of Defence et al., News Story vom 27.06.2018. Unlängst haben sich die Streitkräfte der USA und Grossbritanniens sogar zusammengeschlossen: Corera, BBC News vom 18.11.2021.

159 Siehe: U.S. Cyber Command Public Affairs, News vom 10.09.2020; UK Ministry of Defence et al., News Story vom 19.11.2020. Kritisch hierzu: Sabbagh, The Guardian vom 19.11.2020.

160 Jensen, Critical National Infrastructure, S. 239 f.

161 Der Bundesrat, Medienmitteilung vom 31.03.2021. Zur verabschiedeten Botschaft: Der Bundesrat, Medienmitteilung vom 01.09.2021.

162 Siehe Art. 2 Abs. 1 der Verordnung über die militärische Cyberabwehr (MCAV).

163 Kesan/Hayes, S. 475; (i.Z.m. digitalen Verteidigungsmassnahmen durch Private, die aufgrund von Unklarheiten politische Konsequenzen haben könnten) Owens et al., S. 37.

tive (kinetische und/oder digitale) Verteidigungsmassnahmen völkerrechtlich erlaubt sind. Offensive militärische Massnahmen, wenn auch zwecks Verteidigung lanciert, können selbst völkerrechtswidrig sein, wenn sie die Rechte eines anderen Staats verletzen und dabei nicht völkerrechtlich gerechtfertigt sind. Die einzige Rechtfertigung auf dem Weg der Selbsthilfe, militärisch (gewaltsam) in einen anderen Staat einzudringen, besteht in der ausnahmsweisen Situation eines bewaffneten Angriffs gem. Art. 51 UN-Charta, die das Recht auf eine verhältnismässige[164] Selbstverteidigungsmassnahme auslöst. Ausserhalb des Anwendungsbereichs der Selbstverteidigung gibt es auf dem unilateralen Weg der Selbsthilfe, wie einleitend bereits erwähnt, nur die Möglichkeit *nicht-militärischer* Gegenmassnahmen. Dazu müsste eine entsprechende Völkerrechtsverletzung (z.B. die des Gewalt- oder Interventionsverbots) gegeben sein. Alternativ zur Selbsthilfe können sich Staaten an den Sicherheitsrat oder an ein internationales Gericht wenden.[165]

Die UN GGE von 2015[166] hat neben der grundsätzlichen Anwendbarkeit des traditionellen Völkerrechts (trotz vehementer Debatten innerhalb der Verhandlungen[167] und vor allem auf Insistieren westlicher Staaten hin[168]) auch die Anwendbarkeit der Selbstverteidigung gem. Art. 51 UN-Charta im Cyberkontext bejaht.[169] Die Konturen von Art. 51 UN-Charta im Zusammenhang mit Cyberangriffen sind *bis dato* allerdings umstritten. Auch die Frage, wie völkerrechtliche Gegenmassnahmen im Cyberkontext konkret anzuwenden sind, ist im Einzelnen noch unklar.[170] Die Anwendbarkeit völkerrechtlicher Gegenmassnahmen war mitunter eines der Hauptthemen, an dem innerhalb der UN GGE 2017 der Konsens scheiterte.[171] Obschon die Anwendbarkeit von Gegenmassnahmen im Rahmen der UN GGE 2021 von den meisten Staaten zwar

164 Dazu ausführlicher nachfolgend unter Teil III.B.1. und IV.A.

165 Vgl. Diggelmann/Hadorn, S. 261.

166 Indem in der UN GGE 2015 (basierend auf einem geographischen Verteilschlüssel) 20 Länder vertreten waren – darunter »Schlüssel-Cybermächte« wie die USA, China, Russland, Frankreich, Grossbritannien und Deutschland – wurde dieser Konsens als global repräsentativ erachtet: Rõigas/Minárik, CCDCOE Incyder News vom 31.08.2015. Seit im März 2021 die *allen* Staaten offene OEWG ihren finalen Bericht verabschiedet hat, ist die Globalität jedoch spätestens gegeben.

167 Kuba z.B. sprach sich gegen die Anwendbarkeit der Selbstverteidigung auf Cyberoperationen aus: Rodríguez, Deklaration vom 23.06.2017.

168 So z.B. der USA in UN Doc. A/66/152 (2011), S. 18.

169 Hinkle, S. 12 mit Beispielen in den Fussnoten; Schmitt/Vihul, Just Security vom 30.06.2017.

170 Vgl. Hinkle, S. 12; Egan, S. 177 f.

171 Schmitt/Vihul, Just Security vom 30.06.2017; Lotrionte, S. 93.

bejaht wurde, blieb die Frage nach dem konkreten Anwendungsbereich weiterhin unbeantwortet.[172] Dies hängt wohl auch damit zusammen, dass das Konzept von Gegenmassnahmen an sich bereits umstrittene Aspekte umfasst[173], dass sich unterschiedliche politische Haltungen gegenüberstehen[174] sowie aufgrund der beschriebenen Komplexität von Cyberangriffen. Demzufolge erfordern die bisherigen Ansätze (wie bspw. diejenigen in den Tallinn Manuals[175]) weiterer Klärung durch Staaten, Völkerrechts- und Cyberexperten.

3. Vernachlässigung des Verhältnismässigkeitsprinzips?

Die aufgezeigten Entwicklungen zeigen, dass der Fokus der Debatte *bis dato* sichtlich auf der Frage liegt, welche Völkerrechtsnormen durch offensive Cyberangriffe (*actio*) verletzt sein könnten. Die ebenso zentrale völkerrechtliche Würdigung von Verteidigungs- und Gegenmassnahmen als staatliche Reaktion (*reactio*) auf eine solche Normverletzung wurde eher vernachlässigt.[176] Da das Verhältnismässigkeitsprinzip im Zusammenhang mit Gegenmassnahmen sowie auch mit der Selbstverteidigung ein fundamentales Völkerrechtsprinzip darstellt[177], ist es für die rechtliche Würdigung staatlicher (Selbsthilfe-)Handlungen allerdings zentral. Es ist im herkömmlichen Kontext unbestritten, dass das Verhältnismässigkeitsprinzip für die Überprüfung staatlichen Handelns innerhalb von Konflikten bedeutend und relevant ist.[178] Das Prinzip dient im Grunde der Begrenzung und »Überwachung« einer Reaktion, um eskalato-

172 Dazu: UN Doc. A/76/136 (2021) (siehe die Schweizer Position zu Gegenmassnahmen auf S. 90). Estland hat eine eher extensive Auffassung von Gegenmassnahmen und spricht sich auf S. 28 bspw. sogar für die Anwendbarkeit *kollektiver* Gegenmassnahmen aus. Vgl. dazu: Schmitt, Just Security vom 10.06.2019.

173 Lotrionte, S. 92.

174 Vgl. Schmitt/Vihul, Just Security vom 30.06.2017.

175 Lotrionte, S. 92.

176 Die Verhältnismässigkeit fand z.B. keine Erwähnung im finalen Bericht der OEWG: OEWG, finaler Bericht vom 10.03.2021. Oft wird generell darauf verwiesen, dass Verteidigungs- und Gegenmassnahmen verhältnismässig sein müssen. Dabei wird oft nicht weiter ausgeführt, was die Verhältnismässigkeit konkret erfordert. Siehe dazu die staatlichen Positionen in UN Doc. A/76/136 (2021).

177 Cannizzaro, Countermeasures, S. 889; Franck, Proportionality, S. 716; Ferner: Cannizzaro, Contextualizing Proportionality, S. 779 ff.

178 Dazu u.a. Dinstein, Proportionality and Necessity, 54 ff.; Franck, Proportionality, S. 716 ff.; Newton, S. 29; O'Keefe, S. 1157 ff.

rische Gewaltspiralen zu verhindern.[179] Eine disproportionale Reaktion wäre folglich ungerechtfertigt[180] und würde ihrerseits Verantwortlichkeiten konstituieren.[181] Dies wirkt sich im Ergebnis oft auch darauf aus, wie (und ob) ein Konflikt letztlich gelöst wird.[182] Gerade angesichts der vorangehend erwähnten, jüngeren Entwicklungen, dass Staaten zunehmend digitale Verteidigungskapazitäten ausbauen, ist es deshalb wichtig rechtlich zu klären, welche staatlichen Selbstverteidigungs- und Gegenmassnahmen vor dem Hintergrund des Völkerrechts verhältnismässig sind.

Das Verhältnismässigkeitsprinzip ist nicht nur im Gegenmassnahmenrecht und im *ius ad bellum*, sondern auch im Zusammenhang mit internationalen Handelskonflikten zwischen Staaten[183] sowie für die *ius in bello*-Debatte wichtig.[184] Die Verhältnismässigkeit hat jedoch – und dies ist für die vorliegende Analyse der Legalität von Selbsthilfemassnahmen massgebend – je nach Kontext eine unterschiedliche Bedeutung. Für eine rechtliche Würdigung ist es daher massgebend, ob man sich im Bereich des *ius ad bellum*, innerhalb eines bewaffneten Konflikts (*ius in bello*)[185] oder innerhalb der völkerrechtlichen Staatenverantwortlichkeit gem. ARSIWA befindet.[186] Das Verhältnismässig-

179 Crawford, State Responsibility, S. 697. Franck, Proportionality, S. 715 umschreibt die Verhältnismässigkeit als »*a brake on escalating cycles of transactional violence*«, und auf S. 763 »*to keep countermeasures from spiraling out of control*«. Ähnlich auch: Kaikobad, S. 318; Wicker, S. 67.

180 Franck, Proportionality, S. 716.

181 ARSIWA-Kommentar, Art. 51(1); Crawford, State Responsibility, S. 698.

182 Franck, Proportionality, S. 716.

183 Franck, Proportionality, S. 715; O'Keefe, S. 1166 f.

184 Newton/May, S. 61 ff.; Gardam, Necessity, Proportionality, S. xv.

185 Im *ius in bello* spricht man i.Z.m. Verhältnismässigkeit insb. vom »Verlust und der Verletzung von Zivilisten, der Beschädigung ziviler Gegenstände oder einer Kombination daraus«, die in einem »Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Vorteil« stehen müssen. Siehe das Zusatzprotokoll I zu den Genfer Abkommen vom 12. August 1949, Art. 51(5)(b), Art. 57(2)(a)(iii) und 57(2)(b). Zur Unterscheidung der *ius ad bellum* und der *ius in bello*-Verhältnismässigkeit u.a: Sloane, Cost of Conflation, S. 108 f. Ähnlich: Dinstein, War, Aggression and Self-Defence, S. 251 f.

186 Siehe dazu: Newton/May, S. 33 ff. unter dem Titel »Proportionality: A Multiplicity of Meanings«. Zur Notwendigkeit, die *ius ad bellum*-Verhältnismässigkeit und die Verhältnismässigkeit der Staatenverantwortlichkeit zu unterscheiden auch: Schmitt, Countermeasures Response Option, S. 723 f. Näher dazu unter Kapitel IV. »Cyberangriffe und Verhältnismässigkeit«.

keitsprinzip lässt daher gewissermassen eine Limitierung und gleichzeitig jedoch eine Legitimierung staatlichen Handelns zu,[187] die je nach Rechtsbereich variieren und verschiedenen Zwecken dienen.

Dogmatisch ist die Verhältnismässigkeitsprüfung der Prüfung des Anwendungsbereichs einer Völkerrechtsverletzung nachgelagert. So drängt sich der Verhältnismässigkeitsdiskurs vor dem Hintergrund völkerrechtlicher Selbsthilfemassnahmen auf, wenn Staat A einen Angriff X lanciert hat, indem er z.B. durch einen Cyberangriff in Staat B einen Rüstungskonzern oder ein Elektrizitätswerk blockiert und funktionsunfähig macht (*actio*) und Staat B diesen unilateral als einen Völkerrechtsverstoss qualifiziert und darauf mit einer Gegenhandlung Y reagiert (*reactio*). Geprüft werden muss in diesem Kontext (meist retrospektiv) in einem ersten Schritt, ob die Ausgangshandlung X tatsächlich eine Völkerrechtsverletzung darstellt (z.B. durch die Verletzung des Interventionsverbots oder einen bewaffneten Angriff) und in einem zweiten Schritt, ob die Gegenhandlung Y im Verhältnis zu X verhältnismässig ist bzw. war.[188] Gemessen werden also nicht nur die Ausgangshandlung des Angreifers und deren Konsequenzen, sondern ebenso die Reaktionshandlung des sich Verteidigenden und deren Konsequenzen.

Insgesamt bleibt es sowohl für das Gegenmassnahmenrecht als auch das Selbstverteidigungsrecht schwierig (und unerwünscht[189]), eine exakte Schwelle der (Un-)Verhältnismässigkeit zu definieren.[190] Vor dem Hintergrund des ebenso vagen Konzepts von Cyberangriffen wirft die Anwendung und die Bedeutung des Verhältnismässigkeitsprinzips somit (weitere) schwierige Fragen auf. Da das Prinzip gerade im internationalen Diskurs um Gegenmassnahmen sowie im *ius ad bellum* von fundamentaler Bedeutung ist, soll es in der vorliegenden Dissertation mitsamt seiner inhärenten Flexibilität näher betrachtet werden. Dem völkerrechtlichen Verhältnismässigkeitsprinzip könnte gerade vor dem Hintergrund seines immanenten Ziels, übermässige Sanktionierung zu verhindern, eine zentrale Funktion zukommen. Demzufolge soll in Teil IV einerseits unter A) die Bedeutung und Ausrichung der Verhältnismässigkeit im Rahmen des *ius ad bellum* und andererseits unter B) im Rahmen der völkerrechtlichen Staatenverantwortlichkeit gem. ARSIWA aufgegriffen werden.

187 Newton/May, S. 33.

188 Vgl. Franck, Proportionality, S. 715.

189 Wicker, S. 7. Dazu später eingehender unter Teil IV.

190 Franck, Proportionality, S. 716. Vgl. ARSIWA-Kommentar, Art. 51(5).

4. Erwarteter Erkenntnisgewinn

Um ein für die Staaten voraussehbares, stabiles und friedliches internationales Umfeld zu etablieren, braucht es grundsätzliche Konsense im Hinblick auf die Auslegung relevanter Völkerrechtsnormen. Fehlen die Voraussehbarkeit und die Konsistenz von Normen, verlieren sie die Fähigkeit, durch reziproke Erwartungen Rechtssicherheit und internationale Stabilität zu schaffen.[191]

Die aufgezeigten Entwicklungen zeigen, dass in Bezug auf die Regulierung völkerrechtlich relevanten Verhaltens offene Fragen bestehen bleiben. Mitunter bleiben die vorliegend wegweisenden Fragen offen, welche Völkerrechtsnormen durch Cyberangriffe verletzt sein können und welche staatlichen Reaktionen völkerrechtlich verhältnismässig sind. Die komplexen Akteurskonstellationen und die zunehmenden technischen Verflechtungen stellen enorme, womöglich anhaltende Herausforderungen dar, um den sich (weiterhin) verändernden Untersuchungsgegenstand jeweils rechtlich zu erfassen. Da die von Cyberangriffen ausgehenden, sicherheitspolitischen Risiken aufgrund des Internets *global* sind, ist die gesamte Staatengemeinschaft gefordert. Dabei muss sie sich die Frage nach der (jeweils zu differenzierenden) Verhältnismässigkeit staatlichen Verhaltens im internationalen Umgang mit Cybertechnologien stellen.

Nationale Entscheide, die Auswirkungen auf andere Staaten haben, müssen immer auch völkerrechtlich zulässig sein – insb., wenn Staaten ihren Ruf als verlässliche Partner aufrechterhalten wollen. Neben technischen und politischen Bemühungen ist somit auch eine völkerrechtliche Perspektive gefragt.[192] Gerade angesichts der gegenwärtigen Entwicklungen gewisser Staaten, ihre (offensiven) militärischen Cyberkapazitäten auszubauen, drängt sich die Klärung der völkerrechtlich zulässigen Grenzen auf. Das Völkerrecht kann und soll zur Klärung beitragen, ob gewisse Massnahmen und Gegenmassnahmen erlaubt sind.[193] Der vorliegende völkerrechtliche Beitrag vermag dabei jedoch keineswegs abschliessende Lösungen für das weite, weiterhin politisch aufgeladene Gebiet der Cybersicherheit sowie für den Umgang mit den divergierenden Verständnissen zu internationalen Normen zu offerieren. Zudem kann das Völkerrecht nur insofern einen normativen Wert beanspruchen, als es politisch auch eingehalten und umgesetzt wird. Da Staaten allerdings wiederholt betonten, dass das Völkerrecht für den Cyberkontext relevant bleibt, sollen

191 Lahmann, S. 262 m.V.a. Luhmann, S. 147; Waldron.

192 Schulze, S. 2.

193 Schulze, S. 2.

dennoch wichtige Problemfelder aus der vorliegenden, völkerrechtlichen Sicht beleuchtet werden. Aufgrund des interdisziplinären Charakters der Thematik bleibt der hier vertretenen Ansicht nach für den künftigen Weg eine enge internationale Zusammenarbeit zwischen Vertretern technischer, politischer und rechtlicher Disziplinen unentbehrlich. Technische Verständnisse sind insofern relevant, als dass sie die rechtliche Erfassung des technischen Untersuchungsgegenstands ermöglichen. Ein Mehrwert dieser Dissertation soll demzufolge auch in der Bemühung liegen, die für eine rechtliche Beurteilung relevanten technischen Eigenschaften von Cyberangriffen zu erarbeiten und rechtlich brauchbare Kategorien zu schaffen. Dies soll es ermöglichen, den Untersuchungsgegenstand auch den Personen etwas näher zu bringen, die keine unmittelbare Nähe zu technischen Disziplinen haben. Es sollen zudem einige Grundsatzfragen zum völkerrechtlichen Verhältnismässigkeitsprinzip innerhalb des *ius ad bellum* sowie des Gegenmassnahmenrechts aufgegriffen werden, die über den Untersuchungsgegenstand hinausgehen. Diese Dissertation soll insofern den Diskurs zu Cyberangriffen und zu Aspekten des völkerrechtlichen Verhältnismässigkeitsprinzips um die vorliegende Betrachtung ergänzen.

III. Cyberangriffe und die konzeptuelle Abgrenzung von Krieg, Schädigung und Normverletzung

Die Debatte um die völkerrechtliche Erfassung von Cyberangriffen hat in den letzten Jahren in der Öffentlichkeit sowie in der Lehre enorme Aufmerksamkeit erlangt.[194] Prominent wurde dabei wiederholt auch der Begriff des »Cyberkriegs« diskutiert.[195] Dabei – und dies trägt zur Unübersichtlichkeit des Diskurses bei – wird der Begriff oft pauschal und fachübergreifend verwendet, und es wird nicht klar zwischen Cyberangriff und Cyberkrieg differenziert.[196] Die Definition »Cyberkrieg« ist dabei gerade vor dem Hintergrund des Völkerrechts irreführend. Für die vorliegende Dissertation ist es daher besonders wichtig, zwischen »Krieg« als rhetorische Figur[197] im politischen oder medialen Diskurs und »Krieg« als völkerrechtliches Konzept zu unterscheiden.[198] Aus völkerrechtlicher Sicht handelt es sich nämlich nur dann um einen Krieg, wenn es sich um einen bewaffneten Konflikt zwischen zwei oder mehreren Staaten oder im Rahmen eines völkerrechtlich definierten Bürgerkriegs handelt.[199] Es gibt somit dem vorliegendem Verständnis nach unzählige Cyberoperationen

194 Dazu etwa: Harrison Dinniss; Walter, S. 686.

195 Dazu u.a. Dunn Cavelty, ETH Zukunftsblog vom 15.06.2018; Rid, Cyberwar.

196 Siehe u.a. Hathaway et al., S. 822 f.; Schulze, S. 7; Singer/Friedman, S. 120; Woltag, S. 20.

197 Zur Rolle der Rhetorik im Diskurs um Cyberkrieg: Blank Laurie, Cyberwar, S. 76 ff.

198 Ähnlich: Lotrionte, S. 73.

199 Siehe dazu insb. die Genfer Abkommen vom 12.08.1949; Woltag, S. 20.

oder Cyberangriffe *ausserhalb* bewaffneter Konflikte, die die dazu erforderlichen Voraussetzungen (mitunter diejenigen gem. Art. 51 UN-Charta) nicht erfüllen (dazu nachfolgend unter III.B.1.).[200]

Die Abwesenheit gemeinsamer, einheitlicher Konzepte von Cyberangriffen erschwerte *bis dato* die Ausarbeitung koordinierter Regulierungsempfehlungen und Konsensfindungen.[201] Um einen Untersuchungsgegenstand zu regulieren und voraussehbare Sanktionsmechanismen zu bestimmen, sollte man diesen zuerst (immerhin in den Grundsätzen) verstehen. Damit Regulierungen effektiv und so wenig missbrauchsanfällig wie möglich sind, müssten zudem gemeinsame Verständnisse bezüglich der zentralen Definitionen des zugrundeliegenden Problems bestehen. Mitunter sind die Fragen nach dem erforderlichen Schaden oder anderweitigen Effekten sowie nach dem Kausalzusammenhang für die Bestimmung der Rechtsfolgen einer Verletzung relevant.[202]

Eine erste Herausforderung der vorliegenden Analyse ist somit, die politisch, medial und interdisziplinär verwendeten sowie international divergierenden Definitionsansätze rechtlich sinnvoll zu abstrahieren. Eine Definierung des vorliegenden Untersuchungsgegenstandes »Cyberangriff« erscheint unentbehrlich, um diesen konzeptuell einzugrenzen[203] und um diesen in einem separaten Schritt rechtlich würdigen zu können. Das heisst, es muss vorab definiert werden, was vorliegend unter den Untersuchungsgegenstand fällt. Danach kann in einem zweiten Schritt geprüft werden, ob die für diese Dissertation relevanten völkerrechtlichen Normen darauf anwendbar sind und wann man sich innerhalb jener Anwendungsbereiche bewegt.[204] Insbesondere drängt sich eine begriffliche Differenzierung angesichts der weitreichenden (rechtlichen und faktischen) Konsequenzen eines bewaffneten Konflikts auf. Innerhalb eines bewaffneten Konflikts bzw. eines Krieges greifen nämlich nur noch die rudimentären (»Auffang«-)Normen des humanitären Völkerrechts unter Aussetzung der generell geltenden Völkerrechtslage zu Friedenszei-

200 WOLTAG, S. 21.

201 HATHAWAY et. al., S. 822.

202 Vgl. SCHULZE, S. 66.

203 WOLTAG, S. 20.

204 HATHAWAY et al., S. 826. Eingehender zu den unterschiedlichen rechtlichen Kategorien nachfolgend unter III.B.

ten.[205] Krieg ist insofern eine moralisch und rechtlich problematische (Ausnahme-)Institution.[206] Ebenso ist es aus völkerrechtlicher Sicht zentral, Normverletzungen wie Gewaltanwendungen gem. Art. 2(4) UN-Charta von der rechtlichen Kategorisierung als bewaffneter Angriff gem. Art. 51 UN-Charta zu unterscheiden, da diese beiden Regime wiederum jeweils fundamental verschiedene Rechtsfolgen implizieren (näher dazu nachfolgend unter III.B.).[207] In einem ersten Schritt soll daher unter III.A. eine Definition des Untersuchungsgegenstandes erfolgen, die als Grundlage für die darauffolgende rechtliche Würdigung unter III.B. dienen soll.

205 Eingehender dazu sowie zur damit verbundenen Problematik, Cyberangriffe mit Krieg zu assoziieren: MAY, S. 3 ff., S. 12 ff. Innerhalb bewaffneter Konflikte greifen nur noch die Bestimmungen des *ius in bello* (insb. der Genfer Abkommen I-IV vom 12.08.1949). Siehe deren gemeinsamen Art. 2 und 3.

206 MAY, S. 3.

207 Zur Unterscheidung militärischer und nicht-militärischer Selbsthilfe siehe nachfolgend unter Teil IV.

A. Definition von Cyberangriffen und -schäden

1. Der effektbasierte Ansatz des Tallinn Manuals

Eine verbreitete Definition von Cyberangriffen ist diejenige gem. des Tallinn Manuals.[208] Cyberangriffe werden im Tallinn Manual als defensive oder offensive Cyberoperationen verstanden, bei denen vernünftigerweise davon auszugehen ist, dass sie Verletzungen oder den Tod von Personen, den Schaden oder die Zerstörung von Objekten verursachen.[209] Das Manual unterscheidet damit Angriffe und »gewaltlose« Operationen, wie reine Cyberspionage.[210] Angriffe müssen gem. Tallinn Manual folglich physisch-destruktive Effekte nach sich ziehen. Das heisst, dass für die Kategorisierung von Angriffen i.S. des Tallinn Manuals die *Konsequenzen* und nicht die Beschaffenheit einer Waffe (oder »das Instrument«) relevant sind.[211] Als Angriff würde demnach gelten, wenn bspw. durch eine Blockierung eines Computersystems ein Feuer ausgelöst wird.[212] Die Konsequenzen sollen sich dabei nicht auf kinetische Effekte beschränken, sondern könnten auch chemischer, biologischer oder radioaktiver Natur sein.[213] Es wird darauf verwiesen, dass auch solche Effekte unter Angriffe im völkerrechtlichen Sinne fallen können.[214] Schwierigkeiten bereitet dabei *de facto* insgesamt wohl die Frage, wie man einen durch Cyberangriffe ausgelösten Schaden oder Zerstörung im Einzelnen misst und beziffert.[215]

---

208 Tallinn Manual 2.0, S. 415, R92 C2. Die Etablierung dieser Definition hat den Konsens der 19 involvierten Völkerrechtsexperten aus verschiedenen Ländern erfordert sowie Rückmeldungen vieler Staaten und weiteren Experten erhalten. Ausführlicher zur Ausarbeitung des Leitfadens siehe Tallinn Manual 2.0, S. 3 ff.

209 Tallinn Manual 2.0, S. 415.

210 Tallinn Manual 2.0, S. 415, R92 C2.

211 Tallinn Manual 2.0, S. 415, R92 C3.

212 Tallinn Manual 2.0, S. 415, R92 C3.

213 Tallinn Manual 2.0, S. 415, R92 C3.

214 Tallinn Manual 2.0, S. 415, R92 C3 m.V.a. IStGJ, Tadić-Berufungskammerentscheid, §120, 124 bezüglich chemischer Waffen.

215 Zur Schwierigkeit einer Schadensbemessung bei den DDoS-Angriffen auf Georgien und Estland siehe: Woltag, S. 44 f. und 46 m.w.V.

Darüber hinaus stellt sich die Frage, wie weit sich die Kausalität des ausgelösten Schadens erstrecken darf, um noch auf die ursprüngliche Manipulation zurückgeführt zu werden. Gemäss Tallinn Manual beschränkt sich die »*cause*« nicht auf Effekte am betroffenen Computersystem, sondern soll vielmehr auch vernünftigerweise absehbare Folgeschäden, Folgezerstörung, Verletzungen oder die Herbeiführung von Toten umfassen.[216] Damit fallen nicht nur direkte, sondern auch gewisse indirekte Schäden darunter. Obwohl Cyberangriffe selten direkte physische Schäden am betroffenen Computersystem auslösen, können Folgeschäden an Objekten und potenziell auch an Individuen entstehen. Ein Beispiel dafür ist der eingangs erwähnte Fall Stuxnet, der physische Schäden an der Atomanlage auslöste, ohne das Kontrollsystem selbst zu beschädigen. Ein anderes Beispiel wäre eine Manipulation eines Kontrollsystems eines Dammes, durch die (indirekt) tonnenweise Wasser freigeschaltet werden könnte, ohne das System selbst zu beschädigen.[217]

Intensiv thematisiert wurde weiter, ob die *Funktionsbeeinträchtigung* eines Objekts mittels Cybermitteln eine destruktive Konsequenz i.S. der Tallinn Manual Regel 92 darstellen könne.[218] Die Experten waren sich uneinig: Während einige dies verneinten, vertrat die Mehrheit die Ansicht, dass die Funktionsbeeinträchtigung dann als für einen Angriff relevanten Schaden zu qualifizieren sei, wenn für die Wiederherstellung der Funktion physische Komponenten ersetzt werden müssen. Die Mehrheit bejahte dies im Beispiel einer Cyberoperation, bei der durch die Manipulation eines Kontrollsystems ein Stromnetz ausgeschaltet wird, was dazu führt, dass entweder das Kontrollsystem oder zentrale Komponenten desselben ersetzt werden müssen, um eine funktionierende Stromversorgung wiederherzustellen.[219] Ebenso könne die Einbusse der Nutzbarkeit einer Cyberinfrastruktur gem. einigen Experten, unabhängig von physischen Schäden, einen für einen Cyberangriff relevanten Schaden darstellen.[220] Des Weiteren diskutierte die Expertengruppe, ob eine Cyberoperation ebenfalls darunter falle, wenn sie keine physischen Schäden im obengenannten Sinne, jedoch anderweitige schwerwiegende Konsequenzen nach sich zieht, wie z.B. den Unterbruch einer gesamten E-Mail-Kommunikation eines Landes, ohne das zugrundeliegende Kommunikationssystem zu be-

216 Tallinn Manual 2.0, S. 416, R92 C5.

217 Tallinn Manual 2.0, S. 416, R92 C5.

218 Tallinn Manual 2.0, S. 417, R92 C10.

219 Tallinn Manual 2.0, S. 417, R92 C10.

220 Tallinn Manual 2.0, S. 418, R92 C12. Eine ähnliche Auffassung vertritt das internationale Rote Kreuz im Kontext des humanitären Völkerrechts: ICRC Report 2015, S. 41.

schädigen.[221] Eine Mindermeinung vertrat die Ansicht, dass die internationale Gemeinschaft solche Cyberoperationen grundsätzlich dann als Angriff kategorisieren würde, wenn diese innerhalb eines bewaffneten Konfliktes (Krieg) stattfinden würden.[222] Cyberoperationen, die lediglich zu Irritationen und Unannehmlichkeiten der Zivilbevölkerung führen, seien grundsätzlich nicht als Cyberangriff zu verstehen.[223] Der Begriff der Unannehmlichkeiten wird nicht konkretisiert.[224]

Zusammengefasst kann gesagt werden, dass das Manual gemeinsam mit einem Teil der Lehre von einem effektbasierten Ansatz ausgeht, indem es für Angriffe jeweils (hauptsächlich physisch messbare) Effekte voraussetzt.[225] Obschon gem. Tallinn Manual nicht nur kinetische Effekte unter den Schadensbegriff zu subsumieren sind, bleibt relativ unklar, welche nicht-physischen Schäden von der Definition erfasst sind.[226] Ob ein dahingehend effektbasierter Ansatz im Hinblick auf das vorliegend relevante Konzept von Cyberangriffen sinnvoll ist, bleibt fraglich. Ein Problem liegt mitunter darin, dass Cyberangriffe und Cyberoperationen fast alle Arten von mittelbaren Schäden – also nicht nur physische –, sondern auch immaterielle, ökonomische und politische Schäden auslösen können, die ebenfalls für eine völkerrechtliche Würdigung relevant sein können. Der primäre Fokus des Tallinn Manuals auf herkömmliche physische, chemische, biologische oder radioaktive Schäden ist insgesamt für die nachfolgende Analyse demzufolge wohl zu eng gefasst. Für die vorliegende, völkerrechtliche Würdigung von Cyberangriffen ist es daher wichtig, dass das Konzept eines Cyberangriffs verschiedene Arten sicherheitspolitisch relevanter Schädigungen umfasst. Insgesamt verdeutlicht der Versuch im Tallinn Manual, Cyberschäden und Cyberangriffe zu definieren, dass dies mit komplexen Herausforderungen verbunden ist.

221 Tallinn Manual 2.0, S. 418, R92 C13.

222 Tallinn Manual 2.0, S. 418, R92 C13.

223 Tallinn Manual 2.0, S. 418, R92 C14.

224 Siehe: Tallinn Manual 2.0, S. 418, R92 C14.

225 Siehe u.a. LUCAS, S. 27; OWENS et al., S. 21.

226 Vgl. Tallinn Manual 2.0, S. 342 R71 C12, wo klar wird, dass sich die Experten darin uneinig waren: »*The case of cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled*«.

2. Der effekt- vs. instrumentbasierte Ansatz

Vorliegend sollen je ein Definitionsansatz der USA und der Staaten der Shanghaier Organisation für Zusammenarbeit (SCO)[227] aufgegriffen werden, um divergierende Verständnisse desselben zugrundeliegenden Phänomens zu illustrieren. Die US-Militärdoktrin ist generell eine der prominentesten Doktrinen im Zusammenhang mit Cybertechnologien.[228] Die Auffassung der SCO hingegen bietet mit ihrer Umschreibung von »*information war*« einen illustrativen Gegenpol dazu. Dies bedeutet nicht, dass das Völkerrecht lediglich durch diese erwähnten Länderansichten geprägt ist – insb. nicht, da es fraglich ist, inwiefern Militärdokumente rechtlich vertretbare Definitionen enthalten.[229] Es muss ferner darauf verwiesen werden, dass es sich um erste Ansätze handelt und jüngere Definitionen und Begriffsumschreibungen aus verschiedenen Staaten sowie der Lehre folgten.[230] Die letzteren Ansätze sind für den vorliegend relevanten, eigenen Definitionsansatz jedoch nicht weiter von Einfluss.

Die Vereinigten Stabschefs der USA (im Englischen: U.S. Joint Chiefs of Staff) haben 2010 ein militärisches Lexikon zu Cyberoperationen herausgegeben, in dem eine erste offizielle (militärische) Definition eines Cyberangriffs zu finden ist.[231] Die Definition lautete dabei wie folgt: »A *hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves – for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability.* A *cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack*

227 Die SCO ist eine 2001 gegründete, internationale Organisation mit Sitz in Peking. Sie fokussiert sich auf die sicherheitspolitische Zusammenarbeit ihrer Mitgliedstaaten, auf Wirtschafts- und Handelsfragen sowie auf regionale Stabilität. Es gehören ihr China, Russland, Indien, Kasachstan, Kirgisistan, Pakistan, Tadschikistan und Usbekistan an. Siehe: UN, Political and Peacebuilding Affairs, SCO, abrufbar unter: <https://dppa.un.org/en/shanghai-cooperation-organization> (zuletzt besucht: März 2023).

228 Vgl. Woltag, S. 21.

229 Vgl. Woltag, S. 21.

230 In den USA u.a. U.S. DoD, Dictionary of Military and Associated Terms 2016; U.S. DoD, Dictionary of Military and Associated Terms 2021. Zu weiteren Begriffsansätzen in der US-Militärdoktrin: Woltag, S. 21 ff. Zu Begriffsumschreibungen in bilateralen Abkommen zwischen den USA und China 2015 z.B. Baezner, S. 1 ff.

231 U.S. Joint Chiefs of Staff, Terminology for Cyberspace 2010; Hathaway et al., S. 824.

may be widely separated temporally and geographically from the delivery«.[232] Diese Definition setzt, ähnlich der Definition im Tallinn Manual, an den Effekten bzw. an einer beabsichtigten Schädigung von oder durch Computersysteme an.[233]

Die SCO-Staaten verfolgten in ihrem SCO-Übereinkommen im Dezember 2008 hingegen einen instrumentbezogenen Ansatz.[234] Es ging primär um die Angst vor den potenziellen Gefahren neuer Informations- und Kommunikationstechnologien und Mitteln, die mit dem »Zweck internationaler ziviler und militärischer Sicherheit und Stabilität unvereinbar sein könnten«.[235] Informationskrieg (vorliegend als Äquivalent zu einem Cyberangriff verstanden) impliziert jenem Verständnis zufolge eine »*confrontation between two or more states in the information space aimed at damaging information systems [...] and other structures, undermining political, economic and social systems, mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party*«.[236] Die SCO-Staaten verstehen die Verbreitung von für »soziale, politische und wirtschaftliche Systeme sowie geistige, moralische und kulturelle Bereiche anderer Staaten« schädigenden Informationen als eine der Hauptbedrohungen für die internationale Sicherheit.[237] Der Ansatz der SCO impliziert somit eine andere Auffassung von »Schaden« bzw. geht nicht wie das Tallinn Manual von einem primär physisch wirkenden »Angriff« aus. Wie vorangehend erwähnt, umfasst die Definition eines Angriffs im Tallinn Manual gewaltlose militärische Operationen wie psychologische Cyberoperationen eben nicht.[238] Der Ansatz der SCO-Staaten impliziert daher eine Auffassung von Cyberangriffen als Instrumente, die die politische und gesellschaftliche Stabilität eines Staates auch ohne phy-

232 U.S. Joint Chiefs of Staff, Terminology for Cyberspace 2010, S. 5. Die später publizierten Begriffsverwendungen der Vereinigten Stabschefs und des Verteidigungsdepartements (DoD) der USA lehnen sich mit ihrem grundsätzlichen Fokus auf physische Zerstörungen an die ursprüngliche Definition von 2010 an. Zu einer Übersicht der Dokumente siehe: U.S. Joint Chiefs of Staff, DoD Terminology Program.

233 Gem. Hathaway et al. handelt es sich um einen ziel-basierten Ansatz: Hathaway et al., S. 824.

234 Hathaway et al., S. 824.

235 SCO-Übereinkommen, S. 202.

236 SCO-Übereinkommen, S. 209.

237 SCO-Übereinkommen, S. 203. Auch ersichtlich in: UN Doc. A/56/164/Add.1, (2001), S. 2 ff.

238 Tallinn Manual 2.0, S. 415, R92 C2.

sischen Schaden beeinträchtigen oder gefährden können.[239] Die SCO-Staaten verbinden mit Cyberangriffen somit eher das Konzept einer Einmischung in die inneren Angelegenheiten eines Staates und setzen am Bedürfnis nach Souveränität an.[240] Sie gehen davon aus, dass durch das Internet oder anderweitige Cybertechnologien (bzw. »*information*«) politische Meinungen beeinflusst oder gesteuert werden können (z.B. durch die Beeinflussung von Wahlen).[241] Eine dahingehende Umschreibung der Folgen eines Cyberangriffs oder »*information war*« kann insb. vor dem Hintergrund des völkerrechtlichen Interventionsverbots relevant werden (zum Interventionsverbot siehe nachfolgend unter III.B.2.a).[242]

Die abweichenden Verständnisse dürften einerseits auf kulturelle und ideologische Unterschiede zurückzuführen sein. Andererseits spielen oft auch strategische Differenzen bei Cyberangriffen eine nicht zu vernachlässigende Rolle. Staaten haben nämlich divergierende Ansichten zu rechtlich notwendigen Grenzen sowie unterschiedliche Risiko- und Chanceneinschätzungen.[243] Jeder Staat (oder Akteur) fühlt sich unterschiedlich schnell und in unterschiedlichen Bereichen bedroht und verletzt, was im Ergebnis zu verschiedenen Auslegungen der zugrundeliegenden Rechtsnormen führt.[244] Diese Unterschiede in der Auffassung von Gefahren durch Cybertechnologien oder bezüglich der Kerndefinitionen werden die Bemühungen, klare Konsense für die Anwendung von Völkerrecht zu erreichen, wohl weiterhin prägen. Dennoch sind die verschiedenen Bedürfnisse der Staaten ernst zu nehmen, um ein nachhaltig friedliches und stabiles internationales Umfeld zu fördern. Cyber- oder »Informati-

239 Hathaway et al., S. 825. Siehe dazu auch Tikk-Ringas, S. 4 u.a. m.V.a. Russland in UN Doc. A/54/213 (1999).

240 Vgl. Komov/Korotkov/Dylevski, S. 38. Zu verschiedenen Ansichten zu Souveränität und Cyberraum siehe: Radziwill, S. 101 ff., S. 102. Ferner u.a.: Gady/Austin, S. 5 f.; Giles/Hagestad, S. 413 ff.

241 Diese Ansicht ist bspw. reflektiert in: UN Doc. A/56/164/Add.1, (2001), S. 2 ff.

242 In jüngerer Vergangenheit verstehen allerdings auch die USA Cyberangriffe auf politische Wahlen ohne physische Schäden als sicherheitspolitisch relevante Angriffe. Siehe: The White House, Statements and Releases vom 15.04.2021.

243 Waxman, Cyber-Attacks, S. 458 f.

244 Vgl. dazu: Kennedy, (insb.) S. 18, S. 38 f.

onstechnologien« stellen durchaus unterschiedlich interpretierbare Gefahren und Herausforderungen dar, deren Umschreibung wohl immer zu einem gewissen Grad von eigenen Auffassungen geprägt sein wird.[245]

3. Technische Kategorien von Cyberangriffen

Neben einer für eine rechtliche Würdigung sinnvollen Definition von Cyberangriffen stellt auch die technische Erfassung und Kategorisierung des Konzepts Schwierigkeiten dar. Dabei divergieren nicht nur Ansätze innerhalb der rechtlichen Disziplin, sondern gerade auch die rechtlichen und die technischen Verständnisse.[246] Die technischen Charakteristika eines Cyberangriffs sind für die meisten juristischen Ansätze nicht vordergründig, indem – wie aufgezeigt – oft an einem effekt-[247] oder instrumentbasierten Verständnis angesetzt wird. Man versucht Cyberschäden wie herkömmliche Schäden oder sicherheitspolitisch relevante Beeinflussungen zu behandeln, wodurch man sich bei der Definierung des Untersuchungsgegenstandes implizit vermutlich an bestehenden rechtlichen Konzepten orientiert.

In technischen Disziplinen werden Cyberangriffe i.d.R. anhand der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen (»*confidentiality*«, »*integrity*«, »*availability*«) definiert.[248] Die Vertraulichkeit eines Computersystems ist bspw. verletzt, wenn unbefugt Zugang zu Informationen oder zu einem System erlangt wird. Wenn Daten verändert werden, ist die Integrität des Systems nicht mehr gewährt. Die Verfügbarkeit ist beeinträchtigt, wenn

---

245 Ähnlich wurde in der ersten öffentlichen Sicherheitsratskonferenz zur Cybersicherheit vom 24.06.2021 ersichtlich, dass Staaten jeweils divergierende Prioritäten, Herangehensweisen und Auffassungen zu Cyberbedrohungen haben. Während in einigen Ländern Cyberkriminalität und Falschinformationen besorgniserregnende Themen auf der Agenda sind, scheinen andere eher einen Fokus auf Themen wie bspw. den technischen Kapazitätenaufbau zu haben. Die virtuelle Konferenz »UN Security Council Open Debate on Cybersecurity, Maintaining International Peace and Security in Cyberspace, 29 June 2021«, ist abrufbar unter: <http://webtv.un.org/> (zuletzt besucht: März 2023).

246 Woltag, S. 25.

247 Woltag, S. 25.

248 Ausführlicher dazu: Herrmann/Pridöhl, S. 13 m.w.V. Sich an die sog. CIA-Definition anlehnend u.a.: Burkart/McCourt, S. 1; Singer/Friedman, S. 70 f. Wie bereits vorangehend unter II.B.1.a) erwähnt. Eine neue technische Definition (»Appropriate Access«) vorschlagend, um die Brücken zwischen verschiedenen Perspektiven auf die Informationssicherheit zu schlagen: Lundgren/Möller, S. 419 ff.

Daten blockiert oder gelöscht werden.[249] Zudem sind für eine technische Betrachtungsweise die jeweiligen Akteure oder die Absicht hinter einem Angriff irrelevant. In der Informatik werden technische und menschliche Fehler, blosses »Ausprobieren« von Hackern sowie automatisierte Angriffe von der Definition umfasst, da diese die Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und Daten ebenfalls beeinträchtigen können. Das heisst, dass auch Defekte an der IT-Infrastruktur, Fehler in der Systemsoftware oder unbeabsichtigte Zufallstreffer zu gefährlichen und gegebenenfalls längerfristigen IT-Ausfällen führen können.[250] Informatikern zufolge kann also bereits das unbefugte Eindringen eines (automatisierten) Schadprogramms in ein System oder das Beeinträchtigen von Systemen durch Zufallstreffer von Hackern einen Cyberangriff bedeuten, ohne dass dieser einen politischen Einfluss oder physische Folgen haben muss.[251] Informatiker gehen des Weiteren vielmehr bei jedem Cyberangriff von einem technischen Einzelfall aus. Ihnen zufolge nutzt jeder Cyberangriff eine jeweils andere technische Sicherheitslücke aus und wird in dieser exakten Form womöglich nicht mehr vorkommen.[252] Potenziell können somit durch technische Ausfälle, Schädigungen und Manipulationen alle Rechtsgebiete von Datenschutz, Cyberkriminalität bis hin zu politisch relevanten Sachverhalten tangiert sein.[253] Sowohl Cyberangriffsinstrumente als auch die Techniken (wie Hacking) entwickeln sich dabei ständig weiter. Das Voraussehen von Trends ist deshalb beinahe unmöglich.[254]

---

249 Herrmann/Pridöhl, S. 13. Bei DDoS-Angriffen z.B. wird i.d.R. der Zugang zu Daten blockiert, womit die »Verfügbarkeit« beeinträchtigt wäre. Siehe zu DDoS-Angriffen sogleich unter dem nachfolgenden Abschnitt.

250 Vgl. dazu: Ziga, S. 132.

251 Vgl. Tikk/Kaska/Vihul, S. 98.

252 Dewar, Contextualizing, S. 3.

253 Es macht Sinn, dass sich jede Disziplin auf ihre Stärke konzentriert. Ein bestimmter Grad eines technischen, fächerübergreifenden Verständnisses ist für die Würdigung eines Sachverhaltes dennoch unerlässlich.

254 Dewar, Contextualizing, S. 14.

Für das Verständnis der rechtlichen Analyse dieser Dissertation soll der Untersuchungsgegenstand in die nachfolgenden technischen Kategorien unterteilt werden.[255] Das Konzept von Cyberangriffen soll einerseits in Distributed Denial-of-Service (DDoS)-Angriffe und andererseits in Angriffe durch Computerwürmer, -viren oder trojanische Pferde gegliedert werden.[256] Neben diesen beiden Kategorien gibt es allerdings potenziell weitere Unterkategorien von Angriffen oder Kombinationen verschiedener technischer Instrumente, durch die Sicherheitslücken bestehender Softwares ausgenutzt werden können.[257] Ein Grossteil der für das vorliegende Verständnis relevanten Angriffe kann jedoch unter eine dieser Kategorien oder eine Kombination derselben subsumiert werden.[258] Unter »Hacking« wird der vorliegenden Ansicht nach keine eigene Kategorie, sondern vielmehr eine Technik verstanden, um Angriffe lancieren zu können.[259] Mittels Hacking wird, wie bereits vorangehend unter II.B.1.a) erwähnt, via Sicherheitslücken auf ein Computersystem zugegriffen.

a. Distributed Denial-of-Service-Angriffe

Denial-of-Service-(DoS)-Angriffe sind eine übliche Form von Cyberangriffen.[260] Das Ziel von DoS-Angriffen ist es, einen Zielcomputer mit elektronischen Kommunikationsanfragen zu überhäufen und diesen somit entweder zu verlangsamen oder für den legitimen Nutzer zu blockieren.[261] Mit anderen Worten kann der legitime Nutzer bei einem solchen Angriff nicht mehr auf sei-

255 Es gibt verschiedene Ansätze von (rechtlichen) Kategorisierungen: Sklerov, S. 13 ff. geht von drei Kategorien aus, andere Autoren von zwei oder sogar vier. Siehe u.a. Lehtinen/Russell/Gangemi, S. 79 ff., S. 112 ff. (Cyberangriffe in Viren und Internetverletzlichkeiten kategorisierend); Colarik, S. 84 (Cyberangriffe in Viren und Würmer, DDoS-Angriffe, Web-Manipulationen und unbefugtes Eindringen kategorisierend). Zu weiteren Kategorien: Antolin-Jenkins, S. 139 f.; Ghorbani/Lu/Tavallaee, S. 3; Hathaway et al., S. 821; Heather Dinniss, S. 5; Schulze, S. 24 ff.

256 Woltag, S. 26 ff. Zu ähnlichen Kategorisierungen unter Erwähnung weiterer Techniken: Kerschischnig, S. 31 ff.

257 Zu Beispielen: Pierrot, Hacker, S. 16 ff.; Ghorbani/Lu/Tavallaee, S. 1 ff., insb. S. 4; Woltag, S. 28.

258 Sklerov, S. 15 f.; Woltag, S. 26. Erfahrene Angreifer setzen bspw. trojanische Pferde gemeinsam mit DoS-Angriffen ein: Lehtinen/Russell/Gangemi, S. 79 ff.

259 Burkart/McCourt, S. 1; Dewar, Active Cyber Defense, S. 8.

260 Zum Aufkommen und der Zunahme von DDoS-Angriffen: Nazario, S. 7 ff.

261 Ghorbani/Lu/Tavallaee, S. 11; Lehtinen/Russell/Gangemi, S. 81; Pierrot, Computerviren, S. 43; Tallinn Manual 2.0, Glossar, S. 565; Woltag, S. 26.

nen Computer und die darin enthaltenen Funktionen und Daten zugreifen.[262] DDoS-Angriffe sind dabei im Grunde eine *Vielzahl* von verteilten (»*distributed*«) DoS-Angriffen, die simultan von mehreren kompromittierten Geräten ausgehen.[263] Das heisst, es können gleichzeitig eine Vielzahl von Computern blockiert und damit funktionsunfähig gemacht werden. Beispiele hierfür wären, wenn plötzlich sämtliche Bankomaten einer bestimmten Bank ausser Betrieb sind oder wenn in einem Aussenministerium plötzlich die Computer aller Mitarbeiter streiken. Die breite Verteilung verstärkt die Wirkung von DDoS-Angriffen folglich exponentiell.[264] Die Gruppe der kompromittierten Geräte, von denen die DoS-Signale ausgehen, wird als sog. Botnetz umschrieben.[265] Meist ist ein solches Botnetz breit zerstreut bzw. können sich die kompromittierten Geräte gleichzeitig weltweit befinden. Die jeweiligen »Bots« können dabei vom Kontrollsystem aus (z.B. mittels trojanischen Pferden) ferngesteuert und aktiviert werden.[266] Es gibt keine praktische Begrenzung für die Anzahl der Bots, die in ein Botnetz aufgenommen werden können,[267] und es können alle Arten von Computern, mitunter auch internet of things-Geräte oder Router, kompromittiert werden. Abhängig davon, was die durch DDoS-Angriffe blockierten Computersysteme oder spezifischen Geräte im Einzelnen kontrollieren, können demnach Folgeschäden verschiedener Art ausgelöst werden. Denkbar sind Einbussen durch Arbeits- oder Transaktionsausfälle, der Unterbruch dringlicher Kommunikation bis hin zu Funktionsbeeinträchtigungen kritischer Infrastrukturen.

Da regelmässig simultan mehrere ferngesteuerte Geräte missbraucht werden, ist es insgesamt extrem schwierig, sich gegen DDoS-Angriffe zu verteidigen.[268] Zudem ist bei DDoS-Angriffen die technische Zurückverfolgung des Urhebers zusätzlich erschwert, da die kompromittierten Geräte (bzw. deren IP-Adressen) unabhängig vom Standort missbraucht oder kontrolliert und die Angriffe so weiter gestreut werden können.[269] Dazu kommt die relativ einfache Verfügbarkeit vorprogrammierter Schadprogramme, mittels derer DDoS-Angriffe

262 Damit wäre grundsätzlich die Verfügbarkeit (»*Availability*«) von Daten beeinträchtigt.

263 Siehe: Dewar, Contextualizing, S. 6; Gaycken, S. 110; NCSC, Glossar.

264 Dazu auch: Colarik, S. 103; Sklerov, S. 16 f.

265 Tallinn Manual 2.0, Glossar, S. 563; NCSC, Glossar.

266 Burkart/McCourt, S. 3.

267 Tallinn Manual 2.0, Glossar, S. 563.

268 Bosshardt/Dübendorfer/Plattner, S. 843; Nazario, S. 7. Aus ähnlichen Gründen daher auf präventive Massnahmen verweisend: NCSC, Measures to Counter DDoS Attacks.

269 Lipson, S. 15; Pierrot, Computerviren, S. 44; Woltag, S. 26.

iniziiert werden können.[270] Dies macht diese Angriffskategorie für eine breite Öffentlichkeit zugänglich, was wiederum zu einer enormen Unübersichtlichkeit führt. Neben der Möglichkeit, gleichzeitig mehrere Computer zu blockieren, können DDoS-Angriffe letztlich auch deren Schutzsysteme ausschalten, z.B. durch das Herunterfahren von deren Firewall.[271] Dadurch wird ein Computersystem gleichzeitig für andere Angriffsarten anfällig.[272] Das heisst, durch DDoS-Angriffe können nicht nur viele Computer gleichzeitig kompromittiert und/oder blockiert, sondern auch der Einsatz anderer Schadprogramme erleichtert werden.[273]

b. Trojanische Pferde, Computerviren und -würmer

Während DDoS-Angriffe primär eine Funktionsverlangsamung oder Blockierung von Computer- oder Computernetzwerken auslösen, können trojanische Pferde, Computerviren und -würmer auch auf die Kontrolle des Zielcomputers oder -computersystems abzielen.[274] Alle drei Typen werden i.d.R. durch Schadprogramme ausgeführt, die für spezifische Sicherheitslücken vorprogrammiert werden.[275]

Trojanische Pferde[276] werden grundsätzlich unbemerkt in ein fremdes System eingeschleust, während das System vermeintlich normal weiterzufunktionieren scheint.[277] Mittels trojanischer Pferde können im infiltrierten Computersystem ohne das Wissen des Nutzers daher aktive Funktionen ausgeführt und gestört werden. So kann das infizierte System unbemerkt aus der Ferne kontrolliert und manipuliert werden, und es kann auf Daten zugegriffen werden.[278] Mit dem Zugriff auf ein System kann ein Angreifer somit eine Vielzahl an schädigenden Handlungen ausführen, die letztlich nicht nur Auswirkungen in der digitalen, sondern – je nachdem, was das betroffene System kontrolliert – auch in der physischen Welt haben können.[279]

---

270 Woltag, S. 45.

271 Colarik, S. 103.

272 Colarik, S. 103; Lehtinen/Russell/Gangemi, S. 131 f.; Sklerov, S. 17.

273 Lehtinen/Russell/Gangemi, S. 79 ff.

274 Woltag, S. 27.

275 Woltag, S. 28.

276 Zum Ablauf eines Angriffes durch trojanische Pferde siehe Stiennon, S. 7 f.

277 Joyner/Lotriontе, S. 836; Woltag, S. 27.

278 Pierrot, Hacker, S. 21 f.

279 Colarik, S. 84; Sklerov, S. 17 ff., S. 20.

Computerviren und -würmer werden ähnlich den trojanischen Pferden unbemerkt in Computersysteme infiltriert, um dort vorprogrammierte Funktionen auszuführen. Dabei sind Computerviren auf das infizierte System (»*host systems*«) ausgerichtet. Computerwürmer können sich hingegen replizieren und sich selbständig durch interne Netzwerke oder das Internet[280] auf weitere Systeme verbreiten.[281] Gewisse Schadprogramme sind im Vornherein bereits so programmiert, dass sie sich automatisch reproduzieren, um den Angriff zu streuen.[282] Im Gegensatz zu trojanischen Pferden erlangt man durch Computerviren und -würmer keine Kontrolle (»*remote control*«) über das Zielsystem. Zudem kann ihre Weiterverbreitung in bestimmte Systeme nicht mehr kontrolliert werden, wenn sie einmal in Umlauf gebracht wurden.[283] Grundsätzlich ist es dabei sehr schwierig, vollumfänglich vorauszusehen, welche Computer zusätzlich infiziert werden.[284] Unter die Kategorie der Computerwürmer fällt das eingangs erwähnte Beispiel Stuxnet, also die Schadsoftware, mit der das iranische Atomprogramm beschädigt wurde. Stuxnet wurde spezifisch programmiert, um auf das konkrete SCADA-Kontrollsystem des iranischen Atomprogrammes in Natanz abzuzielen.[285] Dies erfordert grundsätzlich eine aufwändige Koordination und Planung.[286] Im Falle von Computerwürmern besteht dabei, wie erwähnt, allerdings jeweils die Gefahr, dass (mittels Internet oder interner Netzwerkverbindungen[287]) eine Vielzahl weiterer Computer, -netzwerke oder -systeme infiziert werden, die zufällig dieselbe Software haben.[288] Dies können weltweit unzählige Computer und Computersysteme gleichzeitig sein, deren Anzahl im Vornherein schwierig abzuschätzen ist. So hat sich auch Stuxnet in der Folge automatisch weiterverbreitet und weltweit eine hohe Anzahl weiterer SCADA-Kontrollsysteme infiziert, deren Mehrheit eben-

280 Lehtinen/Russell/Gangemi, S. 85; Sklerov, S. 15.

281 Pierrot, Computerviren, S. 29 ff.; Lehtinen/Russell/Gangemi, S. 82. Siehe zu den Begriffen auch: Joyner/Lotrionte, S. 837 (Fn. 43 f.) mit Beispielen und w.V.

282 Singer/Friedman, S. 43.

283 Woltag, S. 28. Ausführlicher zur Unkontrollierbarkeit von Cyberaktivitäten siehe Cook, S. 23.

284 Singer/Friedman, S. 69.

285 Greenberg, Sandworm, S. 97.

286 Sanger, S. 188 ff.; Schulze, S. 16; Springer, Cyber Warfare, S. 31. Ausführlicher zum Hintergrund von Stuxnet: Zetter, S. 1 ff.

287 Neben dem Internet gibt es geschlossene »interne« Netzwerke, wie dasjenige im genannten Beispiel des iranischen Atomprogrammes in Natanz.

288 Pierrot, Computerviren, S. 36.

falls mit Atomanreicherungszentrifugen im Zusammenhang standen.[289] Dies, sowie weitere technische Einzelheiten zu Stuxnet's Funktionsweise, wurden allerdings erst Jahre später entdeckt.[290]

c. Aktive Cyberverteidigung: Hackbacks, Counter-DDoS-Angriffe und weisse Computerwürmer

Über Angriffskategorien hinaus drängt sich im Rahmen der vorliegenden Analyse auch die Subsumierung aktiver Cyberverteidigung unter die vorangehenden technischen Kategorien auf. Denn es sollen nachfolgend nicht nur Angriffskategorien (*actio*) rechtlich gewürdigt werden, sondern unter Teil IV auch die entsprechenden (digitalen) Gegenmassnahmen (*reactio*). Wie bereits unter II.B.2 erwähnt, können Cyber(gegen-)angriffe zu verschiedenen Effekten und (physischen) Schädigungen an Computersystemen Dritter im In- und Ausland führen, da sie grundsätzlich ausserhalb der angegriffenen Infrastrukturen agieren.[291] Es ist durchaus möglich, die Funktionsweise eines Computersystems (sowie u.U. weiterer Systeme) durch aktive digitale Verteidigung zu beeinträchtigen[292] – und zwar unabhängig davon, ob es das System des »echten Angreifers« ist oder nicht. Bei internationalen Sachverhalten kann der Einsatz von Cybergegenangriffen daher völkerrechtlich relevant werden.[293] Das Konzept aktiver digitaler Verteidigung umfasst verschiedene digitale Instrumente und Techniken und muss, wie bereits erwähnt, im vorliegenden Sinne als Überbegriff für Cyberaktivitäten zur Verteidigung von Computernetzwerken und -systemen ausserhalb der angegriffenen Computerinfrastrukturen verstanden werden. Aktive Cyberverteidigung ermöglicht es grundsätzlich einer von einem Cyberangriff betroffenen Partei, einen Angriff zu erkennen, ihn technisch zurückzuverfolgen und dann aktiv darauf zu reagieren, indem der

289 Dewar, Contextualizing, S. 10. Gemäss Baezner/Robin, Stuxnet, S. 6 befanden sich 60% der infizierten Computer im Iran.

290 Langner, S. 4. Langner's Analyse stellt eine der umfassendsten technischen Analysen zu Stuxnet's Funktionsweise und der zugrundeliegenden Hintergrundinformationen dar. Diese wurde im November 2013 publiziert. Zu jenem Zeitpunkt hat Langner bereits darauf verwiesen, dass Stuxnet IT- und weitere Experten weiterhin auf Trab halten wird.

291 Kesan/Hayes, S. 474 f. Ein Angriffssystem kann physisch mittels aktiver Cyberverteidigungsinstrumenten beschädigt werden, indem bspw. die Kühlfunktion eines Ursprungscomputers manipuliert wird und die daraus resultierende Überhitzung zu Schäden führt: Lahmann, S. 127 m.V.a. Tallinn Manual 2.0, S. 20, R4 C11.

292 Vgl. Katyal, S. 64. Implizit auch Lahmann, S. 127.

293 Jensen, Critical National Infrastructure, S. 230; Sklerov, S. 73.

Angriff bspw. unterbrochen und dadurch die Schädigung minimiert wird.[294] KESAN/HAYES sehen aktive digitale Verteidigung somit als in der Erkennungsphase beginnend und unterteilen die Instrumente in drei verschiedene Phasen: In (Früh-)Erkennungssysteme (»*intrusion detection systems*«), Investigations- und Zurückverfolgungstechnologien (»*traceback*«) sowie Gegenangriffskapazitäten (»*counterstrike capabilities*«).[295] Letztere umfassen Methoden, die das Zurücksenden von Daten zum Angriffssystem implizieren.[296] Für diese Dissertation sind deshalb insb. die Gegenangriffskapazitäten bzw. deren Einsatz relevant, da diese ein Eindringen in fremde Systeme (potenziell im In- und Ausland) implizieren und dabei völkerrechtskonform sein müssen. Dem vorliegenden, völkerrechtlichen Verständnis nach bewegt man sich bei Erkennungssystemen sowie grundsätzlich auch bei Investigations- und Zurückverfolgungstechnologien – vorausgesetzt das fremde System wird »nur« ausspioniert – im passiven Bereich der Cyberverteidigung. Bei vielen Instrumenten ist die Kategorisierung als aktiv oder passiv allerdings nicht ganz klar.[297] Dieser Dissertation zufolge fällt jedoch vor allem der Einsatz sog. »Hackbacks«, Counter-DDoS-Angriffe und weisser Würmer unter völkerrechtlich relevante aktive digitale Gegenangriffskapazitäten. Diese Begriffe werden daher nachfolgend näher erläutert.

Ein Grossteil der Lehre und staatlicher Entscheidungsträger spricht im Zusammenhang mit aktiver digitaler Verteidigung von sog. Hackbacks.[298] Wie beim Hacking wird darunter grundsätzlich eine Technik verstanden, mittels derer auf ein fremdes Computersystem zugegriffen wird.[299] Daher werden via Hackbacks grundsätzlich ebenfalls (unbefugt) Änderungen der Vertraulichkeit, der Integrität und der Verfügbarkeit von Computersystemen und -netzwerken

294 KESAN/HAYES, S. 475; OWENS et al., S. 13; SKLEROV, S. 25.

295 KESAN/HAYES, S. 475.

296 KESAN/HAYES, S. 475, eingehender dazu: S. 483 ff.

297 DEWAR und OWENS et al. z.B. sehen sog. »Honeypots« als aktives Verteidigungsinstrument, während KESAN/HAYES, S. 472 (Fn. 284), S. 477 (Fn. 316) dieses als passives Instrument sehen. Indem Honeypots primär zu Investigationszwecken eingesetzt werden und auf dem fremden System kein Aktivwerden implizieren, werden sie vorliegend ebenfalls als passive Instrumente verstanden.

298 LAHMANN, S. 126. Der Begriff der Hackbacks wird auch i.Z.m. der umstrittenen und überwiegend in den USA diskutierten Frage um Gegenmassnahmen durch private Firmen verwendet. Siehe u.a.: CHESNEY, Lawfare vom 14.06.2019. Der Fokus der vorliegenden Dissertation bezieht sich allerdings auf staatliche Hackbacks.

299 DEWAR, Active Cyber Defense, S. 8. Zum Begriff des Hackings siehe vorangehend unter II.B.1.a).

herbeigeführt[300] – unabhängig davon, ob dies zu Angriffs- oder Verteidigungszwecken geschieht. Gemäss Tallinn Manual 2.0 stellen Hackbacks eine Unterkategorie aktiver Cyberverteidigung dar, die gegen eine identifizierte Angriffsquelle gerichtet ist, »um die Effekte zu lindern, den Angriff zu stoppen oder um technische Beweise für die Zurückverfolung der Urheberschaft zu sammeln«.[301] Mittels Hackback können dieser Lesart zufolge Angriffe also analysiert und (idealerweise) neutralisiert werden.[302] Indem man mittels Hackbacks i.d.R. unbefugt in andere Computersysteme oder -infrastrukturen eindringt, sind sie grundsätzlich jeweils (national- oder internationalrechtlich) illegal, wenn sie nicht rechtlich gerechtfertigt sind. Ein sich mit Hackbacks verteidigender Staat unterliegt somit denselben (international-)rechtlichen Schranken und Sanktionen wie ein Angreifer.[303] Verteidigungshandlungen sind nur legitim, wenn die rechtlichen Voraussetzungen dazu gegeben sind. Demnach können Hackbacks u.U. politische oder militärische Folgen haben, wenn man bspw. in »falsche« Systeme eindringt,[304] unbefugt Funktionen beeinträchtigt oder/und unverhältnismässige Effekte auslöst.

Eine weitere diskutierte Verteidigungsform gegen DDoS-Angriffe sind sog. »Counter-DDoS-Angriffe«.[305] Darunter versteht man im Grunde entweder einen Gegenangriff gegen viele kompromittierte Computersysteme oder gegen den zentralen Kontrollcomputer, von dem die Befehle ausgehen.[306] Im letzteren Szenario müsste allerdings der betreffende Kontrollcomputer während des Angriffs überhaupt bekannt sein, was in der Praxis aufgrund der unübersichtlichen Verhältnisse bei DDoS-Angriffen sehr schwierig ist.[307] Gegenangriffe von kompromittierten »Bots« aus sind hingegen im Vornherein nicht möglich, um DDoS-Angriffe zu stoppen, wenn das eigene System im Falle eines Angriffs bereits blockiert ist. Wenn man auf kompromittierte Computer zurückschlägt, läuft man zudem Gefahr, als Brückenkopf verwendete Geräte

300 Vgl. Burkart/McCourt, S. 1.

301 Lahmann, S. 126; Tallinn Manual 2.0., Glossar, S. 565.

302 Dewar, Active Cyber Defense, S. 8 m.w.V.

303 Dewar, Active Cyber Defense, S. 8.

304 Dewar, Active Cyber Defense, S. 8.

305 Kesan/Hayes, S. 475; Lahmann, S. 273 f. m.V. auf den Mechanismus des »CyberCop« Systems der US National Security Agency (NSA). Generell zu Präventions- und Reaktionstechniken bei DDoS-Angriffen: Ghorbani/Lu/Tavallaee, S. 13 ff.

306 Kesan/Hayes, S. 475; Owens et al. S. 64 insb. Fn. 26 (auf das Eskalationsrisiko bei DoS-Gegenangriffen gegen das Kontrollsystem hinweisend). Zu einem erfolgreichen Bsp., ein Botnetz unter Kontrolle zu bringen: Meisner, Microsoft News vom 17.03.2011.

307 Vgl. Bosshardt/Dübendorfer/Plattner, S. 845, S. 854.

(und damit »legitime« Nutzer) zu blockieren und dadurch letztlich die Effekte des ursprünglichen Angriffs zusätzlich zu verstärken.[308] Dies dürfte insb. der Fall sein, wenn weltweit ein breites Botnetz mit einer unübersichtlichen Anzahl an (willkürlich) kompromittierten Geräten vorliegt.[309]

Zur aktiven digitalen Verteidigung zählen ferner technische Instrumente wie sog. weisse Computerwürmer (»*white worms*«[310]).[311] Weisse Würmer können unter die im vorangehenden Abschnitt abgehandelte Kategorie der Computerwürmer gefasst werden. Sie werden als »weiss« bezeichnet, um sie von »bösartigen« Schadprogrammen (Malware) zu unterscheiden, die von Angreifern programmiert, bereitgestellt oder eingesetzt werden.[312] Es handelt sich im Grunde allerdings analog zu »bösartiger« Malware um eine Software, die darauf programmiert wird, nicht autorisierte Funktionen auszuführen. Dadurch wird grundsätzlich auch mittels weisser Würmer die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Informationssystemem zu einem bestimmten Zweck (wie dem der Verteidigung[313]) beeinträchtigt.[314] Eigentümer oder legitime Nutzer von Geräten werden grundsätzlich nämlich erst benachrichtigt, *nachdem* der Wurm bereits eingedrungen ist. Mit anderen Worten: »*It's like having a seasoned criminal break into your house and then, if he succeeds, install an alarm system.*«[315]

Weisse Würmer werden i.d.R. im eigenen System platziert, um Schadprogramme (in Echtzeit) zu identifizieren und können auf verschiedene Funktionen programmiert werden. Bestimmte Würmer wirken wie Antivirensoftware und zerstören die eindringende Malware – wenn diese frühzeitig entdeckt wird und allenfalls noch *bevor* Schädigungen eingetroffen sind. Alternativ können weisse Würmer darauf programmiert sein, eine Malware zu analysieren,

308 Bosshardt/Dübendorfer/Plattner, S. 854.

309 Im Falle des sog. Mirai Botnetzes waren rund 500'000 internet of things-Geräte weltweit kompromittiert: Kambourakis/Kolias/Stavrou, S. 267 ff.

310 Ausführlicher zu weissen Würmern: Castañeda/Emre/Xu, S. 83 ff.; Lu et al., S. 206 ff. Ferner u.a.: Cobb/Lee, S. 71 ff., insb. S. 74 ff.

311 Dewar, Active Cyber Defense, S. 7.

312 Dewar, Active Cyber Defense, S. 7.

313 Cobb/Lee, S. 74; Patterson, Networkworld vom 25.08.2017.

314 So die Umschreibung gem. Cobb/Lee, S. 74.

315 Katyal, S. 65 m.V.a. die Umschreibung von Roberts, ComputerWeekly vom 19.08.2003. Anders wäre die Situation zu beurteilen, wenn der Computerwurm darauf programmiert ist, den legitimen Nutzer lediglich auf die erforderliche Softwareaktualisierung oder die Installierung des Programms aufmerksam zu machen und zum Aktivwerden eine Autorisierung desselben erfordert.

um den Täter zu identifizieren und zu lokalisieren.[316] Wie »bösartige« Computerwürmer auch, sind weisse Würmer allerdings nach ihrer Freilassung ebenfalls sehr schwer zu kontrollieren, indem sie sich meist automatisch weiterverbreiten und einen ursprünglichen Computer oder ein Computernetzwerk mittels interner Verbindungen, USB-Speicherstiften oder dem Internet verlassen können. (Weisse) Computerwürmer replizieren sich, um ihre Funktionen auszuführen, gegebenenfalls auch in weiteren Computersystemen und -netzwerken. Teilweise ist ihre breitflächige Verbreitung sogar beabsichtigt, indem weisse Würmer auf das Schliessen (»*Patchen*«) von technischen Sicherheitslücken programmiert werden und gewissermassen als »Impfungen« von Computersystemen dienen sollen.[317] Allerdings erfolgt grundsätzlich auch die Weiterverbreitung auf weitere Systeme wiederum ohne die Befugnis des legitimen Nutzers oder des Eigentümers eines Geräts, da der Wurm durch die Sicherheitslücke überhaupt eindringen können muss, um diese zu schliessen.[318]

Insgesamt besteht ein enormes Potenzial für unbeabsichtigte Konsequenzen[319] sowie das Risiko eines Kontrollverlusts über einen Computerwurm.[320] Aufgrund der unkontrollierten Weiterverbreitung können weisse Würmer die Funktionen eines am ursprünglichen Angriff unbeteiligten Systems beeinträchtigen und dadurch – trotz ihrer ursprünglich verteidigenden oder schützenden Absicht – an Drittsystemen (unkontrolliert und unbeabsichtigt) schädigend wirken.[321] Angesichts der fehlenden Garantie, dass weisse Würmer bösartige Angriffe tatsächlich erkennen und neutralisieren können, sind diese Risiken nicht zu unterschätzen.[322] Und auch wenn eine Software nicht darauf programmiert wird, sich selbst zu replizieren, ist ihr Einsatz nicht unproblematisch: Einerseits wird durch eine sich nicht-replizierende Programmierung die »schützende« Funktion und Erfolgswahrscheinlichkeit weisser Würmer wesentlich eingeschränkt.[323] Andererseits gibt es keine Garantie dafür, dass die Software nicht versehentlich (z.B. durch das Kopieren eines infizierten Systems) oder absichtlich (von jemandem, der die Software entdeckt hat und diese oder ihre Funktionsweise wiederverwenden möchte) geklaut

316 Dewar, Active Cyber Defense, S. 7.

317 Patterson, Networkworld vom 25.08.2017.

318 Vgl. Castañeda/Emre/Xu, S. 84; Katyal, S. 65; Roberts, ComputerWeekly vom 19.08.2003.

319 Katyal, S. 62: »*[…] viruses, even ›beneficial‹ ones, may have unpredictable consequences for the stability of platforms and applications.*« Siehe auch: Kesan/Hayes, S. 477.

320 Cobb/Lee, S. 71.

321 Dewar, Active Cyber Defense, S. 7.

322 Dewar, Active Cyber Defense, S. 7 f.

323 Cobb/Lee, S. 77.

oder reproduziert wird.[324] Indem man Software einsetzt, gibt man nämlich gleichzeitig die Technik und das Design der Programmierung (sowie die Informationen zu bestehenden Sicherheitslücken) weiter.[325] Dies impliziert die reale Möglichkeit, dass Empfänger ein (Schad-)Programm bei ihrer Entdeckung rückgängig machen, umpogrammieren, klauen, zurück- oder weitersenden können.[326] Damit stellt sich ein nicht zu unterschätzendes Risiko einer »bösartigen« Umprogrammierung und Wiederverwendung von »freigelassenen« Computerprogrammen.[327] Hinzu kommt, dass das rasante Aufkommen einer industriellen Nachfrage nach Schadprogrammen (und Zero-Day-Lücken[328]) ein unumgängliches, generelles Missbrauchspotenzial von zu »guten« *und* zu »bösartigen« Zwecken programmierter Software mit sich bringt.[329] Gemäss Cobb/Lee kann man sagen, dass die Bemühungen von Staaten, »gerechte Software« (zu Verteidigungszwecken) zu entwickeln, kriminelle Unternehmen in der Produktion und Bereitstellung von Schadprogrammen unterstützen, wenn nicht gar fördern, indem sie einen Markt für die Ausnutzung von Sicherheitslücken schaffen.[330] Selbst wenn eine Software selbst nicht wiederverwendet wird, werden gem. Cobb/Lee Teile militärischer Programmierungen bspw. oft bei durch Kriminelle eingesetzten Schadprogrammen wiederentdeckt.[331] Die erwähnten Argumente sprechen allesamt dafür, dass aktive Cyberverteidigung nicht nur differenzierter, sondern auch vor dem Hintergrund ihrer Legalität näher betrachtet werden sollte.[332]

324 Cobb/Lee, S. 77; Langner, S. 19 f.

325 Cobb/Lee, S. 77 m.w.V.

326 Cobb/Lee, S. 77.

327 Cobb/Lee, S. 77. Im Zusammenhang mit Stuxnet: Baezner/Robin, Stuxnet, S. 11; Collins/McCombie, S. 89; Langner, S. 20.

328 Siehe zu Zero-Day-Lücken vorangehend unter II.B.1.a); Burkart/McCourt, S. 3.

329 Cobb/Lee, S. 77.

330 Cobb/Lee, S. 77; Simonite, MIT Technology Review vom 13.02.2013.

331 Cobb/Lee, S. 77; Simonite, MIT Technology Review vom 19.09.2012.

332 Kesan/Hayes, S. 475 sprechen sich dafür aus, dass die Regulierung aktiver Cyberverteidigung essenziell ist, um einen verantwortungsvollen Umgang damit zu sicherzustellen.

d. Zusammenfassung der für die Regulierung relevanten Charakteristika von Cyberangriffen und -Gegenangriffen

Aufgrund der potenziellen völkerrechtlichen Relevanz von sowohl Angriffen (*actio*) als auch von Reaktionen darauf (*reactio*), werden die für die Regulierung relevanten Eigenschaften gemeinsam abgehandelt. Die beiden vorangehend herausgearbeiteten technischen Kategorien (einerseits der DDoS-Angriffe und andererseits der trojanischen Pferde, Computerwürmer und -viren) gelten nämlich für Angriff *und* Verteidigung. Durch jede Form von Hacking, mitunter also bei Hackbacks oder anderweitiger digitaler Techniken, greift man – sowohl bei Angriff als auch Verteidigung – i.d.R. jeweils in einen fremden Computer und damit dessen Vertraulichkeit ein. Unter Umständen werden auch bestimmte Programme (wie z.B. trojanische Pferde[333]) an einen fremden Computer (zurück-)gesendet, mittels derer auch die Integrität oder Verfügbarkeit desselben verändert werden kann.

Für die Regulierung ist zunächst die Frage nach den durch die beiden Angriffskategorien ausgelösten Schädigungen wichtig. Beide Kategorien von Cyberangriffen (DDoS-Angriffe und trojanische Pferde, »weisse« als auch »bösartige« Computerwürmer und -viren) können zu verschiedenen Arten von Blockierungen oder Manipulationen von digitalen Informationen und Befehlen führen. Am einfachsten zu messen sind (unmittelbare und mittelbare) Schäden, wenn diese physisch in der realen Welt oder am System selbst entstehen. Indem Computersysteme zunehmend Funktionen für die physische Welt übernehmen, können – je nachdem, welche Funktionen manipuliert oder blockiert sind – Folgeschäden verschiedener Art entstehen.[334] Wie erläutert, sind Staaten, deren Infrastrukturen in einem hohen Masse an Computersysteme angeschlossen sind, besonders verletzlich. Angriffe, die auf Kontrollsysteme abzielen oder diese blockieren, können also mitunter Systeme treffen, die ganze Chemieanlagen, Kraftwerke, Reaktoren, Wassersysteme, Dämme oder Gasleitungen kontrollieren.[335] Die Beeinträchtigung von Computersystemen kritischer Infrastrukturen ist somit durch beide Kategorien von Angriffen denkbar. Ebenso denkbar sind neben physischen Schäden auch schwieriger zu messende, nicht-physische Schäden (z.B. ökonomischer oder politischer Art). Durch die Unterbrechungen von dringlichen militärischen Kommunikationswegen (wie im Falle der Angriffe auf Georgien 2008) bspw. können in der

333 Vgl. Burkart/McCourt, S. 3.

334 Heather Dinniss, S. 72.

335 Heather Dinniss, S. 5.

Kommunikation zwischen militärischen Stützpunkten Verspätungen generiert werden.[336] Dies kann in Konflikten zu entscheidenden strategischen Nachteilen führen, die materiell nicht direkt nachweisbar sind. Dies gilt ebenso für die unbemerkte Abänderung von Inhalten oder von Kontrollinformationen. Auch in solchen Konstellationen können physisch nicht messbare, immaterielle Schäden entstehen, wenn dadurch bspw. Meinungsbildungen beeinflusst werden oder Fehlinformationen vermittelt werden.

Des Weiteren für die Regulierung relevant sind die Zeitkomponenten von Angriff und Schädigung bzw. die Frage der Unmittelbarkeit eines Angriffs. Bei DDoS-Angriffen kann man im Gegensatz zur Kategorie der trojanischen Pferde, Computerwürmer und -viren einen Anfangs- und Endzeitpunkt des Angriffes festlegen. Man kann davon ausgehen, dass ein Angriff im Gange ist solange eine Blockierung mittels DDoS-Angriffen anhält. Bei trojanischen Pferden, Viren und Würmern ist die Zeitkomponente hingegen komplexer: Indem trojanische Pferde, Würmer und Viren sich i.d.R. bereits vor einer Schädigung und ohne das Wissen des Angegriffenen in einem Computersystem befinden, ist die Bestimmung, wann der Angriff begonnen hat[337] und wann er beendet ist, extrem schwierig. Bei diesen Angriffen wird oft erst *nach* Eintritt einer Schädigung bemerkt, dass man überhaupt angegriffen wurde.[338] Der Beginn eines Angriffs und die Schädigung fallen somit – je nachdem welchen Zeitpunkt man als Beginn festlegt – zeitlich auseinander.

Letztlich bleiben auch im Hinblick auf den für eine rechtliche Würdigung relevanten Kausalzusammenhang zwischen Angriff und Schädigung bei beiden Angriffskategorien Schwierigkeiten bestehen. Die Effekte eines Angriffs sind i.d.R. bei beiden Angriffskategorien selten unmittelbar, sondern vielmehr indirekte Folgen von Manipulationen und Blockierungen von Computersystemen. Es ist daher – wie auch im Tallinn Manual ersichtlich wurde[339] – schwierig zu eruieren, wie weit ein (Folge-)Schaden noch auf ein ursprüngliches Schadprogramm oder eine ursprüngliche Manipulation zurückgeführt werden kann.

336 Woltag, S. 26.

337 Stiennon geht davon aus, dass die erste Phase eines Angriffs grundsätzlich bereits mit dem Ausspionieren durch eine »*footprint analysis*« des Zielsystems beginnt siehe Stiennon, S. 7 f.

338 Bei der Ruag z.B. hat es mehr als ein Jahr gedauert, bis ein Cyberangriff überhaupt bemerkt wurde. Heute widmet man sich u.a. im Schweizer Cyber-Defense-Campus der Früherkennung von Angriffen. Obschon es gem. Lenders nicht möglich sei, Systeme komplett zu sichern, müsse man einen Angriff in Echtzeit feststellen und sofort und möglichst automatisch reagieren können: Betschon, Interview mit Lenders, NZZ vom 05.12.2019.

339 Tallinn Manual 2.0, S. 416, R92 C5.

Indem Schädigungen beider Angriffsarten nicht nur indirekt sind, sondern – im Falle von Computerwürmern – durch eine automatisierte Weiterverbreitung (weltweit) weitere Folgeschädigungen denkbar sind, wird ebendiese Frage zusätzlich erschwert. Mittels Internet können Angriffe innert Sekunden von überall auf der Welt lanciert werden sowie (simultan) Computersysteme überall auf der Welt treffen[340] und sich im Falle von Computerwürmern unkontrolliert weiterverbreiten. Damit wird neben der Definierung des erforderlichen Kausalzusammenhangs auch die Bestimmung des Endes eines Angriffs erheblich erschwert.[341] Diese Schwierigkeiten betreffen gleichermassen Angriffe (*actio*) und Gegenmassnahmen (*reactio*).

4. Eigener Definitionsansatz für die vorliegende Analyse

Eine für die vorliegende Dissertation sinnvolle Definition des Untersuchungsgegenstands basiert auf dem Vorschlag von Hathaway et al., die wie folgt lautet: »A *cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose*«.[342] Dabei soll vorliegend »*for a political or national security purpose*« durch »*with a political or national security impact*« ersetzt werden. Bei dieser Definition geht es folglich nicht primär darum, welche konkreten digitalen Mittel, welche Infiltrierungs- oder Weiterverbreitungskanäle verwendet[343] oder welche konkreten (physischen) Schäden ausgelöst werden. Der Angriff muss in erster Linie vielmehr eine Störung von Computerfunktionen umfassen, wodurch sicherheitspolitische Interessen tangiert oder beeinträchtigt werden.[344] Das Konzept eines Computers ist dabei so weitreichend, dass es Geräte oder Kontrollsysteme umfasst, die kritische Infrastrukturen oder andere Einrichtungen wie den Strassenverkehr, Lifte bis hin zu einzelnen internet of things-Geräten wie Waschmaschinen oder Drucker etc. kontrollieren.[345] Mit Computernetzwerken sind, wie vorangehend unter II.B.1.a) erwähnt, (insb.) durch das Internet

340 Vgl. zur Internationalität u.a.: Schulze, S. 45.

341 Ähnlich zu den Schwierigkeiten der rechtlichen Erfassung von Cyberangriffen aufgrund ihrer Indirektheit, der schwierigen Lokalisierbarkeit ihres Eintreffens und des Ergebnisses: Heather Dinniss, S. 65 ff. Siehe zu einer rechtlichen Würdigung des Beginns und des Endes eines Angriffs nachfolgend unter IV.A.2.b).

342 Hathaway et al., S. 826.

343 Hathaway et al., S. 826.

344 Hathaway et al., S. 826.

345 Clarke/Knake, Cyber War, S. 70 ff.

vernetzte Geräte gemeint.[346] »*Any action taken to undermine the function*« erfasst eine Breite an Möglichkeiten einer Beeinträchtigung durch eine beliebige Cyberhandlung;[347] d.h. die Definition umfasst die Kategorie von DDoS-Angriffen sowie Angriffe durch trojanische Pferde, Würmer und Viren (oder gegebenenfalls weitere Unterkategorien). Dies erlaubt einerseits eine Annäherung an das technische Verständnis einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Computern. Indem die Funktionsbeeinträchtigung in den Vordergrund gestellt wird, umfasst der Untersuchungsgegenstand andererseits eine Vielzahl möglicher (Folge-)Schäden.

Um die Funktion eines Computersystems gem. der vorliegend *völkerrechtlichen* Perspektive zu beeinträchtigen, muss zudem eine aktive Komponente gegeben sein.[348] Cyberzwischenfälle, die keine Funktionsbeeinträchtigung nach sich ziehen, würden dabei folglich nicht unter den hier relevanten Definitionsansatz fallen, obschon teilweise grosse Datenmengen kopiert werden, dies die Vertaulichkeit eines Computers beeinträchtigt und damit anderweitige (politische oder national-rechtliche[349]) Folgen haben kann.[350] Dies wäre bspw. bei einem rein passiven »Ausspionieren« eines Computers der Fall. Obschon in der Praxis Abgrenzungen meist fliessend und nur schwierig auszumachen sind, konstituiert Cyberspionage grundsätzlich keinen Cyberangriff im Sinne dieser Dissertation, da dabei die Funktion eines Ziel-Computers an sich grundsätzlich nicht beeinträchtigt wird.[351] Indem eine Funktionsbeeinträchtigung eines Computers erforderlich ist, reicht die Definition zudem nicht so weit, dass jegliche Meinungsäusserungen im Internet umfasst wären. Hingegen erlaubt die Definition die Erfassung von Cyberhandlungen, die Informationen, Programmierungen oder Webseiten manipulieren oder in unberechtigterweise offenlegen, um z.B. in fremde politische (Wahl-)Prozesse einzugreifen (die rechtliche Würdigung solcher Angriffe folgt dabei in einem separaten Schritt). Das Funktionieren bzw. die Integrität eines Computersystems kann nämlich auch

346 Roscini, Cyber Operations, S. 1; Hathaway et al., S. 830. Neben dem Internet gibt es, wie bereits erwähnt, auch geschlossene »interne« Netzwerke, die Computer miteinander verbinden.

347 Hathaway et al., S. 826.

348 Hathaway et al., S. 830. Ähnlich: Lahmann, S. 35. Ihm zufolge wird das ledigliche Kopieren von Daten im Hinblick auf das Interventionsverbot je nachdem, zu welchem Zweck Daten jeweils kopiert werden bzw. was (z.B. welche Einflussnahme) damit beabsichtigt wird, relevant.

349 In der Schweiz ist für solche Konstellationen insb. Art. 143bis StGB relevant.

350 Zu Beispielen: Hathaway et al., S. 829.

351 Zu einer Definition von Cyberspionage siehe u.a.: Hathaway et al., S. 829.

durch die Manipulation oder die Zweckentfremdung von Informationen tangiert sein.[352] Der Begriff »Cyberangriff« impliziert somit, dass die Handlung oder die Funktionsweise einer Programmierung aktiv sein muss. Dies kann sowohl bei offensiven (*actio*) als auch bei aktiven defensiven Handlungen (*reactio*) der Fall sein.[353] Passive defensive Massnahmen wie Virenscanner, Firewalls[354] oder gem. dem vorliegenden Verständnis auch die passive Informationserhebung zu Investigationszwecken wie mittels Honeypots[355] sind demzufolge nicht erfasst. Aktive Cyberverteidigungskapazitäten wie Hackbacks, Counter-DDoS-Angriffe oder weisse Würmer allerdings schon, wenn dadurch Angriffe abgewehrt und zum Zweck der Verteidigung fremde Computer beeinträchtigt werden.[356] Dabei kann, wie erwähnt, die Schwelle von passiver Informationserhebung zu aktiven Manipulationen (z.B. Eliminierung von Informationen) fliessend sein, da man immer erst in ein System eindringen muss, um dort überhaupt aktiv werden zu können. Hackbacks sind folglich für die vorliegende Analyse dann nicht relevant, wenn sie in gerechtfertiger Weise zu rein passiven Zurückverfolgungs- und Investigationszwecken auf anderen Systemen eingesetzt werden, da solche für eine *völkerrechtliche* Abhandlung der Selbsthilfe nicht vordergründig sind.[357] Obschon solche Massnahmen nicht im Rahmen der nachfolgenden Würdigung aufgegriffen werden, ist dennoch darauf zu verweisen, dass diese durchaus rechtlich relevant werden können. *Jegliches Eindringen in einen Computer* und damit *alle Arten* von Hacking, Hackbacks oder weiterer (Rückverfolgungs-)Techniken muss jeweils unter nationalen Gesetzgebungen gerechtfertigt sein und kann strafrechtliche oder diplomatische Konsequenzen haben.[358] Dies jedoch ist aufgrund des vorliegenden Fokusses auf Völkerrecht Gegenstand anderweitiger Diskussionen.

---

352 Hathaway et al., S. 830. Ähnlich: Walter, S. 687.

353 Hathaway et al., S. 826.

354 Hathaway et al., S. 826. Näher zu Firewalls: Denning, Information Warfare, S. 353.

355 Zu einer Begründung dazu siehe vorangehend unter Fn. 297.

356 Ähnlich: BJ/DV, Gutachten vom 10.03.2009, S. 148 f., S. 175, gem. dem aggressive *computer network exploitations* (CNE) oder defensive Gegenattacken (CND) zu »Angriffen« (CNA) werden können.

357 Grundsätzlich ist gem. Tallinn Manual Spionage völkerrechtlich nicht per se verboten: vgl. Tallinn Manual 2.0, S. 168, R32. Die damit einhergehenden Grenzen sind allerdings Gegenstand anspruchsvoller Diskussionen, womit sie jeweils näher zu betrachten sind. Voliegend sollen sie daher ausgeklammert werden.

358 Dies gilt gleichermassen für »gutartige« Programme: Castañeda/Emre/Xu, S. 84. In der Schweiz ist dafür, wie gesagt, insb. Art. 143bis StGB relevant.

Die für den eigenen Definitionsansatz ausschlaggebende Voraussetzung »*with a political or national security impact*« erlaubt die Unterscheidung eines im Rahmen dieser Analyse relevanten Cyberangriffes von Cyberkriminalität und weiteren Bereichen, in denen nichtstaatliche Akteure grundsätzlich private oder kriminelle Ziele verfolgen.[359] Erfasst werden sollen im vorliegenden Untersuchungsgegenstand Angriffe, die international-politische Sicherheitsbereiche tangieren und deswegen von völkerrechtlicher Relevanz sind. Primär soll dabei nicht ausschlaggebend sein, ob die jeweiligen Schädigungen (politisch) beabsichtigt waren oder nicht. Dadurch werden auch automatisierte Angriffe und technische Fehler vom Untersuchungsgegenstand erfasst, wenn dadurch aktiv Funktionen manipuliert werden und dies Auswirkungen auf die politische und nationale Integrität eines Staates hat. Solche Konstellationen können nämlich vor dem Hintergrund völkerrechtlicher Sorgfaltspflichten von Staaten relevant werden (ausführlicher dazu nachfolgend unter III.B.2.c)). Für eine erfolgreiche völkerrechtliche Zurechnung privater Akteure (oder Programme) an einen Staat muss es sich – an dieser Stelle nur so viel – grundsätzlich um staatliche oder dem Staat gem. den ARSIWA (Staatenverantwortung) oder der *safe harbour*-Doktrin (Selbstverteidigung) zurechenbare Akteure handeln.[360] Oder aber können staatliche Sorgfaltspflichten im Rahmen der sog. Due Diligence betroffen sein, im Rahmen derer die völkerrechtliche Zurechnung an einen Staat wiederum zu unterscheiden ist (dazu ebenfalls ausführlicher nachfolgend unter III.B.2.c)). Diese Ausführungen sind damit insgesamt Gegenstand der rechtlichen Würdigung im nachfolgenden Kapitel B.

Indem sich der hier vertretene Definitionsansatz vom primären Fokus auf physische Schäden entfernt, erlaubt er die Erfassung staatlich relevanter (und aktiver) Cyberangriffe, die verschiedene, auch immaterielle Schäden auslösen. Dies lässt eine differenziertere rechtliche Betrachtung zu, da durch Cyberangriffe eine Vielzahl an sicherheitspolitisch relevanten Effekten herbeigeführt werden kann. Durch Funktionsbeeinträchtigungen von Computersystemen, die mittelbar z.B. breite ökonomische Schädigungen oder politisch motivierte Informationsmanipulationen zur Folge haben, können Cyberangriffe nämlich

359 Hathaway et al., S. 830, (zum Konzept der Cyberkriminalität) S. 834 m.w.H. So unterscheidet die Schweiz bspw. in ihrer nationalen Cyber-Strategie von 2018-2022 (NCS-II) fünf Cyberangriffskategorien: und zwar die der Cyberkriminalität, der Cyberspionage, Cybersabotage und -terrorismus, Desinformation und Propaganda sowie Cyber in Konflikten. Siehe: NCS-II, S. 4 f.

360 Ähnlich: Woltag, S. 24. Zur völkerrechtlichen Zurechnung von nichtstaatlichen Akteuren siehe nachfolgend unter III.B.1.a) und c) (im Rahmen der Selbstverteidigung) und III.B.2.b) (im Rahmen der Staatenverantwortlichkeit).

auch Völkerrechtsnormen ausserhalb des grundsätzlich auf physische Schädigungen ausgerichteten *ius ad bellum* tangieren. Eine begriffliche Beschränkung des Untersuchungsgegenstands auf physische Schäden würde folglich vorab ein gewisses Spektrum möglicher rechtlicher Antworten festlegen.

Hinzu kommt, dass Verletzungen innerhalb der völkerrechtlichen Staatenverantwortlichkeit (»*state responsibility*«) gem. ARSIWA, mitunter also im Gegenmassnahmenrecht, grundsätzlich keinen physischen Schaden voraussetzen. Im Rahmen der Staatenverantwortlichkeit wird jede materielle oder immaterielle Beeinträchtigung einer völkerrechtlichen Rechtsposition als Schaden gezählt.[361] Das heisst mit anderen Worten, dass die *Verletzung* einer völkerrechtlichen Norm *uno actu* die Begründungsvoraussetzung der staatlichen Verantwortlichkeit darstellt.[362] Somit ist kein physischer Schaden erforderlich, um eine Völkerrechtsverletzung gem. ARSIWA zu konstituieren, ausser ein solcher Schaden wird für die Verletzung der primären Norm (z.B. grundsätzlich beim Gewaltverbot gem. Art. 2(4) UN-Charta) vorausgesetzt.[363] Ein Fokus auf (physische) Schäden ist somit im Hinblick auf Normen der Staatenverantwortlichkeit (wie dem Interventionsverbot) nur beschränkt sinnvoll.

Insgesamt lässt es die vorliegend verwendete Definition zu, den Fokus von einem strikt instrument- oder physisch-effektbasierten Ansatz weg zu richten und dadurch Konstellationen zu erfassen, die ungeachtet physischer Schäden staatliche Relevanz erlangen können. Die Definition erfasst mit ihrer Offenheit nämlich verschiedene für Staaten relevante Effekte und Beeinträchtigungen, was eine kontextbezogene Einzelfallwürdigung sowie auch eine Erfassung künftiger, veränderter Angriffsformen erlaubt. Zudem beschränkt sich die Definition nicht nur auf eine bestimmte Akteursgruppe, sondern orientiert sich vielmehr an der sicherheitspolitischen Relevanz. Damit sind grundsätzlich auch (automatisierte) Schadprogramme erfasst. Indem in der nachfolgenden, völkerrechtlichen Analyse neben Art. 51 UN-Charta (*ius ad bellum*) auch die Verletzung von Normen der Staatenverantwortlichkeit (Gewalt- und Interventionsverbot sowie Due Diligence) analysiert werden sollen, ist es sinnvoll auch immaterielle, »sicherheitspolitische« Schädigungen vom Untersuchungsgegenstand zu erfassen. Dies erlaubt es, neben der *ius ad bellum*-Debatte auch eine Würdigung der internationalen Staatenverantwortlichkeit im Cyberkontext aufzugreifen. Denn auch durch Manipulationen und zwangsmässige Ein-

361 SCHULZE, S. 66. Ähnlich dazu: EPINEY, S. 50.

362 ARSIWA-Kommentar, Art. 2(9); SCHRÖDER, S. 702; SCHULZE, S. 66 (m.w.H. in Fn. 88); TANZI, S. 10 ff.

363 Tallinn Manual 2.0, S. 86, R14 C8; ARSIWA-Kommentar, Art. 2(9).

flussnahmen von und durch Informationssysteme, die keine physischen Schäden auslösen, können durchaus Völkerrechtsnormen wie das Gewalt- und Interventionsverbot tangiert sein. Obschon mit der Begriffsverwendung von »Angriff« semantisch an die Analogie einer mit Schäden verbundenen Attacke angelehnt wird,[364] soll dies vorliegend von der rechtlichen Würdigung eines (bewaffneten) Angriffs gem. Art 51 UN-Charta unterschieden werden.[365] Die inhaltliche Distanzierung von physischen Schäden lässt es gleichzeitig zu, sich den abweichenden Ansichten der SCO-Staaten zu nähern.

[364] Die Definition »Cyberangriff« soll an sich keine rechtliche Einordnung nahe legen, sondern dem Ziel einer möglichst umfassenden, zugleich aber neutralen Begriffsumschreibung dienen. Ähnlich: WALTER, S. 686.

[365] Vgl. WOLTAG, S. 24.

B. Völkerrechtliche Würdigung von Cyberangriffen

Aufgrund der divergierenden (rechtlichen und praktischen) Konsequenzen zu Friedens- und zu Kriegszeiten ist es von zentraler Bedeutung, vorab rechtlich zu klären, ob man sich bei einem Cyberangriff überhaupt innerhalb der *ius ad bellum*-Diskussion oder ausserhalb derselben befindet.[366] Die völkerrechtliche Würdigung von (Cyber-)Angriffen führt je nach anwendbarem Regime zu unterschiedlichen Konsequenzen.[367] Die rechtliche Subsumierung eines Cyberangriffs unter das *ius ad bellum*-Regime hat die folgenschwere Konsequenz, dass man mit militärischer Gewalt auf einen Angriff reagieren und – so die lateinische Bedeutung – dies grundsätzlich das Recht »zum Krieg« eröffnet. Befindet man sich daraufhin innerhalb der Kategorie bewaffneter Konflikte (*ius in bello*), führt dies, wie bereits erwähnt, dazu, dass grundsätzlich nur noch die rudimentären Mindeststandards des humanitären Völkerrechts einzuhalten sind.[368] Die Qualifizierung von Cyberangriffen als Völkerrechtsverletzung im Kontext der Staatenverantwortlichkeit hingegen würde gem. den weitgehend als Gewohnheitsrecht anerkannten[369] ARSIWA höchstens nichtmilitärische Gegenmassnahmen ermöglichen. In erster Linie muss also geklärt werden, wie ein betreffender Cyberangriff völkerrechtlich zu würdigen ist – also ob man sich innerhalb des rechtlichen Regimes des *ius ad bellum* oder der völkerrechtlichen Staatenverantwortlichkeit gem. ARSIWA befindet. Daran anküpfend kann eruiert werden, welche militärischen und/oder nicht-militärischen Gegenmassnahmehandlungen verhältnismässig und dadurch gerechtfertigt sind und gegebenenfalls Widergutmachungs- oder Reparationsansprüche ermöglichen.[370]

Im Rahmen des *ius ad bellum* ist insb. die Frage relevant, unter welchen Voraussetzungen ein Cyberangriff einen bewaffneten Angriff im Sinne von Art. 51 UN-Charta darstellen kann. Ausserhalb des *ius ad bellum*-Regimes kommen zwischen dem verletzenden und dem verletzten Staat die Sekundärnormen

366 Die Abgrenzung ist insb. für die weitreichenden rechtlichen und praktischen Folgen eines Kriegs massgebend: NEWTON/MAY, S. 280 f.

367 WOLTAG, S. 85.

368 WOLFENDALE, S. 16.

369 Siehe Ausführungen zur Autorität der ARSIWA unter Fn. 34.

370 Zum Ganzen: WOLTAG, S. 85.

der Staatenverantwortlichkeit gem. ARSIWA zur Anwendung, sollten keine speziellen Rechtsbeziehungen (sog. »Self-Contained Regime«) wie bspw. das System der WTO-Streitbeilegung[371] vereinbart worden sein.[372] Zu den für die Staatenverantwortlichkeit relevanten Völkerrechtsnormen zählen grundsätzlich alle internationalen staatlichen Pflichten, unabhängig davon, ob sie einem oder mehreren Staaten, Individuen, Gruppen oder der internationalen Gemeinschaft als Ganzes geschuldet sind; sowie unabhängig davon, ob die Pflichten aufgrund von Verträgen, gem. traditionellem Völker(gewohnheits-)recht, regional, global oder aufgrund unilateraler Verpflichtungen Geltung beanspruchen.[373] Mitunter sind somit für die internationale Staatenverantwortlichkeit auch die Normen des Gewalts- und Interventionsverbot, Fragen völkerrechtlicher Sorgfaltspflichten sowie weitere völkerrechtliche (Primär- und Sekundär-[374]) Normen relevant.[375] In der vorliegenden Abhandlung sollen im Zusammenhang mit der völkerrechtlichen Staatenverantwortlichkeit das Interventionsverbot und Fragen zu völkerrechtlichen Sorgfaltspflichten (Due Diligence) näher betrachtet werden.

371 Woltag, S. 86.

372 Vgl. Art. 55 ARSIWA. Siehe dazu u.a.: Crawford, State Responsibility, S. 103 ff. m.w.V.; Woltag, S. 86; Zemanek, Unilateral Enforcement, S. 32 ff. insb. unter Bezugnahme auf die Arbeiten der Völkerrechtskommission in ihrer 25. Session 1973 und deren Sonderberichtserstatter Roberto Ago. Vorliegend wird die Haltung vertreten, dass Cyberangriffe kein spezielles Rechtsregime darstellen. Ebenso: Woltag, S 157 f. m.w.V.

373 Crawford, State Responsibility, S. 93 f. m.w.V.

374 Zur Bedeutung von Primär- und Sekundärnormen: Crawford, State Responsibility, S. 64 ff.; David, S. 27 ff.

375 Eingehender zum Verhältnis der UN-Charta mit den Normen der Staatenverantwortlichkeit: Crawford, State Responsibility, S. 106 ff.; Gowlland-Debbas, S. 117 ff., insb. S. 122 ff.

1. *Ius ad bellum*: Bewaffneter Angriff durch Cyberangriffe?

> »*Problems [of interpretation] arise because Article 2(4) [UN-Charter] is a legal rule located in the text of a multilateral treaty which requires adaptation to changing circumstances. The challenge becomes one of remaining faithful to its core meaning without thereby sacrificing the flexibility ordinarily required in interpreting constitutional norms.*«[376]

Mit den Cyberangriffen auf Estland am 27. April 2007 wurde die Staatengemeinschaft mit ihrem System kollektiver Sicherheit gem. SINGER/FRIEDMAN vor einen Jahrhunderttest gestellt.[377] Das beinahe gesamtstaatliche Aussetzen digitaler Infrastrukturen hat die digitale Nation (zu jenem Zeitpunkt noch in überraschender Weise) regelrecht paralysiert. Da Estland die Unterstützung seiner NATO-Verbündeten forderte,[378] kam die Frage auf, ob Cyberangriffe einen bewaffneten Angriff i.S.v. Art. 51 UN-Charta darstellen können, der das Recht auf (kollektive) Selbstverteidigung auslöst. Das Selbstverteidigungsrecht wurde in der Folge eines der meistdiskutierten Themen im Zusammenhang mit Cyberangriffen.[379] Die erwähnten Cyberangriffe auf Estland sind vor diesem Hintergrund insgesamt sehr illustrativ dafür, wie alte Rechtsnormen eines über Jahrzehnte etablierten Systems und neue Technologien (und deren Schädigungsradien) aufeinandertreffen.[380] Sie haben insb. die fundamentale Frage aufgeworfen, was die Bedeutung von völkerrechtlicher »Gewalt« oder »bewaffnetem Angriff« im 21. Jahrhundert ist.[381] Muss »Gewalt« angesichts neuer Technologien neu definiert oder erweitert werden? Oder soll man dem traditionellen Verständnis treu bleiben? Wenn ja, wie können Cyberangriffe darunter subsumiert werden? Vorliegend soll ein Abriss einiger zentraler Problemfelder dieser Diskussion erfolgen.

---

376 GORDON, S. 273.

377 SINGER/FRIEDMAN, S. 122 f.

378 HARRISON DINNISS, S. 39. Während der Angriffe auf Estland 2007 haben verschiedene estnische Regierungsmitglieder die Frage aufgebracht, ob eine kollektive Verteidigung gem. Art. 5 des Nordatlantikvertrags vom 04.04.1949 zum Tragen kommt: SHACKELFORD/ANDRES, S. 1012. Dies wurde anderen Ansichten zufolge allerdings nicht ernsthaft in Betracht gezogen: TIKK/KASKA/VIHUL, S. 25 f. Gemäss der Deklaration des Wales Summit des Nordatlantikrats vom 05.09.2014 können Cyberangriffe allerdings für Art. 5 des Nordatlantikvertrags relevant werden: NATO, Wales Summit Declaration vom 05.09.2014. Siehe dazu: BANKS/CRIDDLE, S. 91.

379 Siehe inter alia: DIGGELMANN/HADORN, S. 261; FOCARELLI, S. 317 ff.; GERVAIS, S. 541 ff.; HARRISON DINNISS, S. 1 ff.; RADZIWILL, S. 125 ff.; TSAGOURIAS, S. 229 ff.; WOLTAG, S. 135 ff.

380 SINGER/FRIEDMAN, S. 122 f.

381 HARRISON DINNISS, S. 40.

a. Grundidee des *ius ad bellum*

Das in Art. 2(4) UN-Charta statuierte Gewaltverbot als fundamentales Prinzip des Völkerrechts verbietet es den Staaten grundsätzlich, gegen die territoriale Integrität oder die politische Unabhängigkeit eines anderen Staates Gewalt anzuwenden oder diesem die Anwendung solcher anzudrohen.[382] Dieses Verbot wird über die UN-Charta hinaus als allgemein anerkanntes, zentrales Völkergewohnheitsrecht (und teilweise sogar als *ius cogens*[383]) gesehen.[384] Von der Idee her ist Gewaltanwendung kategorisch verboten und im Grunde auch kein zulässiges Sanktionsmittel bei Völkerrechtsverletzungen.[385]

Das Prinzip des Gewaltverbots darf nur unter äusserst restriktiven Voraussetzungen durchbrochen werden; und zwar nur, wenn ein angegriffener Staat entweder durch den Sicherheitsrat gem. Art. 42 UN-Charta ermächtigt wurde oder wenn ein bewaffneter Angriff gem. Art. 51 UN-Charta gegeben ist und im Rahmen der individuellen oder kollektiven Selbstverteidigung abgewehrt werden muss.[386] Wichtig zu verstehen ist, dass dieses Recht eine Ausnahme vom Grundsatz des global anerkannten Gewaltverbots ist.[387] Die Grundidee des Selbstverteidigungsrechts ist, dass ein Staat die (verhältnismässige[388]) Möglichkeit zur Beendigung unmittelbarer gewaltsamer Verletzungen seines Territoriums zur Erhaltung seiner Existenz haben soll.[389] Zeitlich ist die Ausübung dieses Rechts auf einen frühestmöglichen und spätestzulässigen Zeitpunkt beschränkt: Es darf nur ausgeübt werden, solange der Angriff noch im Gange

382 Siehe Wortlaut von Art. 2(4) UN-Charta.

383 Siehe IGH, Nicaragua-Urteil, §190. Dazu u.a.: Dinstein, War, Aggression and Self-Defence, S. 109 ff.

384 Der IGH hat dies wiederholt betont: IGH, Nicaragua-Urteil, §190; IGH, Kongo-Urteil, §148; IGH, Schutzmauer-Gutachten, §86 f.; Dahm/Delbrück/Wolfrum, Bd. I/3, S. 822; Dinstein, Computer Network Attacks, S. 100; ferner Harrison Dinniss, S. 40; Woltag, S. 134.

385 Diggelmann, NZZ vom 30.05.2013.

386 Diggelmann, Völkerrecht, S. 158; Gray, The Charter Limitations, S. 86 ff.; Harrison Dinniss, S. 42.

387 Diggelmann, Völkerrecht, S. 158.

388 Die Verhältnismässigkeit wird in der Völkerrechtslehre überwiegend vom prominenten Caroline-Fall aus dem Jahr 1837 abgeleitet: Siehe dazu: Jennings, S. 82 ff. Oft wird auch im kontemporären Diskurs auf den Caroline-Fall verwiesen: u.a. Lahmann, S. 55.

389 Diggelmann, NZZ vom 30.05.2013. Ähnlich in: IGH, Nuklearwaffen-Gutachten, §96. Anderer Ansicht: Dinstein, War, Aggression and Self-Defence, S. 203 f.

ist.[390] Das Selbstverteidigungsrecht ist der Natur nach somit als Abwehr- oder Notwehrrecht mit Beendigungsfunktion konzipiert und nicht als Vergeltungsrecht.[391] Interessant dabei ist – und dies zeigt sich auch am auffälligen Interesse gewisser Staaten an einem Anspruch auf Selbstverteidigung im Cyberkontext – dass ein Recht auf Selbstverteidigung im historisch gewachsenen Selbstverständnis der Staaten grundsätzlich als »naturgegeben« (oder im Englischen »*inherent right*«) gesehen wird.[392] In den Zeiten vor dem Gewaltverbot wurde das Recht zum Krieg (*ius ad bellum*) nämlich als ein dem Staat inhärenter Anspruch und teilweise sogar als legitimes Sanktionierungsmittel gesehen.[393] Indem Krieg also nicht im heutigen Sinne verboten war, erübrigte sich daher die Institution eines ausnahmsweisen Selbstverteidigungsrechts.[394] Mit anderen Worten drängte sich erst mit der globalen Kriegsächtung und dem späteren Gewaltverbot eine Kodifizierung eines solchen (ab jenem Zeitpunkt zur Ausnahme gewordenen) Rechts gegen bewaffnete Angriffe überhaupt auf.[395]

Die exakte Bedeutung eines bewaffneten Angriffs wurde über Jahrzehnte in der Lehre und der internationalen Rechtsprechung (insb. auch durch den IGH) diskutiert und konkretisiert.[396] Der IGH hat dabei ausdrücklich auf die Unklarheit des Begriffs verwiesen.[397] Breiter Konsens besteht immerhin (überwiegend ausserhalb der USA[398]) darin, dass nicht jeder Angriff, der unter Gewalt i.S.v. Art. 2(4) UN-Charta subsumiert wird, einen bewaffneten Angriff i.S.v. Art. 51 UN-Charta konstituiert.[399] Ein bewaffneter Angriff setzt einen erheblichen, kausalen Verlust an Menschenleben oder weitreichende Zerstörung

390 Diggelmann/Hadorn, S. 262; Kammerhofer, Restrictivist Rules, S. 629; Schachter, In Defense of International Rules, S. 132.

391 Diggelmann/Hadorn, S. 262. Ausführlicher dazu nachfolgend unter den in Teil IV.A abgehandelten Aspekten der Verhältnismässigkeit.

392 Siehe Wortlaut von Art. 51 UN-Charta. Dazu u.a. auch: Gray, The Charter Limitations, S. 86.

393 Eingehender dazu: Lesaffer, S. 35 ff.

394 Lesaffer, S. 35 ff. Ferner: Woltag, S. 175.

395 Vgl. Wortlaut von Art. 51 UN-Charta: »*nothing shall impair*«. Dazu auch: Woltag, S. 175.

396 Diggelmann/Hadorn, S. 262; Harrison Dinniss, S. 77 ff.; Woltag, S. 177.

397 IGH, Nicaragua-Urteil, §176.

398 Die USA und ein grosser Teil der US-Lehre geht davon aus, dass eine Gewaltanwendung mit einem bewaffneten Angriff gleichzustellen ist. Die Unterscheidung zwischen verschiedenen Schwellen der Gewaltanwendung im Nicaragua-Urteil z.B. wurde insb. durch US-amerikanische Autoren kritisiert, siehe z.B.: Kirgis et al., S. 258 ff.; vgl. dazu Harrison Dinniss, S. 50.

399 Dinstein, Computer Network Attacks, S. 100; Harrison Dinniss, S. 77; Woltag, S. 176; Kammerhofer, Restrictivist Rules, S. 629 m.v.a. IGH, Nicaragua-Urteil, §191, §195.

voraus, womit auf die Intensität der Folgen oder möglicher Folgen abgestellt wird.[400] Das Selbstverteidigungsrecht hängt somit nach überwiegender Ansicht nicht von der Qualifikation einer Waffe oder der Beschaffenheit und Funktion des Ziels (wenn z.B. kritische Infrastrukturen angegriffen werden) ab.[401] Wegweisend für die Beurteilung sind vielmehr die Effekte eines bewaffneten Angriffs, die weitgehend nach dem sog. (z.T. kritisierten[402]) *scale and effects*-Ansatz des IGH gewürdigt werden. Dieser verlangt eine genügend hohe Schwelle, um einen Angriff von »blossen Grenzvorfällen« abzuheben.[403] Dabei ist die Intensität jeweils anhand der Umstände des Einzelfalles zu würdigen und bleibt in diesem Sinne flexibel.[404] So hat der IGH im Ölplattformen-Urteil das Bombardieren eines einzelnen Militärschiffs als unter Umständen genügend erachtet, um einen bewaffneten Angriff zu konstituieren,[405] während er gleichzeitig ein isoliertes Abfeuern einer Rakete auf ein Handelsschiff als ungenügend erachtet.[406] Dem IGH zufolge ist es daher nicht möglich, das Konzept *in abstracto* definitiv festzulegen.[407] So würde bspw. auch ein (physisches) Zerstören von Heizsystemen in einer warmen Region je nachdem keinen bewaffneten Angriff darstellen, während dies in einer kalten Region, in der daraufhin Individuen erfrieren würden, unter Umständen anders zu würdigen wäre. Der Unterschied wäre, dass im ersten Beispiel zwar das Gewaltverbot nach Art. 2(4) UN-Charta verletzt sein könnte, was allenfalls nichtmilitärische Massnahmen legitimieren könnte, die Intensität des konkreten

400 Diggelmann/Hadorn, S. 262; Heintschel von Heinegg, Informationskrieg, S. 141; Woltag, S. 177. Ferner dazu auch: Dinstein, War, Aggression and Self-Defence, S. 209 ff.; Harrison Dinniss, S. 78; Randelzhofer/Nolte, S. 1401 ff.

401 Diggelmann/Hadorn, S. 262; Woltag, S. 177 m.V.a. IGH, Nuklearwaffen-Gutachten, §39. Zu verschiedenen Interpretationen völkerrechtlicher Gewalt ferner: Waxman, Cyber-Attacks, S. 428 ff. Hingegen von der Beschaffenheit und Funktion des angegriffenen Ziels ausgehend z.B.: Li, S.186 f.

402 Siehe dazu: Harrison Dinniss, S. 78.

403 IGH, Nicaragua-Urteil, §195. Siehe dazu auch: Corten, Law Against War, S. 403; Kretzmer, S. 242 ff.; Randelzhofer/Nolte, S. 1409. Kritisch dazu: Dinstein, War, Aggression and Self-Defence, S. 209 ff.

404 Green, S. 41; Lahmann, S. 49.

405 IGH, Ölplattformen-Urteil, §72. Eingehender zum Urteil: Laursen, Oil Platforms Case, S. 135 ff.; Orakhelashvili, S. 753 ff. Auch das Tallinn Manual statuiert, dass der IGH im Nicaragua Fall zwar festhält, dass es eine gewisse Schwere braucht, um die Schwelle des bewaffneten Angriffs zu erreichen, diese jedoch nicht weiter spezifiziert: Tallinn Manual 1.0, S. 55 R13 C6.

406 IGH, Ölplattformen-Urteil, §64. Zu einer (kritischen) Betrachtung des Ölplattformen-Urteils und den damit verbundenen Methoden des IGH: Raab, S. 719 ff.

407 Lahmann, S. 49. Ähnlich: Green, S. 41; Taft, S. 295 ff.; von Carlowitz, S. 88.

Einzelfalles allerdings nicht ausreichen würde, um eine militärische Selbstverteidigungsmassnahme auszulösen.[408] Im Vergleich zum Gewaltbegriff ist der Anwendungsbereich des bewaffneten Angriffs also grundsätzlich enger und das Erfordernis von Zerstörung und Verletzten höher.[409] Somit soll ein Staat bei der Verletzung des Gewaltverbots nicht automatisch mit militärischer Gewalt reagieren können dürfen.[410] Hinzu kommt, dass für die Bejahung eines bewaffneten Angriffs gewissen Ansichten zufolge jeweils zumindest ein *momentum* eines Vorsatzes enthalten sein muss.[411] Wird ein für einen bewaffneten Angriff relevanter Schaden vollkommen unbeabsichtigt ausgelöst, würde dieser Lesart zufolge der notwendige *animus aggressionis* fehlen, was folglich eine gewaltsame Selbstverteidigung ausschliessen würde.[412] Der IGH scheint dieses Argument in seiner Ölplattformen-Entscheidung zu unterstützen, indem er eine »spezifische Intention« einer Schädigung in seine Würdigung miteinbezog und willkürliche (Folge-)Schädigungen unbeabsichtigter Ziele nicht für das Recht auf Selbstverteidigung ausreichen liess.[413] Vor dem Hintergrund, eine Eskalation möglichst zu vermeiden, scheint diese Haltung überzeugend.[414] Daher sollen auch der vorliegenden Ansicht nach zumindest Elemente einer (Eventual-)Vorsätzlichkeit für die Bejahung von Art. 51 UN-Charta vorausgesetzt werden.

Jüngere Entwicklungen haben des Weiteren die kontroverse Debatte aufgeworfen, ob bewaffnete Angriffe nach Art. 51 UN-Charta auch bei nichtstaatlichen Akteuren bejaht werden können.[415] So wurde im Zusammenhang mit den terroristischen Anschlägen vom 11. September 2001 (fortan: 9/11) zumindest eine teilweise Bereitschaft einer solchen Möglichkeit manifestiert.[416] Das Thema ist allerdings komplex und Gegenstand einer anspruchsvollen De-

408 IGH, Nicaragua-Urteil, §195; Diggelmann/Hadorn, S. 262.

409 Woltag, S. 176; Heintschel von Heinegg, Informationskrieg, S. 141; Randelzhofer/Nolte, S. 1401 f.

410 Woltag, S. 176.

411 Lahmann, S. 50 f. m.w.V. Anderer Ansicht: Zemanek, MPEPIL 2013, §9.

412 Lahmann, S. 51; Ruys, S. 177.

413 IGH, Ölplattformen-Urteil, §64; Lahmann, S. 51.

414 Ebenso: Lahmann, S. 60.

415 Eingehender zur Selbstverteidigung gegen nichtstaatliche Akteure i.Z.m. 9/11: Gray, Use of Force, S. 120 ff.; Ruys, S. 419 ff. Siehe auch: Kress, S. 585.

416 Tallinn Manual 2.0, S. 435 R71 C18. Siehe dazu: UN Doc. S/RES/1368 (2001); UN Doc. S/RES/1373 (2001), in denen terroristische Anschläge als Bedrohung der internationalen Sicherheit anerkannt werden und auf das Recht auf Selbstverteidigung verwiesen wird. Ähnlich bestätigte die NATO die grundsätzliche Anwendbarkeit von Art. 5 des Nordatlantikvertrags: NATO, Press Release, Statement by the North Atlantic Council vom 12.09.2001.

batte.[417] Letztlich muss eine Selbstverteidigungshandlung zudem jeweils dem Verhältnismässigkeitsgrundsatz genügen, mitunter also die Erfordernisse der Unmittelbarkeit und Notwendigkeit erfüllen.[418]

b. Unterschiedliche Verständnisse des *ius ad bellum*

Die vorangehend angeführten Ansichten zum Anwendungsbereich der Selbstverteidigung – und dies ist eine wesentliche Herausforderung internationaler Konsensfindungen – divergieren nicht nur in der Lehre, sondern gerade auch unter Staaten teilweise beträchtlich.[419] So gehen, um ein prominentes Beispiel zu nennen, die Ansichten der USA und von Kontinentaleuropa in dieser Frage auseinander.[420] Interpretationen völkerrechtlicher Normen, die letztlich zu (militärischen) Entscheiden führen, müssen nicht nur kritisch hinterfragt, sondern auch im jeweiligen kulturellen Kontext verstanden werden. Für diese Dissertation sind diese Divergenzen insofern relevant, als sie auch die Interpretationsmöglichkeiten von Art. 2(4) und Art. 51 UN-Charta im Cyberkontext beeinflussen.[421] Die im vorangehenden Abschnitt erläuterten Voraussetzungen der Selbstverteidigung sind typisch für den gem. Banks/Criddle in Kontinentaleuropa vorherrschenden »*conventional restrictivism*«,[422] der primär die Beschränkung der Gewaltanwendung und eine restriktive Handhabung des Selbstverteidigungsrechts (hohe Schwelle) zum Ziel haben. Diese Lesart sieht die Stärkung universellen Friedens durch eine Beschränkung unilateraler Gewaltanwendung (auch zur Verteidigung) auf das absolut Erforderliche als übergeordnetes Ziel der UN-Charta (auch als sog. *ius contra bellum*[423] umschrie-

417 Diggelmann/Hadorn, S. 272; Kammerhofer, Restrictivist Rules, S. 637 ff. m.w.V. Teilweise wird in der Lehre sogar geltend gemacht, dass keine Zurechenbarkeit an einen Staat vorausgesetzt sei. Dies enspricht allerdings überwiegend nicht der Absicht der Vertragsstaaten: Gray, Use of Force, S. 139 ff. m.w.V. Zudem vertritt auch der IGH eine enge Auslegung von Art. 51 UN-Charta und setzt die Zurechenbarkeit an einen Staat voraus: IGH, Nicaragua-Urteil, § 57, §113 ff.

418 Jennings, S. 82 ff. Ausführlicher dazu nachfolgend in Teil IV.A.

419 Substanziell zu den inhärenten Uneinigkeiten in der Lehre im Hinblick auf das Selbstverteidigungsrecht: Kammerhofer, Kelsenian Perspective, S. 5 ff., insb. S. 56.

420 Siehe dazu: Banks/Criddle, S. 67 ff. Zu den divergierenden Interpretationen siehe auch: Gray, The Charter Limitations, S. 94 f. Kammerhofer, Uncertainties, S. 199 ff. und S. 201 f. m.w.V.

421 Banks/Criddle, S. 69 ff.

422 Banks/Criddle, S. 70.

423 Siehe dazu: Corten, Law Against War, S.1 ff.; Van Steenberghe, S. 747 ff.; Woltag, S. 85.

ben).[424] Selbstverteidigung ist dieser Ansicht zufolge, wie im vorangehenden Abschnitt beschrieben, als Selbsthilfe nur ausnahmsweise erlaubt, wenn der betroffene Staat keine anderweitigen nicht-militärischen Mittel hat, um seine territoriale Unversehrtheit und politische Unabhängigkeit zu verteidigen. Das Ziel von Art. 51 UN-Charta ist dieser Lesart zufolge nicht der primäre Schutz von Individuen vor jedem staatsübergreifenden Angriff, sondern vielmehr, dass ein Staat – wie vorangehend erwähnt – seine Existenz in einer eng definierten Ausnahmesituation verteidigen können soll.[425] Dieser Ansatz dient demzufolge dem übergeordneten Ziel der UN-Charta, übermässige Gewalt möglichst zu beschränken.

In der US-amerikanischen Lehre hingegen hat sich gem. Banks/Criddle die Tendenz eines sog. »*customary restrictivism*« entwickelt, dem anderweitige Grundideen zugrunde liegen als dem in Europa vorherrschenden »*conventional restrictivism*«. Die Stärkung universellen Friedens und die Gewalteinschränkung als Hauptziele des europäischen *conventional restrictivism* haben in jenem Ansatz vergleichsweise wenig Resonanz gefunden[426] und passen gem. Banks/Criddle nicht in die Tradition US-amerikanischer Lehre zum *ius ad bellum*.[427] Prominent ist, dass ein Teil der US-amerikanischen Ansicht nicht zwischen der Schwelle einer Gewaltanwendung gem. Art. 2(4) UN-Charta und einem bewaffneten Angriff gem. Art. 51 UN-Charta unterscheidet.[428] Einige Autoren kritisieren in diesem Zusammenhang die vom IGH im Nicaragua-Urteil vorgenommene Unterscheidung von bewaffneten Angriffen und geringe-

424 Banks/Criddle, S. 69. Ihnen zufolge argumentieren *conventional restrictivists* typischerweise auch gegen die Anwendbarkeit der Selbstverteidigung gegen nichtstaatliche Akteure ohne die Einwilligung des betreffenden Staates, da dies nicht mit dem Sinn und Zweck der UN-Charta übereinstimme. Zur Verschiebung des *ius ad bellum* hin zum *ius contra bellum* auch: Heintschel von Heinegg, Friedenssicherung, S. 1131 ff.

425 Banks/Criddle, S. 70; Kammerhofer, Uncertainties, S. 201 f.

426 Zu ähnlichen Schlüssen: Kammerhofer, Restrictivist Rules, S. 633.

427 Banks/Criddle, S. 69.

428 Siehe u.a. Sofaer, S. 422; Schmitt, Grey Zones, S. 15. Dazu auch: Dinstein, War, Aggression and Self-Defence, S. 205; Roscini, Cyber Operations, S. 105 m.V.a. die richterliche Gegenmeinung von Simma im Ölplattformen-Urteil, §12; Tallinn Manual 1.0, S. 47 R11 C7. Im Tallinn Manual hingegen haben sich die Experten darauf geeinigt, dass ein bewaffneter Angriff eine höhere Schwelle des »*scale and effects*« erfordert: Tallinn Manual 1.0, S. 55 R13 C5; Tallinn Manual 2.0, S. 341, R71 C6.

ren Gewaltanwendungen.[429] Der Gerichtshof hatte den USA in jener Entscheidung durch seine restriktive Würdigung von Art. 51 UN-Charta das Recht auf Selbstverteidiung abgesprochen, da Grenzvorfälle keinen bewaffneten Angriff konstituieren können sollen.[430] Kritischen Ansichten zufolge sollen allerdings auch geringere Grenzvorfälle das Recht auf Selbstverteidigung erlauben.[431] Die hohe Schwelle eines bewaffneten Angriffs würde Staaten davon abhalten, ihre Zivilbevölkerung im Einzelfall schützen zu können.[432] Mit anderen Worten wird letzterer Haltung zufolge eine kritische Lücke für effektive Reaktionsmöglichkeiten für Staaten gesehen, wenn sie Opfer einer Gewaltanwendung wurden, die der Lesart des *conventional restrictivism* (und dem IGH) zufolge noch keinen bewaffneten Angriff konstituieren würde.[433] Ein Staat sei durch die Unterscheidung von Gewaltanwendungen und bewaffneten Angriffen bei kleineren Angriffen oder bei Angriffen durch private Akteure (wie es diese im Cyberkontext oft gibt) »wehrlos« ohne die Autorisierung des UN-Sicherheitsrats.[434] Damit gemeint ist, dass sie nicht *unilateral militärisch* auf Gewaltanwendungen unterhalb der Schwelle eines bewaffneten Angriffs nach Art. 51 UN-Charta reagieren können. Die Tolerierung verschiedener Formen geringerer Gewaltanwendungen – so eine dahingehende Argumentation – führe insgesamt zu einem Anstieg von Gewalt im internationalen Umfeld.[435] Eine Unterscheidung von Grenzvorfällen und bewaffneten Angriffen würde sich zudem erübrigen, wenn man der Lesart folgt, dass die Prinzipien der Verhältnis- und Notwendigkeit genügenden Schutz gegen exzessive Gewaltanwendungen bieten würden.[436] Der Gewalt*einschränkung* dienende Ansichten innerhalb der USA beziehen sich daher gem. Banks/Criddle – anders als in Kontinentaleu-

429 Dinstein, War, Aggression and Self-Defence, S. 209 ff. Dazu auch: Schachter, In Defense of International Rules, S. 143 m.V.a. IGH, Nicaragua-Urteil, (Gegenmeinung Richter Schwebel) betreffend §191 ff.; Macdonald, S. 150 f.; Hargrove, S. 139. Eingehender zur Kritik an der Unterscheidung eines bewaffneten Angriffs und Grenzvorfällen des IGH: Gray, Use of Force, S. 155;

430 IGH, Nicaragua-Urteil, §191, §195, §230. Im Zusammenhang mit der Unterscheidung von Grenzvorfällen und bewaffnetem Angriff hat der IGH in seinem Nicaragua-Urteil den oft zitierten »*scale and effects*«-Ansatz etabliert: Siehe unter §195 sowie vorangehend unter B.1.a).

431 So z.B. Hargrove, S. 139; Kunz, S. 878; Badr, S. 1, S. 10 ff.

432 Näher zu den unterschiedlichen Auffassungen siehe Kammerhofer, Uncertainties, S. 201 f. m.V.a. Bowett, S. 8 ff.; Ago, S. 61 §106.

433 So z.B.: Dinstein, War, Aggression and Self-Defence, S. 209 ff. Dazu (jedoch anderer Ansicht): Randelzhofer/Nolte, S. 1401 ff.; Woltag, S. 176.

434 Banks/Criddle, S. 70.

435 Reisman, S. 39 f.

436 Higgins, S. 251 mit Verweis auf die Schwierigkeiten solcher Debatten.

ropa – stark auf die generell von der Staatengemeinschaft anerkannten, gewohnheitsrechtlichen Rechtsprinzipien der Notwendig- und Verhältnismässigkeit.[437] Diese beiden Prinzipien werden zudem oftmals angeführt, um sich *für* militärische Massnahmen auszusprechen, indem eine gewaltsame Verteidigung in bestimmten Konstellationen als notwendig erachtet wird,[438] die restriktiven Ansichten zufolge ausgeschlossen wäre.[439]

Das US-amerikanische Verständnis des *ius ad bellum* ist des Weiteren stark von der Idee geprägt, dass dieses mit der Zeit weiterentwickelt und durch die ständige Etablierung von Staatenpraxis und *opinio iuris* neuen Gefahren angepasst werden können soll.[440] Gemäss Banks/Criddle weist diese Haltung Parallelen zur Tradition des *common-law* auf, das durch Gerichtsentscheidungen kontinuierlich weiterentwickelt wird.[441] Diese Auffassung bezieht sich auch auf die für die Interpretation des *ius ad bellum* relevante Verhältnismässig- und Notwendigkeit, da diese Rechtsprinzipien neue Entwicklungen erfassen können sollen.[442] Im Ergebnis erlaubt eine solche Lesart eine relativ flexible, sich unter Umständen vom historischen Sinn und Zweck sowie vom Wortlaut entferndende Interpretation des *ius ad bellum*. Diese US-amerikanisch geprägte Einstellung zum *ius ad bellum* spiegelte sich in verschiedenen völkerrechtlich relevanten Konflikten[443] wider und beeinflusst die Debatten zur antizipatorischen Selbstverteidigung,[444] zu Selbstverteidigungshandlungen gegen nichtstaatliche Akteure[445] sowie die Debatte zur Regulierung von Cyberangriffen[446] (dazu später eingehender). Eines der Hauptargumente dahinter ist, dass eine historische Auslegung des *ius ad bellum* ungenügend sei, um neue Veränderungen und Gefahren zu erfassen.[447] Daher soll es möglich sein, dieses an sich

437 Banks/Criddle, S. 68 m.w.V.

438 Diese US-Argumentationslinie ist u.a. bspw. ersichtlich in: Clinton, Letter to Congressional Leaders vom 21.08.1998. Eingehender dazu: Banks/Criddle, S. 81; Murphy, S. 163.

439 Zur Notwendig- und Verhältnismässigkeit bei der Selbstverteidigung eingehender nachfolgend unter Kapitel IV.A.

440 Banks/Criddle, S. 92.

441 Banks/Criddle, S. 76 m.V.a. Dyzenhaus, S. 131.

442 Banks/Criddle, S. 68.

443 Zu einer Abhandlung der Argumentationslinien der USA in Konflikten in Afghanistan, dem Irak oder Syrien: u.a. Gray, Limits of Force, 101 ff.

444 Eingehender zur US-Haltung zur antizipatorischen Selbstverteidigung m.w.V.: Banks/Criddle, S. 77 ff.; Franck, Recourse to Force, S. 97 ff.

445 Siehe eingehender dazu: Banks/Criddle, S. 80 ff.; Gray, Limits of Force, S. 113 ff.

446 Eingehender dazu m.w.V.: Banks/Criddle, S. 87 ff.

447 Zur Bush-Doktrin siehe u.a.: Bradford, S. 1365 ff.

ändernde Bedürfnisse der internationalen Gemeinschaft anpassen zu können.[448] Einer solchen Lesart zufolge soll das Selbstverteidigungsrecht demnach auch an moderne Technologien (wie Cyberangriffe) angepasst und – das ist für die vorliegende Dissertation zu betonen – potenziell auch *ausgeweitet* werden können.[449]

Im Ergebnis lässt die US-amerikanisch geprägte Ansicht in gewissen Konstellationen die Anwendung von Gewalt zu, die vom europäischen *conventional restrictivism* kategorisch ausgeschlossen wären.[450] Es wird argumentiert, dass durch eine enge Interpretation von Art. 51 UN-Charta zugunsten des Friedens zwischen Staaten an Recht und Sicherheit für individuelle Opfer staatsübergreifender Angriffe eingebüsst werde. Dies sei angesichts der zunehmenden Gefahren für die Sicherheit in einer von Massenvernichtungswaffen und Terroranschlägen geprägten Welt nicht vertretbar.[451] Diese Haltung widerspiegelt letztlich ein vom in Kontinentaleuropa verbreiteten Ansatz abweichendes Verständnis des Sinn und Zwecks des Systems kollektiver Sicherheit der UN-Charta:[452] Als primärer Zweck der Selbstverteidigung wird in den USA überwiegend eine gerechte Weltordnung gesehen, die »politische Selbstbestimmung von Staaten und einen vernünftigen Grad an Sicherheit für dessen Bürger garantieren soll«.[453] Dieser Lesart zufolge stellt das Selbstverteidigungsrecht gewissermassen ein von der Souveränität abgeleitetes Recht und zugleich eine Verantwortung eines Staates dar, sein Volk vor Verletzungen zu schützen.[454] Insofern, und dies wurde auch im Zusammenhang mit 9/11 ersichtlich, scheinen die USA im Gegensatz zu Europa eher gewillt, Interpretationsspielräume im kollektiven Sicherheitssystem der UNO dahingehend auszulegen, dass ein Staat zur »Förderung von Sicherheit« Gewalt anwenden

448 Banks/Criddle, S. 92 m.V.

449 Gray, Limits of Force, S. 113. Ein Teil der US-Lehre argumentiert, dass eine militärische Selbstverteidigung die politische Unabhängigkeit oder die territoriale Integrität eines anderen Staates nicht verletzt. Siehe z.B. Bradford, S. 1376 ff.

450 Banks/Criddle, S. 68 m.V.a. O'Connell, Self-Defense, S. 894 f.

451 Banks/Criddle, S. 73.

452 Banks/Criddle, S. 73.

453 Banks/Criddle, S. 73 m.V.a. Glennon, S. 2; Rawls, S. 91.

454 Banks/Criddle, S. 74 m.w.V. Ausführlicher zu den unterschiedlichen Verständnissen der Selbstverteidigung als Recht oder als Ausnahme: Kammerhofer, Kelsenian Perspective, S. 5 ff., insb. S. 50. Ferner dazu auch: Dinstein, War, Aggression and Self-Defence, S. 200 ff. (unter Verwendung der Begriffe »Recht« oder »Pflicht«).

können soll.[455] Ein Grossteil der US-amerikanischen Lehre ist also nicht bereit, einer restriktiven Auslegung von Art. 51 UN-Charta zu folgen, die Frieden zwischen Staaten auf Kosten von »Gerechtigkeit und Sicherheit eigener Bürger« bevorzugt.[456]

Was jedoch heisst »gerecht«, was ist ein »vernünftiger Grad an Sicherheit«, und schliesst Stabilität Gerechtigkeit aus? Fördert man nicht gerade mehr Sicherheit und schützt man letztlich nicht mehr Individuen durch die *Verhinderung* von Krieg? Diese Fragen zeigen, dass Interpretationsspielräume zum Sinn und Zweck des *ius ad bellum* bestehen bleiben, dass es im Völkerrecht nicht immer um Gerechtigkeit für eigene Staatsangehörige, sondern (zumindest einer Interpretationsmöglichkeit zufolge) oft auch um die Schaffung eines internationalen Gleichgewichts geht. Diese Dissertation folgt im Hinblick auf das Selbstverteidigungsrecht dem in Kontinentaleuropa vorherrschenden Ansatz des *conventional restrictivism* und muss auch in diesem Kontext verstanden werden. Die Beschränkung militärischer Gewalt auf den restriktiv anzunehmenden Ausnahmefall von Art. 51 UN-Charta wird dahingehend verstanden, dass diese historisch gesehen kein Versehen, sondern Absicht ist.[457] Diese mitunter vom IGH gestützte,[458] rechtliche Unterscheidung von Art. 51 UN-Charta und Art. 2(4) UN-Charta ist gerade dazu gedacht, dass ein Konflikt mit weniger schwerwiegenden Gewaltanwendungen nicht eskaliert.[459] Gewaltanwendungen gem. Art. 2(4) UN-Charta, die keinen bewaffneten Angriff darstellen, sollen bewusst nur *nicht-militärische*, gewaltfreie Konfliktlösungsmethoden und

455 Banks/Criddle, S. 73 m.V.a. Fletcher/Ohlin; Bradford; Ohlin, Legitimate Defense, S. 119 ff.

456 Banks/Criddle, S. 73. Vgl. Dazu auch: Schachter, Armed Force, S. 1628.

457 Siehe u.a. Randelzhofer/Nolte, S. 1402 f.; Woltag, S. 177.

458 IGH, Nicaragua-Urteil, §191, §195, §230. Dazu, dass der IGH auch im Öl-Platformen-Urteil einen restriktiven Ansatz zur Gewaltanwendung verfolgte und dabei keine der seitens USA vorgebrachten Argumente bestätigte, die Selbstverteidigung extensiver anzuwenden: von Carlowitz, S. 79 ff.

459 Randelzhofer/Nolte, S. 1402. Vgl. dazu auch Schachter, Armed Force, S. 1628, der vor dem Hintergrund einer restriktiven Auslegung des Gewaltverbots auf die Einbusse von Gerechtigkeit für Frieden Bezug nimmt. Er anerkennt zwar, dass Art. 2(4) UN-Charta Gewalt nicht durchwegs einschränken kann, wenn Territorialansprüche involviert und friedliche Alternativen nicht vorhanden sind. Im Ergebnis sieht er dies jedoch nicht als berechtigte Argumente, um Art. 2(4) UN-Charta zu extensiv zu verstehen und eskalatorische Gewalt zu legitimieren: »*Yet unfortunate as this may be it cannot be an argument for opening up a large exception to article 2(4). That would legitimize the use of force on a scale that cannot be tolerated when force tends to escalate and spread*«.

eben *keine* gewaltsame, militärische Verteidigung ermöglichen.[460] Fälle ausserhalb des Anwendungsbereichs eines bewaffneten Angriffs befinden sich daher nicht in einem rechtsleeren Raum, sondern es können Ausgleichs- und Reparationsansprüche sowie *nicht-militärische* Gegenmassnahmen gem. ARSIWA geltend gemacht oder die Angelegenheit dem UN-Sicherheitsrat vorlegt werden, der die Vorfälle als Friedensbedrohung oder gem. Art. 39 UN-Charter als Aggression qualifizieren kann.[461] Zudem führt die US-amerikanisch geprägte Lesart der vorliegenden Ansicht nach im Ergebnis zu einer höheren Gewichtung der Notwendig- und Verhältnismässigkeit: Durch eine Ausweitung des Anwendungsbereichs des Selbstverteidigungsrechts auf geringere Gewaltanwendungen, neue Technologien, nichtstaatliche Akteure und/oder antizipatorische Konstellationen würden die Notwendig- und die Verhältnismässigkeit zur *letzten* Beschränkungsmöglichkeit militärischer Gewaltanwendungen des sich verteidigenden Staats.[462] Dies wiederum würde im Grunde Gewaltanwendungen eher begünstigen als beschränken. Es ist fraglich, ob die Verhältnismässig- und Notwendigkeit als letzte Ventile für eine Beschränkung exzessiver Gewalt ausreichend sind, zumal man sich – wie bereits erwähnt – im Bereich der Selbstverteidigung im weiter gefassten Spektrum *militärischer*, *gewaltsamer* Reaktionsmöglichkeiten bewegt.

Eine Ausweitung des Anwendungsbereichs von Art. 51 UN-Charta würde den Radius gewaltsamer Selbstverteidigungsmöglichkeiten erheblich erweitern. Darunter – da vom Anwendungsbereich von Art. 51 UN-Charta grundsätzlich umfasst – würde insb. auch der Radius *kollektiver* militärischer Selbstverteidigung fallen. Kollektive Selbstverteidigung bedeutet, dass nicht nur der verletzte Staat, sondern auch Drittstaaten in die gewaltsamen, militärischen Verteidigungsmassnahmen involviert werden dürfen. Die Würdigung ebendieses Umstandes war gerade auch im Nicaragua-Urteil des IGH massgebend: Durch die Beschränkung von Art. 51 UN-Charta auf schwerwiegende, bewaffnete Angriffe wollte er den Einbezug von Drittstaaten in gewaltsame, militärische Verteidigungshandlungen ausschliessen[463] und dadurch einer Eskalation möglichst entgegenwirken. Verneint man nämlich einen bewaffneten Angriff, dann gibt es kein Recht auf Selbstverteidigung und dadurch auch nicht auf kol-

460 Randelzhofer/Nolte, S. 1402. Anderer Ansicht: Kranz, S. 302.

461 O'Connell, Cyber Security, S. 204 f.; Woltag, S. 177.

462 Siehe dazu nachfolgend die einleitenden Ausführungen zu Kapitel IV.

463 Gray, Use of Force, S. 156.

lektive Selbstverteidigung. Die Notwendig- und Verhältnismässigkeit alleine schliessen eine Konfliktbeteiligung von Drittstaaten nicht aus, sondern können lediglich den Umfang ihrer zulässigen Reaktion einschränken.[464]

Gemäss BANKS/CRIDDLE wird der amerikanische Ansatz die globale Cyberregulierung durch Etablierung von Staatenpraxis und potenziellem Gewohnheitsrecht massgeblich beeinflussen.[465] Daraus folgern sie, dass europäische *conventional restrictivists* sich vermehrt in einen Dialog mit den amerikanischen Experten über das Recht der Gewaltanwendung einbringen sollten, um bei der Auslegung des *ius ad bellum* im Cyberkontext mitwirken zu können – oder in ihren Worten: »*if only to have a voice in the progressive development of customary jus ad bellum*«.[466] Diese Schlussfolgerung geht (vermutlich berechtigt) von einem grossen Einfluss der USA in diesem Prozess der Cyberregulierung aus.[467] Wichtig ist, dass man sich der unterschiedlichen Ansichten bewusst ist und über die Hintergründe der gegenseitigen Argumente spricht, wenn man zu global vertretbaren und nachhaltigen Lösungen kommen soll. Für die Thematik zentral ist zudem, dass voreilige und vereinfachte Schlüsse im Cyberkontext mit Zurückhaltung zu ziehen sind. Die inhaltliche Gleichsetzung von Gewaltanwendung und bewaffnetem Angriff (die nicht weitgehend akzeptiert ist) bspw. fördert im Cyberkontext nämlich Unklarheiten und Graubereiche im Zusammenhang mit der Selbstverteidigung.[468] Diese Unklarheiten sollen mitunter Gegenstand des nachfolgenden Abschnitts sein.

c. Cyberangriffe und Art. 51 UN-Charta

Die vehement diskutierte Frage nach der Auslegung von Art. 51 UN-Charta im Cyberkontext bleibt, wie bereits erwähnt, sowohl innerhalb der Staatengemeinschaft als auch der Lehre umstritten. Es fragt sich mitunter, inwiefern die divergierenden Ansichten des *conventional* und des *customary restrictivism* diese Schlussfolgerungen beeinflussen. Insgesamt besteht ein grundsätzlicher Konsens unter Völkerrechtlern beider Ansätze, dass Reaktionen auf Cyber-

464 Ausführlicher dazu: GRAY, Use of Force, S. 156 f. m.w.V.

465 BANKS/CRIDDLE, S. 93.

466 BANKS/CRIDDLE, S. 93.

467 Ähnlich verweist GRAY auf Autoren, die potenziell jede US-Handlung i.Z.m. Selbstverteidigung als Präzedenzfall behandeln würden, der Gewalt rechtlich neu legitimiert: GRAY, Use of Force, S. 175 m.V. auf AREND/BECK; WEISBURD; D'AMATO. Diese Tendenz sei auch ersichtlich i.Z.m. den extensiven Auslegungen der USA nach 9/11 und dem Syrien Konflikt: GRAY, Use of Force, S. 200 ff.

468 SCHMITT, Grey Zones, S. 15 u.a. m.V.a. TAFT, S. 299 ff.

angriffe den Anforderungen der Charta und weiterer gewohnheitsrechtlicher Prinzipien standalten müssen.[469] Die detaillierte Anwendung dieser Prinzipien ist allerdings noch nicht gänzlich geklärt.[470] Die Debatte um Art. 51 UN-Charta scheint weitgehend zwischen extensiven, Cyberangriffe möglichst in den Anwendungsbereich einbindende, und restriktiven Herangehensweisen polarisiert.[471] Wie vorangehend ersichtlich wird, ist der genaue Anwendungsbereich des Selbstverteidigungsrechts an sich bereits umstritten, womit im Hinblick auf die Erfassung neuer Technologien weitere Schwierigkeiten hinzukommen. Cyberangriffe mit ihren eigenen Charakteristika machen die Thematik besonders komplex, was auch die Etablierung eines internationalen Konsenses zur Auslegung des völkerrechtlichen Selbstverteidigungsrechts erschwert.[472] *Bis dato* wurde innerhalb der Staatengemeinschaft offiziell noch kein bewaffneter Angriff durch einen Cyberangriff bejaht.[473] Dennoch scheint grundsätzlich Einigkeit zu bestehen, dass ein Cyberangriff das Potenzial hat, diese »Schwelle« zu erreichen.[474] Ein solches Szenario erscheint angesichts der technischen Möglichkeiten, breite Zerstörungen anzurichten, durchaus im Bereich des Denkbaren.[475]

Von einer Mehrheit wird die Ansicht vertreten, dass Cyberangriffe das Recht auf Selbstverteidigung gem. Art. 51 UN-Charta auslösen können sollen, wenn die Effekte des Angriffs denjenigen herkömmlicher bewaffneter Angriffe

469 Banks/Criddle umschreiben diese Entwicklungen i.Z.m. der Regulierung von Cyberangriffen als eine hybride Form des »*customary restrictivism*«: Banks/Criddle, S. 87. Das Tallinn Manual ist dabei im Hinblick auf die kulturell divergierenden Haltungen besonders interessant, da es von Experten aus Europa sowie den USA verfasst wurde. Es illustriert z.B., in welchen Punkten man sich einigen konnte.

470 Vgl. Roguski, S. 2.

471 Vgl. Harrison Dinniss, S. 113; Banks/Criddle, S. 67 ff.

472 Harrison Dinniss, S. 75; Banks/Criddle, S. 88.

473 Gray, Use of Force, S. 135 m.V. auf Tallinn Manual 1.0, S. 57 R13 C13. Ähnlich in Tallinn Manual 2.0, S. 384 R82 C16; Woltag, S. 178 m.w.V. Siehe allerdings jüngere Entwicklungen in Israel wie vorangehend unter Fn. 133 erwähnt.

474 Heintschel von Heinegg, Informationskrieg, S.141; Roscini, Cyber Operations, S. 115; Woltag, S. 178, S. 196. Dazu auch: Randelzhofer/Nolte, S. 1419 f. Implizit auch in den UN GGE Konsensberichten und im finalen OEWG Bericht vom 10.03.2021, wonach die Selbstverteidigung grundsätzlich im Cyber Kontext anwendbar sein soll.

475 Gemäss Dunn Cavelty handelt es sich *bis dato* in der Praxis jedoch um hypothetische Annahmen, da Cyberangriffe durch Staaten klar und bewusst unterhalb der Gewaltverbotsschwelle eingesetzt werden, siehe Dunn Cavelty, ETH Zukunftsblog vom 15.06.2018.

gleichkommen.[476] Schwierigkeiten bereitet zunächst allerdings, dass Cyberangriffe i.d.R. keine mit herkömmlichen Waffen vergleichbaren Effekte erzielen,[477] indem sie primär auf ein Computersystem wirken und, wie bereits unter III.A.3. beschrieben, je nachdem, was das Computersystem kontrolliert, ganz unterschiedliche, und oft jeweils neue Formen von Schäden auslösen. Aus einer Funktionsbeeinträchtigung resultierende Schäden sind somit jeweils Folgeeffekte, die bei DDoS-Angriffen durch die Blockierung von Systemsfunktionen und bei trojanischen Pferden, Viren und Würmern durch deren Manipulation erfolgen. Die möglichen Effekte von Cyberangriffen sind demgemäss weder konsequent gleichartig[478] noch unmittelbar.[479] Es muss somit jeweils eine Einzelfallbetrachtung von Cyberangriffen und deren Konsequenzen erfolgen,[480] um diese adäquat qualifizieren zu können.

Wie vorangehend erläutert, setzt die Zulässigkeit gewaltsamer Selbstverteidigung gem. Art. 51 UN-Charta Verletzte, Tote und/oder breite physische Zerstörung voraus. Es handelt sich traditionellerweise um bewaffnete, physische und staatsübergreifende Gewalt.[481] Im Hinblick auf die völkerrechtliche Qualifizierung von Cyberangriffen hat sich weitgehend etabliert, analog auf die Intensität der Effekte (»*scale and effects*«) abzustellen.[482] Dabei besteht allerdings Uneinigkeit, welches *Mass* an Zerstörung, Schäden, Verletzten oder Toten erforderlich ist, um diese Schwelle zu erreichen.[483] Strittig bleibt zudem, *welche*

476 Tallinn Manual 1.0, S. 54 R13 C3 f.; Tallinn Manual 2.0, S. 330 R69. Dazu auch: Diggelmann/Hadorn, S. 263. Gemäss Banks/Criddle, S. 89 f. vertritt ein Teil der amerikanischen Lehre einen ähnlich effektbasierten Ansatz, gemäss dem die Schädigungen denjenigen eines kinetischen Angriffs gleichkommen müssen. Sie verweisen dabei u.a. auf Schmitt, Jensen und Watts. Sich ebenfalls auf einen effektbasierten Ansatz stützend: Hinkle, S. 11.

477 Harrison Dinniss, S. 75.

478 Schmitt, Computer Network Attack, S. 912.

479 Diggelmann/Hadorn, S. 263.

480 Harrison Dinniss, S. 80.

481 Banks/Criddle, S. 88; Harrison Dinniss, S. 75.

482 So auch das Tallinn Manual 2.0, S. 339 R71. Dazu: Banks/Criddle, S. 88; Diggelmann/Hadorn, S. 263.

483 Banks/Criddle, S. 88 f.; Schmitt, Grey Zones, S. 13; Tallinn Manual 1.0, S. 56 R13 C7. Tallinn Manual 2.0, S. 341, R71 C9. Im Tallinn Manual 2.0 wird in R71 C10 das Beispiel von Stuxnet angeführt, um die Uneinigkeit der Schwelle zu illustrieren (einige sahen Stuxnet als bewaffneten Angriff, die anderen nur als Gewaltanwendung).

Effekte[484] im Einzelnen gleichwertig sind mit jenen herkömmlicher Angriffe: So wird nicht klar zwischen physischen, nicht-physischen, mittelbaren und unmittelbaren Effekten unterschieden[485] – Aspekte, deren Klärung sich, wie bereits erwähnt, gerade im Cyberkontext aufdrängt. Mitunter bleibt es umstritten, ob das Selbstverteidigungsrecht auf Cyberangriffe Anwendung findet, die, wie am Beispiel Estlands, zwar extensive ökonomische Folgen, doch keine physischen Schäden, Verletzte oder Tote nach sich ziehen.[486] Einige sind der Ansicht, dass es physische Zerstörung oder Verletzungen von Personen erfordert, um einen bewaffneten Angriff zu bejahen.[487] Andere richten den Fokus auf die Auswirkungen auf das nationale Interesse eines Staates, unabhängig davon, ob diese physischer Natur sind.[488] Letzterer Argumentation zufolge könnte auch ein nicht-physisch wirkender Cyberangriff u.U. eine gewaltsame Selbsthilfehandlung rechtfertigen, wenn er einen Staat massiv schädigt. Als prominentes Beispiel wird oft das umstrittene Szenario eines Angriffs auf eine Börse angeführt:[489] Gemäss einem Teil der Experten im Tallinn Manual sollen solche nicht-physischen, ökonomischen – im Tallinn Manual als »katastrophale Effekte« umschriebenen – Schäden reichen, um einen bewaffneten Angriff zu konstituieren. Einige Experten sind gar der Ansicht, dass Cyberangriffe gegen staatliche kritische Infrastrukturen generell als bewaffnete Angriffe gelten sollten, auch wenn sie keine physische Effekte auslösen.[490] Der vorliegend vertretenen Ansicht nach setzt Art. 51 UN-Charta allerdings, wie im traditionellen Kontext auch, *physische* Schäden bzw. Tote und/oder breite Zerstörung

484 Im Tallinn Manual wird diese Unklarheit am Beispiel eines Angriffes auf eine Kläranlage angeführt, deren Beeinträchtigung indirekt eine Trinkwasserverschmutzung und Krankheiten auslösen kann, die voraussehbar sind und deshalb berücksichtigt werden müssen, siehe Tallinn Manual 2.0, S. 343 R71 C13.

485 Diggelmann/Hadorn, S. 263 m.V.a. Tallinn Manual 2.0, S. 330 R69.

486 Banks/Criddle, S. 89.

487 Tallinn Manual 2.0, S. 342 R71 C12.

488 Tallinn Manual 2.0, S. 342 R71 C12 m.V.a. Advisory Council on International Affairs 2011, S. 21, der eine implizite Bejahung der Niederlande enthalte, dass es keine physische Destruktion brauche. Auch erwähnt in: Schmitt, Just Security vom 10.06.2019. In UN Doc. A/76/136 (2021), S. 64 hat die Niederlande allerdings festgehalten, dass es zu dieser Frage keinen internationalen Konsens gäbe.

489 Tallinn Manual 1.0, S. 56 R13 C9; Tallinn Manual 2.0, S. 343, R71 C12. Ähnlich: Kilovaty, Economic Cyber Warfare, S. 210 ff.

490 Tallinn Manual 1.0, S. 56 R13 C9; Tallinn Manual 2.0, S. 343, R71 C12; Jensen, Critical National Infrastructure, S. 221 ff.; Sharp, S. 129 f. Es handelt sich dabei in der Lehre jedoch um eine Mindermeinung. Die Mehrheit der Autoren orientiert sich an physischen Schäden: Banks/Criddle, S. 88; Harrison Dinniss, S. 75.

voraus.[491] Die Ansätze, dass für die Bejahung eines bewaffneten Angriffs von physischen Schäden abgesehen werden können soll, entsprechen nicht dem vorliegenden Verständnis der historischen Auslegung von Art. 51 UN-Charta. Die für die Selbstverteidigung relevanten physischen Schäden und Zerstörungen sind im Cyberkontext nur eine – meist nicht vor dem Eintritt der Schädigung absehbare[492] – mögliche Folge von Cyberangriffen. Will man ökonomische oder politische Effekte für die Bejahung eines bewaffneten Angriffes als ausreichend gelten lassen, muss man sich zudem bewusst sein, dass dadurch nicht unproblematisches Neuland betreten würde: Der Sicherheitsrat hat ökonomische Schädigungen noch nie als Friedensbedrohung kategorisiert, die Zwangsmassnahmen gem. Kapitel VII der UN-Charta erlauben würden.[493] Da Entwicklungen zeigen, dass Cyberangriffe mit weitreichenden ökonomischen Schäden und politischen Einflussnahmen tatsächlich und zunehmend erfolgen,[494] stellt die Debatte, ob ökonomische und politische Gewalt wirklich ausreichend sein soll, um eine gewaltsame Reaktion zu rechtfertigen, einen erheblichen Brennpunkt dar. Die Komplexität der Problematik wird zusätzlich erhöht, indem vage und unklare Formulierungen wie »massive« oder »katastrophale ökonomische Schäden« auch im Hinblick auf das erforderliche *Mass* extrem missbrauchsanfällig sind.[495] Diese können durch Staaten und deren Entscheidungsträger unterschiedlich ausgelegt werden, was wiederum zu Unberechenbarkeit und Unvoraussehbarkeit führt.[496]

Die vorangehenden Ansichten würden in qualitativer Hinsicht eine heikle Ausweitung des Rechts auf Selbstverteidigung bedeuten. Bejaht man die Möglichkeit, dass nicht-physisch wirkende Angriffe unter den Anwendungsbereich von Art. 51 UN-Charta subsumiert werden können, bewegt man sich sehr nah dem in den USA verbreiteten Ansatz, nicht zwischen den Konzepten des bewaffneten Angriffs gem. Art. 51 UN-Charta und des Gewaltverbots gem.

491 Im Ergebnis ebenso: Harrison Dinniss, S. 113; Woltag, S. 179. Ähnlich: Diggelmann/Hadorn, S. 264 f.

492 Dazu nachfolgend unter IV.A.2.b) ausführlicher.

493 Diggelmann/Hadorn, S. 264.

494 Bereits 2010 wurden bspw. die Londoner Börse, 2012 die Börse von Tel Aviv und im August 2020 die Neuseeländer Börse zeitweise lahmgelegt. Siehe dazu: Harrison Dinniss, S. 41; Farrer, The Guardian vom 26.08.2020; Knell, BBC News vom 16.01.2012; Radziwill, S. 50, S. 72. Mit weiteren Beispielen u.a.: Dewar, Contextualizing, S. 10.

495 Diggelmann, NZZ vom 30.05.2013.

496 Vgl. Kilovaty, Jus Ad Bellum, S. 112. Eingehend zu (Un-)Voraussehbarkeit und politischen Strategien: Schelling, S. 1 ff.

Art. 2(4) UN-Charta zu unterscheiden.[497] Lockert man die Kriterien der Selbstverteidigung, um diese neue Form von »Cybergewalt« zu erfassen, muss man sich bewusst sein, dass damit ein erheblicher und missbrauchsanfälliger Ermessensspielraum geschaffen wird, der sich zunehmend von der traditionellen Anwendung von Art. 51 UN-Charta entfernt. Da gegenwärtig noch keine substanzielle Staatspraxis dazu besteht, kann dies in vielen Fällen zu Graubereichen führen.[498] Diese Graubereiche können – je nach Auslegung – zu fundamentalen Änderungen der Anwendung von Art. 51 UN-Charta in künftigen Konflikten führen.

Des Weiteren besteht Uneinigkeit darüber, ob durch nichtstaatliche Akteure ausgeübte Cyberangriffe rechtlich gesehen einen bewaffneten Angriff darstellen können.[499] Dies wurde durch verschiedene Staaten[500] sowie die Mehrheit der Experten im Tallinn Manual[501] bejaht, bleibt jedoch sehr umstritten.[502] Wenn durch Private lancierte Cyberangriffe als bewaffnete Angriffe i.S.v. Art. 51 UN-Charta gelten sollen, dann würde diese Würdigung – wenn überhaupt – anhand der jüngeren, jedoch höchst kontroversen *safe haven*-Doktrin erfolgen.[503] Dieser zufolge kann ein Staat für die Angriffe Privater verantwortlich werden, wenn er nicht gewillt oder nicht in der Lage ist, die Angriffe zu verhindern.[504] Angesichts der weitreichenden Anonymität, dem hohen Anteil privater Akteure, dem (automatisierten) Einbinden unbeteiligter Drittpersonen bei Cyberangriffen sowie dem zunehmenden Aufkommen sog. hybrider

497 Diggelmann/Hadorn gehen davon aus, dass die Ansichten der Expertengruppe allenfalls dadurch beeinflusst sein könnte, dass bei der Würdigung von Art. 2(4) UN-Charta – obschon »Gewalt« grundsätzlich immer militärisch verstanden wurde – ökonomische und politische Schädigungen in der Praxis eine Rolle spielen können: Diggelmann/Hadorn, S. 264 m.V.a. Randelzhofer/Dörr, S. 200 ff.

498 Kilovaty, Jus Ad Bellum, S. 112; Schmitt, Computer Network Attack, S. 909.

499 Schmitt, Grey Zones, S. 14. Eingehender dazu: Bussolati, S. 102 ff., S. 121 ff. Ferner auch: Blank Laurie, Non-State Actors, S. 406 ff.

500 Siehe z.B. Deutschland in UN GGE 2021 in UN Doc. A/76/136 (2021), S. 43. Ähnlich anerkennt Frankreich, dass die Staatenpraxis tendenziell in die Richtung geht, Handlungen nichtstaatlicher Akteure von Art. 51 UN-Charta zu erfassen: French Ministry of the Armies, International Law Applied to Operations in Cyberspace, September 2019, S. 8 f. Dazu auch: Roguski, S. 22.

501 Tallinn Manual 2.0, S. 345 R71 C18.

502 Lahmann, S. 62; Tallinn Manual 2.0, S. 345 R 71 C18.

503 Diggelmann/Hadorn, S. 271 f. m.V.

504 Dazu, dass eine grosse Mehrheit der Staatengemeinschaft diese Doktrin nicht akzeptiert: Corten, Unwilling or Unable, S. 777 ff. Ferner auch: Tibori-Szabó, S. 73 ff.; Ohlin, Unwilling and Unable, S. 113 ff., insb. S. 117.

Kriege[505] ist es gerade im Cyberkontext jedoch zusätzlich heikel, das Verhalten Privater als bewaffnete Angriffe zu qualifizieren. Cyberangriffe gehen oftmals von vielen Computern gleichzeitig aus, die sich unter Umständen innerhalb verschiedener Staaten befinden. Dies macht die Zurechnung an einen Staat unter der *safe haven*-Doktrin sowie Fragen der Verhältnismässigkeit unübersichtlich und komplex.[506] Sowohl bei DDoS-Angriffen als auch bei Angriffen durch Schadprogramme wie Würmer, Viren oder trojanische Pferde stellt sich weiterhin die zentrale Schwierigkeit, den Urheber eines Cyberangriffs zurückzuverfolgen.[507] Im Zweifel – ohne Gegenbeweis – kann folglich nicht davon ausgegangen werden, dass ein Staat involviert ist oder, wenn es sich um nichtstaatliche Akteure handelt, kann kaum eruiert werden, von welchem Territorium aus diese handeln. Oft könnte also nicht mit Sicherheit festgestellt werden, gegen welchen Staat sich eine Selbstverteidigung überhaupt richten müsste.[508] Hinzu kommt im Cyberkontext die Schwierigkeit für einen Staat sicherzustellen, dass keine schädigende Cyberangriffe vom eigenen Territorium aus lanciert werden, und es stellt sich die Frage, ab wann er konkret als nicht gewillt und in der Lage angesehen wird, solche zu unterbinden.[509] Mit anderen Worten sind die Anforderungen (eines Nachweises) für eine Zurechnung im Rahmen der *safe haven*-Doktrin sehr unklar.[510] Somit würde die Möglichkeit, private Hacker an einen Staat im Rahmen von Art. 51 UN-Charta zurechnen zu können, zusätzliche Graubereiche schaffen. Nach vorliegend vertretener Meinung ist die Erweiterung des Anwendungsbereichs auf privates Verhalten daher sehr kritisch zu betrachten – wenn nicht abzuweisen. Gerade im Hinblick auf die unübersichtlichen und nicht klar definierbaren Akteursgruppen im Cyberraum würde der potenzielle Radius von Selbstverteidigungshandlun-

505 Diggelmann, Völkerrecht, S. 92. Die Diskussion neuer, »hybrider« Kriege betrifft vorüberwiegend die zunehmende Verlagerung auf parastaatliche und teilweise sogar private Akteure sowie die gewandelten Finanzierungsformen. Neben der Entstaatlichung ist auch eine »Asymmetrisierung kriegerischer Gewalt« sowie eine Autonomisierung derselben festzustellen: Münkler, S. 11 ff.

506 Vgl. Harrisson Dinniss, S. 95 ff. Sie ist aufgrund der Verhältnismässigkeit kritisch dazu eingestellt, das Verhalten nichtstaatlicher Akteure im Cyberkontext in Art. 51 UN-Charta miteinzubeziehen.

507 Harrison Dinniss, S. 76, S. 99 ff.

508 Diggelmann/Hadorn, S. 265.

509 Eingehend zu den Schwierigkeiten i.Z.m. dem »Unable or Unwilling«-Standard: Starski, S. 456 ff.

510 Banks/Criddle, S. 75 ff.; Starski, S. 456 ff. m.w.V. Siehe auch Schmitt, U.S. Security Strategies, S. 738, S. 762, (zum unklaren Beweismass) S. 757. Ferner: Waxman, States that *Might* Have Weapons of Mass Destruction, S. 1 ff.

gen (zu) beträchtlich ausgeweitet. Der Tendenz nach würde eine solche Ausweitung allerdings in die bereits erwähnten, jüngeren Entwicklungen einer zunehmenden völkerrechtlichen Erfassung hybrider, vom Staat zunehmend losgelöster Kriege passen.[511] Eine der grössten Herausforderungen in diesem Zusammengang wird für die Staatengemeinschaft bleiben, dass diese diffuse Form hybrider Kriege neben ihrer Unübersichtlichkeit typischerweise einen hohen Anteil an zivilen Opfern sowie die auffällig geringe Beachtung der Regeln des humanitären Völkerrechts zur Folge haben.[512] Die gegenwärtige Tendenz, dass man das Recht auf Selbstverteidigung nicht nur explizit bejaht, sondern tendenziell auch ausweitet, könnte folglich weitgehende praktische Konsequenzen nach sich ziehen.

Des Weiteren stellt auch die Frage nach dem erforderlichen Vorsatz im Rahmen von Art. 51 UN-Charta im Cyberkontext eine wesentliche Herausforderung dar. Einige Autoren sind der Ansicht, dass – auch wenn ein Cyberangriff zu relevanten Schädigungen führen sollte – das Recht auf Selbstverteidigung nur dann ausgelöst werden soll, wenn die Konsequenzen für den Angreifer zumindest voraussehbar waren. Dazu müsste ein Zusammenhang zwischen dem Vorsatz des Angreifers und der Schädigung bestehen.[513] Demzufolge müsste die Schädigung eine direkte Konsequenz des Angriffs sein und eben nicht ein unvorhergesehener, versehentlicher Nebeneffekt.[514] Diese Folgerung lehnt sich ähnlich der Argumentation des IGH im Ölplattformen-Urteil an den Gedanken an, einer Eskalation im Falle unbeabsichtiger Beschädigungen möglichst entgegenzuwirken.[515] Die Experten des Tallinn Manuals konnten sich in diesem Punkt nicht einigen: Während ein Teil der Experten zumindest einen gewissen Grad an Vorsatz voraussetzte, sah die Mehrheit der Experten das *scale and effects*-Erfordernis als einizige Bewertungsgrundlage für die Qualifizierung eines bewaffneten Angriffs.[516] Gerade im Cyberkontext würde ein gänzliches Absehen von einem Vorsatz angesichts des realistischen Szenarios von Kollateralschäden die Schwelle zu einem bewaffneten Angriff in vielen Fällen deutlich senken. Lahmann führt in diesem Zusammenhang das Beispiel der Weiterverbreitung von Stuxnet über das iranische Atomkraftwerk in Natanz

511 Zu diesen Entwicklungen u.a.: Diggelmann, Völkerrecht, S. 92; Münkler, S. 7 ff.

512 Diggelmann, Völkerrecht, S. 93 f.

513 Silver, S. 90 ff. Ähnlich schlägt Petkis ein Verständnis vor, das die Absicht (»*purpose*«) eines Angriffs mitwürdigen soll: Petkis, Rethink Proportionality, S. 1446 ff.

514 Lahmann, S. 60. Ähnlich erfordern Randelzhofer/Nolte, S. 1419 »substanzielle, unmittelbare destruktive Effekte«. Ähnlich auch: Silver, S. 90.

515 Lahmann, S. 60.

516 Tallinn Manual 2.0, S. 339 R 71 C14. Dazu: Lahmann, S. 60.

hinaus an: Nehmen wir an, die unkontrollierte Weiterverbreitung dieser Schadenssoftware hätte einen Drittstaat in für Art. 51 UN-Charta relevanter Weise beschädigt. Würde man der letzteren Interpretation folgen und keinen Vorsatz voraussetzen, würde der Radius des Anwendungsbereichs von Art. 51 UN-Charta auf eine Vielzahl weiterer Staaten erweitert, die dadurch zu Konfliktparteien würden.[517] Das dadurch zusätzlich implizierte Eskalationspotenzial stellt der hier vertretenen Ansicht nach in der Gesamtbetrachtung ein weiteres Argument dafür dar, Art. 51 UN-Charta zurückhaltend zu bejahen und zumindest ein gewisses *momentum* an Absicht vorauszusetzen. Die vorliegende Einschätzung ist es allerdings, dass gerade im Cyberkontext *unbeabsichtigte Folgeschäden* nicht unbeschränkt in Kauf genommen werden können sollen. Vielmehr werfen absichtlich freigelassene Schadprogramme die Frage nach den erforderlichen Sorgfaltspflichten eines Staates auf. Diese Frage erfordert inbesondere angesichts des Wissens um die realistische Möglichkeit und Absehbarkeit von schwerwiegenden Kollateralschäden eine nähere Betrachtung. Dies soll jedoch im Einzelnen Gegenstand anderweitiger Analysen sein.

Das Bedürfnis gewisser Staaten, am Recht auf Selbstverteidigung im Cyberkontext festzuhalten (und damit gegebenenfalls Ausweitungen und Abänderungen in Kauf zu nehmen oder gar anzustreben), dauert an.[518] Angesichts dessen muss man offen über die mit einer solchen »Anpassung« des Selbstverteidigungsrechts verbundenen Konsequenzen im Cyberkontext sprechen. In Erinnerung zu rufen ist dabei – und dies nochmals in aller Deutlichkeit –, dass es im Kontext der UN-Charta grundsätzlich *kein* Recht auf Krieg gibt.[519] Angesichts dessen sowie der beschriebenen Schwierigkeiten, Cyberangriffe technisch und völkerrechtlich klar zu erfassen, wird vorliegend für eine restriktive Auslegung der Kriterien von Art. 51 UN-Charta plädiert. Das heisst, dass man die Zurechnung an private Akteure (wenn überhaupt) nur restriktiv bejahen soll, dass gravierende physische Zerstörungen und/oder Tote gegeben

517 Lahmann, S. 60.

518 Siehe u.a. Estland, die Niederlande und die USA in UN Doc. A/76/136 (2021), S. 30, S. 64, S. 137. Die NATO hat die Verteidigung im Cyberspace zu einem Teil ihrer Hauptaufgaben kollektiver Selbstverteidigung erklärt. Die Entscheidung, wann ein Cyberangriff zur kollektiven Selbstverteidigung führt, solle jeweils von Fall zu Fall gefällt werden. Siehe unter NATO, Cyber Defence, abrufbar unter: <https://www.nato.int/cps/en/natohq/topics_78170.htm> (zuletzt besucht: März 2023).

519 Diggelmann, NZZ vom 29.03.2018. Eingehend dazu: Hathaway/Shapiro, The Internationalist; Kress, S. 603.

sein müssen und immerhin ein gewisser (Eventual-)Vorsatz zu den betreffenden Schädigungen bestehen muss, damit sich ein Sachverhalt überhaupt im Anwendungsbereich von Art. 51 UN-Charta bewegt.

2. Staatenverantwortlichkeit: Normverletzung durch Cyberangriffe?

Im Rahmen der Staatenverantwortlichkeit ist ein Staat gem. Art. 1 und 2 ARSIWA für ihm zurechenbare Völkerrechtsverstösse durch Handeln oder Unterlassen grundsätzlich verantwortlich.[520] Vorausgesetzt sind für die Verantwortlichkeit einerseits die *Verletzung* einer völkerrechtlichen Norm und andererseits die *Zurechenbarkeit* derselben an den Staat.[521] Der Verstoss muss vom verletzten Staat bewiesen werden.[522] Als Völkerrechtsverstoss gelten mitunter die Verletzung des Gewalt- und Interventionsverbots.[523] Darüber hinaus stellen sich im Rahmen der Staatenverantwortlichkeit, angesichts der wachsenden Möglichkeit transnationaler Schädigungen, zunehmende Fragen völkerrechtlicher Sorgfaltspflichten (sog. Due Diligence). Die Staatenverantwortlichkeit betrifft dabei all jene (potenziell durch Cyberangriffe ausgelöste) Völkerrechtsverletzungen, die sich ausserhalb des Anwendungsbereichs von Art. 51 UN-Charta befinden.[524] Das heisst, sie sind dort von Relevanz, wo die *ius ad bellum*-Debatte ihre Grenze findet.[525] Da ein bewaffneter Angriff gem. Art. 51 UN-Charta im Cyberkontext nach vorliegend vertretener Meinung sehr restriktiv anzunehmen ist, könnte dies potenziell die grosse Mehrheit von Schädigungen durch Cyberangriffe betreffen.[526] Gemäss dieser Einschätzung hat die Staatenverantwortung somit das Potenzial, eine zentrale Rolle in der Regulierung von Reaktionsmöglichkeiten bei Cyberangriffen zu erhalten.[527]

---

520 Dazu eingehend: Crawford, State Responsibility, S. 93 ff.; Crawford James, Brownlie's Principles, S. 526 ff.; Crawford/Olleson, S. 416; Dahm/Delbrück/Wolfrum, Bd. I/3, S. 864 ff.; Schulze, S. 51; Woltag, S. 86. Dieser Grundsatz der Staatenverantwortlichkeit wurde durch den IGH in verschiedenen Fällen bestätigt. Bereits der StIGH hat diesen Grundsatz im Chorzów-Fall festgehalten. Siehe dazu im Cyberkontext auch: Schmitt, Countermeasures Response Option, S. 700; Tallinn Manual 2.0, S. 84 R14.

521 Crawford/Olleson, S. 415 ff.; Schulze, S. 51.

522 Krieger, S. 15; Woltag, S. 87.

523 Vgl. Tallinn Manual 2.0, S. 85.

524 Lotrionte, S. 75.

525 Hinkle, S. 12.

526 Vgl. Hinkle, S. 12.

527 Ähnlich: Hinkle, S. 12; (i.Z.m. der staatlichen Verantwortlichkeit für privates Verhalten) Sklerov, S. 44 ff.

In diesem Kapitel sollen mögliche Konstellationen völkerrechtlicher Normverletzungen – und zwar des Interventionsverbots sowie völkerrechtlicher Sorgfaltspflichten – analysiert werden. Wie vorangehend beschrieben, folgt diese Dissertation dem Ansatz, strikt zwischen Art 2(4) UN-Charta und dem eng anzunehmenden Ausnahmefall von Art. 51 UN-Charta zu unterscheiden. Eine Verletzung des Gewaltverbots gem. Art. 2(4) UN-Charta eröffnet der vorliegenden Lesart zufolge somit denselben rechtlichen Rahmen *nicht-militärischer* Gegenmassnahmen gem. ARSIWA[528] wie eine Verletzung des Interventionsverbots oder völkerrechtlicher Sorgfaltspflichten. Daher soll der Anwendungsbereich von Art. 2(4) UN-Charta vorliegend nicht selbständig aufgegriffen werden. Indem das Interventionsverbot gewissermassen als Auffangtatbestand des Gewaltverbots[529] verstanden werden kann, erübrigt sich für die vorligende Analyse die Diskussion, ob ökonomische und politische Gewalt unter das Gewaltverbot gem. Art. 2(4) UN-Charta subsumiert werden sollen[530] bzw. soll eine dahingehende Diskussion Gegenstand anderweitiger Analysen sein. Wichtig ist für die vorliegende Abhandlung vielmehr, wie bereits erwähnt, dass die Unterscheidung eines bewaffneten Angriffs gem. Art. 51 UN-Charta und Art. 2(4) UN-Charta zu strikt zu differenzierenden Rechtsfolgen sowie zu unterschiedlichen Zurechnungs- und Verhältnismässigkeitsfragen führt. Bei einer Verletzung von Sorgfaltspflichten, des Gewalt- oder Interventionsverbots und einer erfolgreichen rechtlichen Zurechnung dieser Verstosse gem. Art. 1 und 2 ARSIWA hat der verletzte Staat grundsätzlich die Möglichkeit auf verhältnismässige Gegenmassnahmen sowie auf Retorsionshandlungen (und kein Recht auf Selbstverteidigung). Die Aspekte dieser Rechtsfolgen sollen Gegenstand des darauffolgenden Kapitels IV. sein.

a. Interventionsverbot

Das Interventionsverbot gilt als Korrelat der souveränen Gleichheit sowie der territorialen und politischen Unabhängigkeit von Staaten innerhalb der internationalen Gemeinschaft.[531] Es kann aus Art. 2(1), (4) sowie Art. 2(7) UN-Charta abgeleitet werden und wird teilweise als Völkergewohnheitsrecht betrach-

528 IGH, Nicaragua-Urteil, §249; Roscini, Cyber Operations, S. 104; Jensen, Cyber Deterrence, S. 797.

529 Vgl. Schulze, S. 114.

530 Zu einer Zusammenfassung des Gewaltbegriffs der UN-Charta u.a.: Dörr, MPEPIL 2019, §11 ff.

531 IGH, Nicaragua-Urteil, §202, §251. Für den Cyberkontext: Schmitt, Grey Zones, S. 4.

tet.[532] So zählt auch der IGH das Interventionsverbot zu den Kernelementen des völkerrechtlichen Gewohnheitsrechts.[533] Das Prinzip verbietet den Staaten zwangsmässiges oder zwangsähnliches Einwirken auf die inneren oder äusseren Angelegenheiten eines anderen Staates.[534] Jeder Staat ist also dazu verpflichtet, die personelle, territoriale und politische Integrität anderer Staaten zu respektieren.[535] Indem mittels Cyberangriffen mittlerweile zunehmend in andere Staaten eingegriffen werden kann wie z.B. mittels Wahlkampfmanipulationen[536] oder ökonomischer Schädigungen[537] und man sich, wie vorangehend aufgezeigt, in den seltensten Fällen innerhalb des Anwendungsbereichs von Art. 51 UN-Charta bewegt, drängt sich die Klärung des Interventionsverbots im Cyberkontext auf.[538] Die rechtliche Würdigung von Cyberangriffen im Lichte des Interventionsverbots ist somit ein Thema von zunehmender Bedeutung.[539]

i. Grundidee des Interventionsverbots

Zur Grundidee des Grundsatzes gegenseitiger Nichteinmischung in innere Angelegenheiten zählt historisch gesehen das Ziel der Konflikteindämmung. Die Entstehung des Prinzips muss im Zusammenhang mit den Konfessionskriegen im Europa des 16. und 17. Jahrhunderts verstanden werden: Das aus der Souveränität abgeleitete Interventiosverbot sollte damals den konfessionell motivierten Interventionen Grenzen setzen und trug dadurch wesentlich zum Frieden bei.[540] Durch die gegenseitige Achtung der Souveränität sollten kollidierende Zugriffsmöglichkeiten vermieden und dadurch Konflikte verhindert

532 Nolte, Article 2(7), S. 284; Watts, S. 253 f.

533 IGH, Nicaragua-Urteil, §202; IGH, Kongo-Urteil, §202; IGH, Korfu Kanal-Urteil, S. 35. Der IGH hat im Hinblick auf die herrschende Ansicht und die Staatenpraxis massgebend zur Klärung des gewohnheitsrechltichen Status beibetragen: Watts, S. 250 ff. m.w.V. Zum Interventionsverbot ferner: Crawford, Brownlie's Principles, S. 431; Shaw, u.a. S. 194.

534 IGH, Nicaragua-Urteil, §205; Diggelmann/Hadorn, S. 8; Schmitt, Grey Zones, S. 7; Tallinn Manual 2.0, S. 312, R66.

535 Siehe u.a. die Präambel der Declaration on Friendly Relations (UN Doc. A/RES/2625 (XXV); IGH, Nicaragua-Urteil, §202.

536 Sanger/Shane, New York Times vom 09.12.2016; Tikk/Hovhannisyan/Kerttunen/Salminen, S. 42 f.

537 Dewar, Contextualizing, S. 10.

538 Watts, S. 270.

539 Watts, S. 249 f.

540 Diggelmann, Völkerrecht, S. 15.

oder abgekühlt werden.[541] Das Prinzip birgt somit ein wichtiges Deeskalationspotenzial – nicht nur im Hinblick auf die nicht-militärischen Reaktionsmöglichkeiten, sondern bereits im Vorfeld. Es kann bei seiner Beachtung in massgeblicher Weise Stabilität im internationalen Umfeld fördern.[542] Die Bedeutung des Interventionsverbots ist somit gerade im dezentralen System gleicher und souveräner Staaten nicht zu unterschätzen. Das Prinzip hat das Potenzial dazu beizutragen, dass bei seiner Klärung bzw. der Vergegenwärtigung und Bestätigung seiner Geltung im internationalen (Cyber-)Umfeld die Respektierung der Souveränität anderer Staaten und dadurch Frieden und Stabilität gefördert werden kann.[543]

Trotz seiner Wichtigkeit wurde das Interventionsverbot in der Praxis durch Staaten kontinuierlich verletzt und blieb beträchtlich ambivalent – es wurde von einigen als Rechtsprinzip gar in Frage gestellt.[544] Der genaue Anwendungsbereich des Interventionsverbots bleibt weitgehend umstritten und wird oft im Zusammenhang mit spezifischen Fallgruppen diskutiert.[545] Einigen Ansichten zufolge kann das Prinzip nicht mit neuen, territoriumsübergreifenden Phänomenen mithalten.[546] Globale, transnationale Phänomene wie der Cyberraum fordern das territorial ausgerichtete Nationalstaatenkonzept und das daran anknüpfende Interventionsverbot unverkennbar heraus. Das moderne Völkerrecht beruht allerdings bis heute auf dem Denken in Kategorien gleicher, souveräner Staaten.[547] Und solange dies der Fall sein wird, wird das Interventionsverbot zentral bleiben.

Eine Verletzung des Interventionsverbots setzt grundsätzlich voraus, dass ein Staat in zwangsähnlicher Weise in die inneren oder äusseren Angelegenheiten (*domaine réservé*) eines anderen Staates eingreift und dies nicht gerechtfertigt ist.[548] Staaten sind sich weder über die erforderliche Intensität des Zwangs einig, noch darüber, was im Einzelnen die geschützten inneren und äusseren Angelegenheiten eines Staates sind.[549] Dies führt zu Graubereichen bei der

541 Diggelmann, Völkerrecht, S. 199.

542 Ausführlicher zur Bedeutung der Souveränität für die internationale Stabilität: Crawford, Sovereignty, S. 117 ff.

543 Watts, S. 270.

544 Dazu: Nolte, Article 2(7), S. 282, S. 310 m.w.V.; Watts, S. 249.

545 Watts, S. 270; Woltag, S. 112 u.a. m.V.a. Kunig, MPEPIL 2008, §1. Dazu auch: Schulze, S. 105 m.w.V.

546 Woltag, S. 112 m.V.a. Chesterman, MPEPIL 2009, §23.

547 Diggelmann, Völkerrecht, S. 28. Ähnlich: Alvarez, S. 26.

548 Schmitt, Grey Zones, S. 7; Schröder, S. 706. Zu Rechtfertigungsgründen: Watts, S. 269 f.

549 Watts, S. 270.

Anwendung des Prinzips.[550] Im Nicaragua-Urteil wurde der *domaine réservé* umschrieben als »*[a] prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely.*«[551] Gemeint sind grundsätzlich Bereiche, die alleine dem Staat unterstehen, wie »Entscheidungen zum politischen, ökonomischen, sozialen und kulturellen System«.[552] Im heutigen von Interdependenzen geprägten internationalen Umfeld wird der dem Staat vorbehaltene *domaine réservé* zunehmend schwieriger zu definieren. Einigen Beobachtern zufolge wird der Bereich gar kleiner, indem Probleme vermehrt global ausgerichtet sind und die internationale Gemeinschaft als Ganzes betreffen.[553] Damit gemeint sind Probleme, die sich aufgrund der zunehmenden internationalen (politischen und wirtschaftlichen) Verflechtungen ergeben – die exemplarisch gerade auch den global vernetzten Cyberbereich zunehmend betreffen werden. Einer anderen Haltung zufolge sind durch die verstärkte Verflechtung hingegen mildere, unauffälligere Einflussnahmen als mit Gewalt möglich, wodurch der Begriff der Intervention im 20. Jahrhundert nicht enger, sondern weiter zu verstehen sei.[554] So ist Roscini zufolge eine Erweiterung des Begriffs insb. für die Erfassung von Cyberangriffen notwendig.[555]

Eine weitere Herausforderung ist die konkrete Definition des erforderlichen Zwangs. Allgemeingültige und anerkannte Kriterien gibt es nicht.[556] Im Kern geht es um Eingriffe, die dem Zielstaat Entscheidungsfreiheiten nehmen und ihn dazu bringen, so zu handeln wie er es ohne den Eingriff nicht getan hätte.[557] Dem betreffenden Staat muss ein gewisses Verhalten aufgezwungen werden, wobei eine Druckausübung ohne Zwangselement nicht ausreicht.[558]

---

550 Schmitt, Grey Zones, S. 7.

551 IGH, Nicaragua-Urteil, §205. Dazu u.a. Schmitt, Grey Zones, S. 7.

552 IGH, Nicaragua-Urteil, §205; Declaration on Friendly Relations (UN Doc. A/RES/2625 (XXV), S. 123; Declaration on the Inadmissibility of Intervention (UN Doc. A/RES/36/103 (1981)), Annex, S. 79 §2(b); Schmitt, Grey Zones, S. 7; Schulze, S. 103 m.w.V.

553 Schulze, S. 103. Ähnlich: Tallinn Manual 2.0, S. 314 R66 C6 und S. 316 R66 C13, (siehe allerdings zu klaren Bereichen des *domaine réservé*) S. 315 R66 C10; Jensen, Tallinn Manual 2.0, S. 775.

554 Vgl. Kunig, MPEPIL 2008, §3.

555 Roscini, Cyber Operations, S. 65.

556 Schulze, S. 105. Auch die in diesem Kontext oft diskutierte Declaration on Friendly Relations (UN Doc. A/RES/2625 (XXV) und das Nicaragua Urteil bieten keine klaren Kriterien für die Anwendung in der Praxis: Diggelmann/Hadorn, S. 9.

557 Schmitt, Grey Zones, S. 8; Tallinn Manual 2.0, S. 318 f., R66 C21.

558 Diggelmann/Hadorn, S. 8; Lahmann, S. 37; Kunig, MPEPIL 2008, §1; Watts, S. 256 m.w.V.

Im Einzelnen bleibt die Abgrenzung von völkerrechtswidrigem Zwang und erlaubtem Druck vage.[559] Klare Szenarien wie z.B. militärische Eingriffe[560] konstituieren Interventionen, während es bei wirtschaftlichen Aktivitäten und der Sicherung wirtschaftlicher Vorteile grundsätzlich nicht der Fall ist bzw. die Würdigung der Grenzen unzulässiger Intervention schwieriger wird.[561] Auch erhebliche systemkritische Äusserungen stellen grundsätzlich keine unzulässige Intervention dar,[562] da der Staat seine Entscheidungsmacht behält.[563] Anders wäre dies bei finanzieller Unterstützung von Rebellen, deren Ausbildung oder Versorgung mit Waffen, um eine Regierung zu stürzen, wie dies in der prominenten Nicaragua-Entscheidung des IGH diskutiert wurde. In einem solchen Fall würde ein Zwangselement gegenüber der fremden Staatsgewalt bejaht.[564] Dazwischen liegende Szenarien sind allerdings weniger eindeutig[565] und bleiben daher Gegenstand der jeweiligen Einzelfallbetrachung. Zudem können auch an sich unbedenkliche Szenarien jeweils gewisse Schwellen erreichen und in Graubereiche des (Un-)Erlaubten kommen: Beispielsweise können grundsätzlich erlaubte, systemkritische Meinungsäusserungen bei der Erfüllung eines Zwangselements zu Graubereichen (un-)erlaubter Propaganda führen. Obschon eine Beeinflussung durch Propaganda nicht *per se* verboten ist, kann diese als Intervention gelten, wenn in der Folge die Entscheidungsfreiheit der Adressaten wesentlich eingeschränkt wird oder wenn in massgeblicher Weise und vergleichbar mit finanzieller und logistischer Unterstützung Zwang ausgeübt wird.[566]

559 Diggelmann/Hadorn, S. 9. Zur Vagheit des erforderlichen Zwangs auch: Watts, S. 270.

560 IGH, Nicaragua-Urteil, §205. Der IGH umschreibt das Zwangselement bei Gewaltanwendungen durch direkte militärische Handlungen oder die indirekte Unterstützung bewaffneter Aktivitäten als »particularly obvious«; Watts, S. 259.

561 Unilaterale Wirtschaftsembargos wurden vom IGH grundsätzlich als keine Intervention qualifiziert, da es, vereinfacht gesagt, jedem Staat freisteht, mit wem er handeln möchte. Anders bei ökonomischen Blockaden oder zwangsweisen Versuchen, einem Staat die Beteiligung an der Weltwirtschaft zu verwehren, da dabei der nötige Zwang bejaht würde: IGH, Nicaragua-Urteil, §245; Watts, S. 260.

562 Diggelmann/Hadorn, S. 8.

563 Schmitt, Grey Zones, S. 7.

564 IGH, Nicaragua-Urteil, §109 ff., S. 108 §205; Diggelmann/Hadorn, S. 267; Schmitt, Grey Zones, S. 8.

565 Schmitt, Grey Zones, S. 7.

566 Watts, S. 261 m.w.V.

ii. Cyberangriffe und Interventionsverbot

Das gewohnheitsrechtlich anerkannte Interventionsverbot findet grundsätzlich auch Anwendung auf staatliche Handlungen im Cyberraum.[567] Dabei mag auch eine konstante Cyberaktivität in fremden Netzwerken[568] die rechtliche Bedeutung des Prinzips nicht zu untergraben.[569] Staaten dürfen – wie im nicht-digitalen Kontext auch – nicht mittels Cyberangriffen zwangsweise in die inneren Angelegenheiten eines anderen Staates eingreifen. Für eine Verletzung des Interventionsverbots sind daher ebenfalls ein Eingriff in den *domaine réservé* sowie das Zwangselement massgebend.[570] Wann diese beiden Elemente konkret gegeben sind, bleibt dabei jedoch relativ vage.[571] So waren die Experten im Tallinn Manual bspw. uneinig, wann das zwangsähnliche Element erfüllt ist[572]: Gemäss der Mehrheit der Expertengruppe muss die entsprechende Handlung darauf ausgerichtet sein, Ergebnisse (»*outcomes*«) im Zielstaat oder das Verhalten bezüglich einer dem Staat vorbehaltenen Angelegenheit (*domaine réservé*) zu beeinflussen.[573] Ebenso blieben sie uneinig im Hinblick darauf, ob der Zwang die Effekte direkt auslösen muss. Die Mehrheit verneinte dies, unter der Voraussetzung, dass ein gewisser Kausalzusammenhang bestehe.[574] Die Beantwortung der Frage, wann Cyberangriffe das Interventionsverbot verletzen, ist damit letztlich in jedem Einzelfall zu würdigen.[575]

---

567 Ossoff, S. 295 ff.; Schmitt, Countermeasures Response Option, S. 705; Schmitt, Cyber Election Meddling, S. 48 ff.; Watts, S. 253; Wheatley, S. 161 ff. Auch die Expertengruppe des Tallinn Manuals war sich einig, dass das gewohnheitsrechtliche Interventionsverbot auch auf Cyberangriffe Anwendung findet: Tallinn Manual 2.0, S. 312 R66 C1. Das Prinzip wurde grundsätzlich auch in den UN GGE Berichten (u.a. UN Doc. A/76/136 (2021)) bejaht.

568 Zur Unterscheidung von Zwang und Spionage: Lahmann, S. 35 f.

569 Watts, S. 253; Tallinn Manual 2.0, S. 314 R66 C5. Ähnlich ferner: IGH, Nicaragua-Urteil, §186.

570 Tallinn Manual 2.0, S. 314, R66 C6; Lahmann, S. 33 ff. Siehe auch UN Doc. A/RES/70/174 (2015), §28(b). Zu ausgewählten Staatenasichten zum Interventionsverbot: Roguski, S. 7 ff.

571 Dazu auch: Roguski, S. 8.

572 Einig waren sie sich darin, dass die Abgrenzung von (un-)erlaubtem Zwang im Einzelfall nicht immer klar sei: Tallinn Manual, S. 319 R66 C22. Der Zwang muss für eine Verletzung des Interventionsverbot jedoch von einer gewissen Intensität sein: vgl. Schmitt, Just Security vom 10.06.2019.

573 Tallinn Manual 2.0, S. 318, R66 C19. Dazu auch: Lahmann, S. 34.

574 Tallinn Manual 2.0, S. 320, R66 C24; Jensen, Tallinn Manual 2.0, S. 775.

575 Schulze, S. 114 m.w.V.; Stein/Marauhn, S. 25.

Vorliegend soll anhand von Beispielen eine Annäherung an mögliche Verletzungskonstellationen erfolgen. Die klarsten Fälle einer Intervention durch Cyberangriffe sind diejenigen, die als völkerrechtliche Gewalt qualifiziert werden können, da Gewalt die stärkste Form der Zwangseinwirkung darstellt.[576] Gegebenenfalls gilt dies für Cyberangriffe, die physische Zwangseinwirkungen nach sich ziehen.[577] Somit könnte das Beschädigen der iranischen Atomanlage durch Stuxnet als eine Verletzung des Interventionsverbots gesehen werden,[578] wenn diese rechtlich und technisch einem Staat zugerechnet werden kann (dazu nachfolgend ausführlicher). Das für eine Intervention erforderliche Zwangselement setzt dabei allerdings keine physischen Schäden voraus.[579] Angriffe, die nicht in den Anwendungsbereich von Art. 51 UN-Charta fallen, befinden sich somit nicht in einem rechtsfreien Raum, sondern lassen sich gegebenenfalls unter das Interventionsverbot subsumieren.[580] Um das Beispiel eines von einem Cyberangriff ausgehenden folgenschweren Börsenabsturzes aufzugreifen: Obwohl solche Angriffe mangels physischer Schädigungen nach vorliegend vertretener Ansicht keinen bewaffneten Angriff gem. Art. 51 UN-Charta darstellen, können sie gegebenenfalls in zwangsähnlicher Weise die Infrastruktur des Finanzplatzes des jeweiligen Staates schwächen. Dadurch könnte u.U. das Vertrauen in die Institutionen geschwächt sowie insb. auch die Staatsgewalt und der Staat beschädigt werden.[581] Ähnlich könnten auch Cyberangriffe auf politische Akteure, Wahl- oder Wahlergebnismanipulationen u.U.

576 Tallinn Manual 2.0, S. 319 R66 C22; Roscini, Cyber Operations, S. 65; Schulze, S. 114; Woltag, S. 124.

577 Schulze, S. 114 m.w.V. auf S. 89.

578 Die Experten im Tallinn Manual kategorisierten Stuxnet als Intervention: Tallinn Manual 2.0, S. 319 R66 C26. Stuxnet neben einer Intervention auch als verbotene Gewaltanwendung i.S.v. Art. 2(4) UN-Charta qualifizierend: u.a. Schulze, S. 127 m.w.V; Buchan, S. 221. Ein Teil der Expertengruppe des Manuals qualifizierten Stuxnet darüber hinaus auch als bewaffneten Angriff: Tallinn Manual 2.0, S. 342 R71 C10. Letztere Qualifizierung ist vorliegend allerdings aus den unter III.B.1. erläuterten Gründen abzulehnen.

579 Tallinn Manual 2.0, S. 318, R66 C20.

580 Woltag, S. 111 ff.

581 Diggelmann/Hadorn, S. 267. Ähnlich: BJ/DV, Gutachten vom 10.03.2009, S. 166 (allerdings ohne nähere Begründung).

eine Intervention darstellen.[582] Wahlen stellen trotz zunehmender Interkonnektivität nämlich Angelegenheiten innerhalb des *domaine réservé* eines Staates dar.[583] Dabei könnten bereits Angriffe auf einzelne Politiker die Schwelle überschreiten, wenn der Angriff in zwangähnlicher Weise eine Beeinflussung des politischen Prozesses bezweckt. DIGGELMANN/HADORN erwähnen etwa das Beispiel, als Frankreichs Präsident Emmanual Macron kurz vor den Wahlen grossangelegten Cyberangriffen zum Opfer fiel und mit dem Ziel einer politischen Einflussnahme massenhaft private – teilweise gefälschte – Informationen veröffentlicht wurden.[584] Die Absicht hinter dem Angriff war, ihn vor der entscheidenden Runde als politischen Akteur zu schädigen.[585] Ein weiteres prominentes Beispiel sind die Cyberangriffe auf die US-Päsidentschaftswahlen 2016.[586] Die Demokraten wurden im damaligen Wahlkampf wesentlich geschwächt, indem geheime Dokumente der Partei gehackt und veröffentlicht wurden. Mitunter soll diese Veröffentlichung zum Rücktritt verschiedener Parteimitglieder und zu Spannungen zwischen den Lagern von Clinton und Sanders geführt haben.[587] Auch in solchen Konstellationen ist aus völkerrechtlicher Sicht insb. die Frage zentral, ob und wann das Zwangselement erfüllt ist.[588] Staatliche Versuche, die öffentliche Meinungsbildung in anderen Staaten zu beeinflussen, sind im Grunde nichts Neues, und solange dies öffentlich geschieht, würde ein Zwangselement verneint.[589] Auch ein Eindringen in andere Netzwerke, um (in passiver Weise) an Informationen zu kommen, würde

582 DIGGELMANN/HADORN, S. 267; SCHMITT, Cyber Election Meddling, S. 49 ff. Ähnlich SCHULZE: Ihm gemäss fallen absichtliches Verfälschen von Wahlergebnissen oder das bewusste, auf Defacement oder Video Morphing basierende Streuen von Fehlinformationen zur Beeinflussung der Meinungsbildung, unter das Interventionsverbot: SCHULZE, S. 114, S. 30 ff. Ähnlich: ROSCINI, Cyber Operations, S. 65; Tallinn Manual, S. 45 R10 C10. Zu einer zrückhaltenden und differenzierten Abhandlung von Zwang bei politischen Einflussnahmen: LAHMANN, S. 36 ff.

583 LAHMANN, S. 38. Dazu eingehender: OSSOFF, S. 295 ff.

584 BORGER, The Guardian vom 06.05.2017.

585 DIGGELMANN/HADORN, S. 267 m.V.a. Agenturmeldung reu/afp/dpa, NZZ vom 06.05.2017. Mit zurückhaltender Annahme des Zwangselements: LAHMANN, S. 37 f.

586 SANGER/SHANE, New York Times vom 09.12.2016; TIKK/HOVHANNISYAN/KERTTUNEN/SALMINEN, S. 42 f.; SCHMITT, Cyber Election Meddling, S. 32 ff.

587 LIPTON/SANGER/SHANE, New York Times vom 13.12.2016; LIPTON/SHANE, New York Times vom 13.12.2016; MARTIN/RAPPEPORT, New York Times vom 24.06.2016; SCHMITT, Grey Zones, S. 1.

588 Eingehender dazu: WHEATLEY, S. 161 ff.; LAHMANN, S. 36. KILOVATY ist demgegenüber der Ansicht, dass staatliche Einflussnahmen in politische Prozesse auch dann das Interventionsverbot verletzen, wenn das Zwangselement nicht vorliegt: KILOVATY, Doxfare, S. 146 ff.

589 LAHMANN, S. 36.

grundsätzlich noch keine Intervention darstellen, solange diese Informationen nicht zwangsmässig eingesetzt werden, um ein (politisches) Verhalten im Zielstaat zu bezwecken (und dies auch tatsächlich tun).[590] Eine zwangsmässige Einflussnahme wäre grundsätzlich nur dann anzunehmen, wenn davon auszugehen ist, dass ein Wahlprozess aktiv manipuliert und dadurch das Wahlergebnis massgeblich beeinflusst wird.[591] Ob und unter welchen Bedingungen solche Cyberangriffe den für eine Intervention notwendigen Zwang letztlich jedoch erfüllen, ist *in abstracto* nicht präzise auszumachen.[592] Die verbleibenden »Graubereiche« dieser Abwägung könnten gem. SCHMITT durchaus mitursächlich gewesen sein, dass die USA bspw. die Cyberangriffe auf die Wahlprozesse 2016 weder als Verletzung kategorisierten noch Gegenmassnahmen anordneten.[593]

Ähnlich könnten bei erfolgreicher Zurechnung und im Sinne einer Gesamtwürdigung die Cyberangriffe auf Georgien am 8. August 2008 u.U. als eine Verletzung des Interventionsverbots gesehen werden.[594] Die Blockierungen von Regierungswebseiten, die Manipulation von Inhalten[595] und die digitale Isolation von Georgien nach aussen[596] könnten im Hinblick auf das Mass insgesamt als zwangsmässige Einwirkung auf innere Angelegenheiten von Georgien qualifiziert werden. Ähnlich könnten die Angriffe auf Estland am 27. April 2007 aufgrund ihrer breiten ökonomischen Schäden unter den Anwendungsbereich

590 WATTS, S. 256. Ähnlich: Tallinn Manual 2.0, S. 323 R66 C33, in der die Expertengruppe reinen Spionageakten das Zwangselement absprechen. Dies sei auch dann der Fall, wenn das Eindringen in die digitalen Infrastrukturen ein unbefugtes Knacken von Passwörtern oder Firewalls impliziere. (Dies sei jedoch u.U. von Tallinn Manual 2.0, S. 168 ff. R32 zu differenzieren). Zur Schwierigkeit, »Zwang« im Cyberkontext anzuwenden auch: LAHMANN, S. 33 ff. LAHMANN bezweifelt im Ergebnis, dass durch Cyberangriffe ausgelöste Effekte vom herkömmlichen Begriff des Zwangs addressiert werden können: LAHMANN, S. 261 f.

591 LAHMANN, S. 37 mit dem Bsp. einer Manipulation elektronischer Stimmauszählungssystemen unter Verweis auf WRIGHT, Rede vom 23.05.2018; SCHMITT, Grey Zones, S. 8. TIKK/HOVHANNISYAN/KERTTUNEN/SALMINEN, S. 42 umschreiben solche Beeinflussungen als »*plausible indirect behavioral effects*«.

592 LAHMANN, S. 36 f.; SCHMITT, Grey Zones, S. 8; SCHMITT, Cyber Election Meddling, S. 32 ff., S. 48 ff.

593 SCHMITT, Grey Zones, S. 8. Ausführlicher zu SCHMITT's Ansichten zu Gegenmassnahmen im Rahmen der Staatenverantwortlichkeit siehe: SCHMITT, Countermeasures Response Option, S. 697 ff.

594 SCHULZE, S. 28 f., S. 126.

595 Gemäss Schulze als »Defacement«-Angriffe umschrieben: SCHULZE, S. 125.

596 Der Zugang zu ausländischen Netzwerken sowie das Versenden von Nachrichten wurde weitgehend verunmöglicht: SCHULZE, S. 126.

einer verbotenen Intervention (und nicht in denjenigen eines bewaffneten Angriffs) fallen.[597] Durch die massiven Wellen von DDoS-Angriffen sowie durch die Manipulationen von Webseiten, den unzähligen Spam-E-Mails und der Online-Propaganda[598] kann argumentiert werden, dass zwangsähnlich auf die Wirtschaft und das Vertrauen in öffentliche Institutionen eingewirkt wurde. Hintergrund dieses Konflikts waren politische Spannungen zwischen Estland und der russischen Minderheit,[599] womit eine bezweckte politische Einflussnahme auf einen inneren ethnischen Konflikt[600] naheliegend ist.[601] LAHMANN verweist ferner darauf, dass Cyberangriffe einigen Autoren zufolge, auch ohne konkrete politische Absichten, ein Zwangselement beinhalten können, wenn der angegriffene Staat dazu gebracht wird, (Verteidigungs-)Massnahmen zu ergreifen, die er sonst nicht hätte ergreifen müssen. In diesem Sinne könne es als genügend erachtet werden, dass im Falle Estlands das staatliche Netzwerk vom Internet abgekoppelt werden musste, um die DDoS-Angriffe zu stoppen.[602] Neben der Blockierung staatlicher Webseiten gab es zudem auch materielle Schäden und eine Beeinträchtigung des Informationsflusses Estlands nach aussen.[603] Zu den ohnehin bereits intensiven Auwirkungen auf verschiedene Staats- und Privatwirtschaftszweige kommt hinzu, dass die Angriffe über mehrere Wochen anhielten, was das Mass an zulässigem politischen Druck wohl übersteigt.[604]

iii. Zusammenfassung

Grundsätzlich besteht ein weitgehender Konsens, dass mittels Cyberangriffen in unzulässiger Weise in den *domaine réservé* von Staaten eingegriffen werden kann.[605] Dabei bleiben in Bezug auf die Frage, welche Konstellationen im Einzelnen darunter fallen, Unklarheiten bestehen.[606] Insgesamt muss das Interventionsverbot im Cyberkontext daher differenziert betrachtet und jeweils im Einzelfall abgewogen werden. Dies eröffnet in Bezug auf Cybervorfälle durchaus auch sinnvolle Spielräume: Durch die Einzelfallwürdigung kann das durch

597 Vgl. TIKK/KASKA/VIHUL, S. 24 f. Im Ergebnis ähnlich: LAHMANN, S. 34.
598 TIKK/KASKA/VIHUL, S. 20.
599 TIKK/KASKA/VIHUL, S. 15 f.
600 Vgl. Tallinn Manual 2.0, S. 318 R66 C19.
601 SCHULZE, S. 123 f.
602 LAHMANN, S. 34 m.V.a. WOLTAG, MPEPIL 2015, §6.
603 TIKK/KASKA/VIHUL, S. 24 f.
604 SCHULZE, S. 124. Im Ergebnis auch BUCHAN, S. 226.
605 LAHMANN, S. 41; ROGUSKI, S. 7.
606 ROGUSKI, S. 8.

Cyberangriffe breite Spektrum unterschiedlicher Effekte und Schäden erfasst werden. Das Interventionsverbot ermöglicht somit – anders als die Ausrichtung auf physische Schäden beim bewaffneten Angriff – politische und ökonomische Schäden miteinzubeziehen. Mit dem Interventionsverbot besteht folglich eine völkerrechtliche Grundlage, Cyberangriffe mit erheblichen Konsequenzen für einen Staat zu erfassen – und zwar ausserhalb der *ius-ad-bellum*-Debatte.[607] Allerdings drängt sich eine eingehendere Diskussion des Prinzips, mitunter des erforderlichen Zwangs und des *domaine réservé* in der modernen und zunehmend vernetzten Welt auf, da die Möglichkeit von (zwangsmässigen) Einflussnahmen auf andere Staaten durch digitale, transnationale Kanäle wohl weiterhin zunehmen wird.[608]

Die Staatengemeinschaft hat sich grundsätzlich weitgehend zur Geltung des Interventionsverbots im Cyberkontext bekannt.[609] Die Souveränität von Staaten soll daher auch im Kontext von Cyberangriffen weiterhin respektiert werden. Durch die Bestätigung einer Norm wird folglich auch deren weiterbestehende Geltung bestätigt. Eine Auseinandersetzung mit dem Interventionsverbot durch die Staaten kann dabei zu einer Schärfung der Konturen des Prinzips im Cyberkontext beitragen.[610] Die Erfahrungen mit der historischen Entstehung des Interventionsverbots und seiner Deeskalationswirkung in den Konfessionskriegen zeigen, dass sein Potenzial auch in der Gegenwart nicht zu unterschätzen ist. Letztlich sind politische Einflussnahmen und Einmischungen nichts Neues – Cybertechnologien ermöglichen lediglich neue Mittel und Methoden, um dies zu erreichen.

607 Ähnlich: BUCHAN, S. 226. Die völkerrechtlichen Aspekte des Interventionsverbots lassen letztlich auch eine Erfassung von dem der SCO-Staaten vertretenen Verständnis von Cyberangriffen als politische oder soziale Einmischungen zur Destabilisierung eines Staatssystems zu. Zu diesem Verständnis siehe vorangehend unter III.A.2.

608 LAHMANN, S. 36 ff.

609 UN Doc. A/RES/70/174 (2015), §28(b); UN Doc. A/76/136 (2021); ROGUSKI, S. 7 f.

610 WATTS, S. 270.

b. Rechtliche Zurechnung eines Völkerrechtsverstosses an einen Staat

i. Grundidee der völkerrechtlichen Zurechnung

Im Kontext der Staatenverantwortlichkeit muss eine Normverletzung (wie eine unzulässige Intervention) gem. Art. 2 ARSIWA einem Staat zugerechnet werden können, um eine Völkerrechtsverletzung konstituieren zu können.[611] Grundsätzlich gilt ein Staat dann als verantwortlich für einen Völkerrechtsverstoss, wenn dieser durch das Handeln oder Unterlassen eines staatlichen Organs ausgeführt wird.[612] Das heisst, grundsätzlich ist ein Staat nicht verantwortlich für das Verhalten privater Personen oder Unternehmen.[613] Die Verantwortlichkeit eines Staates für privates Handeln entsteht nur unter bestimmten Bedingungen: Wenn er einen Privaten gem. Art. 5 ARSIWA zum betreffenden Handeln ermächtigt, wenn der Private gem. Art. 8 ARSIWA auf Instruktionen hin oder unter der Kontrolle des Staates handelt, wenn der Private bei Abwesenheit oder Nichterfüllung der Staatsgewalt gem. Art. 9 ARSIWA an dessen Stelle *de facto*-Elemente staatlicher Gewalt ausübt oder wenn der Staat das betreffende Handeln gem. Art. 11 ARSIWA als sein eigenes anerkennt.[614]

Handlungen von *de iure*-Staatsorganen sind unabhängig ihrer Funktion, Position oder Charakters innerhalb der staatlichen Organisation dem betreffenden Staat zuzurechnen.[615] Es ist irrelevant, ob das staatliche Organ gem. nationalem Recht ermächtigt ist, in Vertretung des Staates auf internationaler Ebene zu handeln.[616] Die Eigenschaft als Staatsorgan wird folglich eher grosszügig angenommen.[617] Zudem spielt es keine Rolle, von welchem Ort oder Territorium aus die jeweilige Handlung erfolgt, da die Organeigenschaft des Herkunftstaats das für die Zurechnung relevante Kriterium ist.[618] *De facto*-

611 Stern, S. 201 f.

612 Art. 2 ARSIWA; Woltag, S. 87.

613 IGH, Korfu Kanal-Urteil, S. 18; IGH, Teheraner Geiselfall, §58 ff.; Dahm/Delbrück/Wolfrum, Bd. I/3, S. 906; De Frouville, S. 261 ff.; Diggelmann/Hadorn, S. 270; Kees, MPEPIL 2011, §1.

614 Diggelmann/Hadorn, S. 270; Schröder, S. 699 ff.; Woltag, S. 88. Ausführlicher zu Zurechnungskonstellationen für rechtswidriges Verhalten Privater: Epiney, S. 33 ff.

615 ARSIWA-Kommentar, Art. 4(2), (11). Schröder, S. 706; Woltag, S. 88.

616 Dahm/Delbrück/Wolfrum, Bd. I/3, S. 891; Tallinn Manual 2.0, S. 88 R15 C3; Woltag, S. 88. Vgl. ARSIWA-Kommentar, Art. 4(2), (11).

617 Vgl. Tallinn Manual 2.0, S. 87 R15 C3.

618 Hierzu u.a.: Dörr, S. 644 ff.; Schulze, S. 55.

Staatsorgane oder durch den Staat zur Ausübung von Elementen staatlicher Gewalt ermächtigte Personen werden wie Staatsorgane behandelt.[619] Es ist unbestritten, dass Cyberangriffe, die durch das staatliche Militär, die Polizei, Nachrichtendienste oder andere Behörden ausgeführt werden, dem Staat zuzurechnen sind.[620] Dasselbe gilt für den Fall, in dem ein Staat eines seiner Organe einem anderen Staat zur Verfügung stellt. Die Handlungen werden letzterem Staat zugerechnet, wenn Elemente seiner staatlichen Gewalt ausgeübt werden.[621] Bei staatlichen Organen wird nicht nur die Organeigenschaft breit angenommen, sondern auch die Handlungen werden eher grosszügig zugerechnet: Wenn staatliche Organe in einer offiziellen Funktion internationale Verpflichtungen verletzen, wird der betreffende Staat verantwortlich, auch wenn die Handlungen die vom Staat erteilte Befugnis übersteigen oder gegen seine Anweisungen verstossen (sog. Handlungen »*ultra vires*«).[622] Solange das betreffende Organ in offizieller Funktion handelt,[623] ist es unerheblich, welche Motive ausschlaggebend waren oder ob die öffentliche Macht missbraucht wird.[624] *Ultra vires*-Handlungen führen grundsätzlich auch bei zur Ausübung öffentlicher Gewalt befugten Akteuren zur Verantwortlichkeit des betreffenden Staates.[625]

Schwieriger zu beurteilen ist die Zurechnung privaten Handelns an einen Staat. Es kommt auf die Enge der Beziehung zwischen unmittelbar privat Handelnden und dem Staat an. Insbesondere wirft die Definition der erforderlichen Kontrolle i.S.v. Art. 8 ARSIWA Fragen auf.[626] Diese Thematik führte zu weitgehenden Debatten zum vom IGH im Nicaragua-Urteil entwickelten »*effective control*«-Test[627] und des sog. »*overall control*«-Test der Berufungskammer des Internationalen Strafgerichtshofs für das ehemalige Jugoslawien

619 Art. 4, 5 und 8 ARSIWA; Kees, MPEPIL 2011, §2; Palchetti, MPEPIL 2017, §1 ff.; Woltag, S. 88 f.

620 Woltag, S. 89. Das Tallinn Manual, S. 87 R15 C2 nennt z.B. das US Cyber Command, the Netherlands Defence Cyber Command oder Israels Unit 8200 als staatliche Akteure.

621 ARSIWA-Kommentar, Art. 6(1); Tallinn Manual 2.0, S. 93 R16.

622 Art. 7 ARSIWA; Tallinn Manual 2.0., S. 89 R15 C6.

623 Verantwortlichkeit entsteht nicht bei rein privaten Handlungen oder Unterlassungen, wie bei unbefugtem Zugang zu privaten Bereicheungszwecken: Tallinn Manual 2.0., S. 89 R15 C7.

624 ARSIWA-Kommentar, Art. 4(13); Tallinn Manual 2.0., S. 89 R15 C7.

625 ARSIWA-Kommentar, Art. 5(6); Tallinn Manual 2.0., S. 90 R15 C12.

626 Siehe eingehender dazu: Mačák, S. 405 ff.

627 IGH, Nicaragua-Urteil, §115. Ähnlich auf die effektive Kontrolle abstellend in: IGH, Bosniengenozid-Urteil, §400.

im Tadić-Fall[628].[629] Die Debatten sollen vorliegend nicht im Einzelnen rekapituliert werden. Festzuhalten ist in Bezug auf den »*overall control*«-Test, dass dieser, obschon er auch in Bezug auf Cyberangriffe diskutiert wurde[630], sich grundsätzlich nicht für den vorliegend relevanten Kontext der Staatenverantwortlichkeit eignet. Inhaltlich wurde dieser nämlich vielmehr im Zusammenhang mit Primärnormen des humanitären Völkerrechts etabliert, um bewaffnete Koflikte zu kategorisieren,[631] und er würde den Kontext der Staatenverantwortlichkeit übermässig ausweiten.[632] Damit soll vorliegend für rechtliche Zurechnungsfragen (bei Cyberangriffen) der »*effective control*«-Test des IGH relevant sein.[633] Dieser Massstab ist hoch angesetzt: Im Nicaragua-Fall ging es um unmittelbar agierende private Rebellengruppen, deren Handlungen allenfalls im Rahmen der Staatenverantwortlichkeit den USA zurechenbar hätten sein sollen.[634] Die USA übten Einfluss auf die in Nicaragua gegen die Regierung vorgehenden Contra-Rebellen aus. Der IGH rechnete die Handlungen den USA allerdings nicht an, da die Rebellen nicht direkt »gesteuert« gewesen seien und die USA somit keine »effektive Kontrolle« über die Rebellen gehabt hätten.[635]

ii. Cyberangriffe und völkerrechtliche Zurechnung

Das Tallinn Manual lehnt sich mit seiner Regel 17 zur Zurechnung privaten Handelns in lit. (a) an Art. 8 ARSIWA und in lit. (b) an Art. 11 ARSIWA an.[636] Instruktionen werden gem. Regel 17(a) des Tallinn Manuals 2.0 bspw. ange-

628 IStGJ, Tadić-Urteil, §98 ff. (unter Bezugnahme auf den Ansatz des IGH).

629 Der »effective control« und der »overall control«-Test stellten (gemeinsam mit weiteren Urteilen wie dem IGH, Bosniengenozid-Urteil oder auch Urteilen des EGMR) Gegenstand einer weitergehenden Zurechungs-Debatte dar: Crawford, State Responsibility, S. 146 ff.

630 Im Zusammenhang mit Cyberangriffen aufgegriffen wurde die Debatte u.a. durch Schulze, S. 134 ff. (den »*overall control*«-Ansatz bei der Staatenverantwortlichkeit für Cyberangriffe im Ergebnis ablehnend); Woltag, S. 91 ff.

631 Dies im Ergebnis bestätigend: Crawford, State Responsibility, S.156; Tallinn Manual 2.0, S. 96 R17 C6 m.V.a. IGH, Bosniengenozid-Urteil, §404 ff.

632 IGH, Bosniengenozid-Urteil, §406.

633 So auch: Tallinn Manual 2.0., S. 96 R17 C5 (siehe nachfolgend).

634 Diggelmann/Hadorn, S. 11.

635 IGH, Nicaragua-Urteil, §115 f.; Diggelmann/Hadorn, S. 11.

636 Siehe Tallinn Manual 2.0, S. 94 R17: »*Attribution of cyber operations by non-State actors Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own*«.

nommen, wenn ein Staat private IT-Firmen oder einzelne Hacker beauftragt, gewisse Arten von Cyberangriffen zu programmieren, ohne sie in die offiziellen staatlichen Strukturen zu integrieren.[637] Die Begriffe »*direction*« und »*control*« werden oft gemeinsam behandelt und beziehen sich auf eine kontiniuerliche Ausübung von Kontrolle (»*authority*«) über eine betreffende Cyberhandlung.[638] Die Experten im Tallinn Manual waren sich einig, dass der »*effective control*«-Ansatz des IGH den Anwendungsbereich von Cyberangriffen erfasse.[639] Demzufolge übe ein Staat dann effektive Kontrolle über einen spezifischen Cyberangriff eines Privaten aus, wenn er über die Durchführung und den Verlauf jenes Angriffs bestimme und die ausgeführte Handlung oder das Programm einen »integralen Bestandteil« desselben darstelle.[640] Unter »effektive Kontrolle« falle des Weiteren die Fähigkeit, sowohl betreffende Handlungen für einen Cyberangriff als auch die Beendigung laufender Cyberangriffe anzuordnen.[641] Die generelle Unterstützung oder Ermunterung nichtstaatlicher Cyberangriffe durch einen Staat reicht demnach nicht aus, um ihm diese zuzurechnen.[642] Darunter würde den Experten im Tallinn Manual zufolge auch nicht ohne Weiteres das Zurverfügungstellen von Schadprogrammen fallen.[643] Allerdings könnte das Zurverfügungstellen bei substantiellem Wissen um eine damit ausgelöste Völkerrechtsverletzung und gegebener Verhinderungsmöglichkeit eine Verantwortlichkeit aufgrund der Due Diligence-Pflicht begründen (siehe nachfolgend). Des Weiteren stellen sich bei Cyberangriffen, die sich automatisiert weiterverbreiten (z.B. Stuxnet), im Hinblick auf die Beendigungsmöglichkeit Schwierigkeiten. Kann man jene (automatisierte) Weiterverbreitung überhaupt »kontrollieren« und stoppen?

---

637 ARSIWA-Kommentar, Art. 8(2); Tallinn Manual 2.0, S. 95 f. R17 C4. Nicht zu verwechseln sind Instruktionen mit dem Ermächtigen Privater zur Ausübung von Elementen staatlicher Gewalt: Tallinn Manual 2.0, S. 95 f. R17 C4. Mikanagi, S. 1027 sieht neben der Akteursfrage auch die für den Angriff genutzte Infrastruktur als massgebend für die Zurechnung eines Angriffs an einen Staat. Nach vorliegender Haltung spielt die Würdigung einer (privaten oder staatlichen) Infrastruktur allerdings weniger im Rahmen der Zurechnung gem. ARSIWA als i.Z.m. sorgfaltspflichtsrechtlichen Fragen der Due Diligence eine Rolle (siehe nachfolgend), da Infrastrukturen jeweils als Brückenkopf missbraucht werden können. Ähnlich dazu: Tallinn Manual 2.0, S. 91 R15 C14.

638 Crawford, State Responsibility, S. 146; Tallinn Manual 2.0, S. 96 R17 C5.

639 Tallinn Manual 2.0, S. 96 R17 C5 f. m.V.a. IGH, Nicaragua-Urteil, §115; IGH, Bosniengenozid-Urteil, §400.

640 ARSIWA-Kommentar, Art. 8(3).

641 Tallinn Manual 2.0, S. 96 R17 C6.

642 Tallinn Manual 2.0, S. 97 R17 C8.

643 Tallinn Manual 2.0, S. 97 R17 C8.

Bei einer automatisierten Weiterverbreitung von Schadprogrammen müsste man sich fragen, ob diese als integraler Bestandteil des jeweiligen Cyberangriffs zu werten ist. Wenn sich Angriffe (automatisiert) weiterverbreiten, könnte man sich nämlich im Bereich von *ultra vires*-Handlungen bewegen. In diesem Zusammenhang sind die Ausführungen zur Regel 17 im Tallinn Manual interessant. Im Gegensatz zur grundsätzlichen Anrechnung von *ultra vires*-Handlungen bei staatlichen Akteuren[644] werden über die Befugnisse hinausgehende Cyberangriffe privater Akteure dem Staat grundsätzlich nicht angerechnet.[645] Private Handlungen sind einem Staat nur anzurechnen, wenn diese einen integralen Bestandteil des betreffenden Cyberangriffs darstellen, über den der Staat effektive Kontrolle hat.[646] Ist dies der Fall, werden die Handlungen dem Staat, trotz einer Missachtung staatlicher Anweisungen durch die Privaten, zugerechnet.[647] Wenn sich Schadprogramme also weiterverbreiten und in Drittstaaten Schäden anrichten, kommt es einerseits darauf an, ob es sich um staatliche oder nichtstaatliche Akteure handelt und andererseits darauf, ob die völkerrechtswidrige Handlung (d.h. der Einsatz eines sich weiterverbreitenden Schadprogrammes) mit dem Angriff zusammenhängt oder darüber hinausgeht.[648] Dies muss allerdings jeweils im Einzelfall gewürdigt werden.[649] Grundsätzlich würde man einem Staat Völkerrechtsverletzungen jedoch zurechnen, wenn er private Unternehmen beauftragt, Cyberangriffe (als Angriff oder als Gegenmassnahme) gegen ein Computersystem eines anderen Staates zu lancieren und sich das betreffende Schadprogramm auf Systeme eines Drittstaats ausbreitet und diese beschädigt. Die Weiterverbreitung würde einem Staat angerechnet, da das Verhalten des Unternehmens mit dem beauftragten Cyberangriff zusammenhing, obwohl die Ausbreitung nicht Teil der Anweisungen war.[650] Anders wäre es, wenn ein Staat einen privaten Akteur instruiert, Schadprogramme in die staatlichen Netzwerke eines anderen Staates einzuschleusen und jener das Schadprogramm missbraucht, um

644 Siehe vorangehende Ausführungen zu R15 und 16 des Tallinn Manuals.

645 Tallinn Manual 2.0, S. 97 R17 C11.

646 Tallinn Manual 2.0, S. 98 R17 C13.

647 ARSIWA-Kommentar, Art. 8(7) f.; Tallinn Manual 2.0, S. 98 R17 C13.

648 Vgl. ARSIWA-Kommentar, Art. 8(8); Tallinn Manual 2.0, S. 98 R17 C13. Zu Schwierigkeiten bei der Zurechnung des Handelns staatlicher Organe: Dahm/Delbrück/Wolfrum, Bd. I/3, S. 890 ff.; Woltag, S. 89.

649 ARSIWA-Kommentar, Art. 8(7) f.; Tallinn Manual 2.0, S. 97 R17 C11.

650 Tallinn Manual 2.0, S. 98 R17 C12.

einen Drittstaat anzugreifen.[651] Letztere private Handlung würde dem Staat nicht angerechnet werden, da sie über die Befugnisse hinausgeht und keinen Bestandteil des eigentlichen Angriffs darstellt.[652]

Gemäss der Regel 17(b) des Tallinn Manuals 2.0 sollen analog zu Art. 11 ARSIWA private Handlungen einem Staat letztlich auch in dem Masse zugerechnet werden, in dem er sie als seine eigenen anerkennt.[653] Dies wurde im Teheraner Geiselfall als Gewohnheitsrecht anerkannt.[654] In jenem Fall hat der IGH entschieden, dass der Iran sich für das Festhalten von US-Geiseln zwischen 1979 und 1981 verantwortlich gemacht hat, indem iranische Regierungsvertreter die Geiselnahmen durch private Akteure offiziell billigten.[655] Der Standard ist dabei eng auszulegen; so müssen die Voraussetzungen der Anerkennung (»*acknowledgement*«) und der Annahme (»*adoption*«) kumulativ gegeben sein, wobei es mehr braucht als eine ledigliche Billigung oder stillschweigende Genehmigung.[656]

iii. Zwischenfazit

Grundsätzlich ist die Zurechnung von Cyberangriffen im Rahmen der Staatenverantwortlichkeit denselben rechtlichen Voraussetzungen unterworfen wie herkömmliche Verstösse[657], obschon sich neuartige Schwierigkeiten stellen. Für die rechtliche Zurechnung von Völkerrechtsverletzungen an einen Staat gem. den ARSIWA wird daher primär auf den Akteur hinter der Verletzungshandlung und dessen Nähe zum Staat abgestellt.[658] Politisch oder kriminell motivierte Handlungen Privater werden ohne staatliches Mitwirken den ARSIWA zufolge einem Staat i.d.R. daher nicht angerechnet. Für die Zurechnung privaten Handelns besteht zudem mit dem »*effective control*«-Ansatz des IGH eine hohe Hürde. Es wird eine enge Verbindung bzw. die effektive Kontrolle eines Staates in Bezug auf jede Handlung verlangt. Im Beispiel der DDoS-Cyberangriffe auf Estland 2007 hätte für die Zurechnung eines privaten

651 Tallinn Manual 2.0, S. 98 R17 C12.

652 Tallinn Manual 2.0, S. 98 R17 C12.

653 Tallinn Manual 2.0, S. 99, R17 C15 ff.

654 IGH, Teheraner Geiselfall, §74; Tallinn Manual 2.0, S. 99, R17 C15.

655 IGH, Teheraner Geiselfall, §74.

656 ARSIWA-Kommentar, Art. 11(6), (9); Tallinn Manual 2.0, S. 99, R17 C16 m.w.V.

657 Woltag, S. 89; Mikanagi/Mačák, S. 53. Im Ergebnis auch: Huang, S. 54. D'Aspremont, S. 592 argumentiert insb. aufgrund der Beweisschwierigkeiten im Cyberkontext für eine Reform der Zurechnungsnormen der Staatenverantwortlichkeit.

658 Mikanagi/Mačák, S. 60 ff.

Handelns die Kontrolle grundsätzlich über jeden einzelnen DoS-Angriff oder zumindest über die Streuung der Angriffe (z.B. mittels eines Kontrollsystems) vorliegen müssen. Indem u.a. eine unbekannte Anzahl Private mittels online-Anleitungen die betreffenden DDoS-Angriffe ausführen konnte, ist fraglich, ob eine effektive Kontrolle über jede einzelne Handlung möglich und ob die einzelnen Angriffe integrale Bestandteile des (Gesamt-)Angriffs waren. Da man davon ausgehen musste bzw. die verfügbaren Schadprogramme darauf ausgerichtet waren, dass diese durch Private ausgeführt würden, könnte man dies im Gesamtkontext jedoch annehmen. Allerdings nur, wenn die Angriffe auch nachweislich auf staatliche Instruktionen hin lanciert oder zur Verfügung gestellt wurden. Bei staatlichen Akteuren dagegen ist die rechtliche Zurechnung gem. ARSIWA extensiver. Es muss nicht jede Handlung im Einzelnen gewürdigt werden. Primär ist vielmehr die staatliche Funktion, in der Angriffe lanciert werden, ausschlaggebend.

Da in der Praxis die Akteurskonstellationen oft unübersichtlich und/oder gemischt sind, bleiben wesentliche Herausforderungen bestehen. Das heisst, man muss jeden komplexen Einzelfall würdigen. Staaten arbeiten nämlich teilweise nahe mit privaten Firmen zusammen, und eingesetzte Schadprogramme können (durch weitere Akteure) umprogrammiert und wiederverwendet werden. Hinzu kommt, dass die Reichweite potenzieller Schäden durch technologische Möglichkeiten wie einer (automatisierten) Weiterverbreitung von Computerwürmern wohl weiter zunehmen wird. Cyberangriffe können gleichzeitig von mehreren Staatsterritorien ausgehen und (unkontrolliert) in mehreren Staaten (schädigend) wirken. Damit stellen sich nicht nur Schwierigkeiten im Hinblick auf mögliche Organeigenschaften, sondern es verändern sich auch die Fragen des erforderlichen Kausalzusammenhangs. Es muss daher abgewogen werden, wie weit man für Folgeschäden in Drittstaaten Verantwortlichkeiten annehmen will – insb., wenn es sich um Staaten handelt, die nicht an geopolitischen Konflikten beteiligt sind. Einerseits sollte nach vorliegender Ansicht die Staatenverantwortlichkeit zurückhaltend angewendet werden, um Konflikte zwischen Urheberstaat und Drittstaaten möglichst zu vermeiden. Andererseits sollten Dritt- und Folgeschäden von Cyberangriffen, die von einem Staat in Auftrag gegeben oder »kontrolliert« werden, rechtlich erfasst werden können. Ähnliche Fragen stellen sich im Hinblick auf Due Diligence-Pflichtverletzungen (siehe nachfolgend unter III.B.2.c).

iv. Technische Beweisprobleme

Die im vorangehenden Abschnitt diskutierte völkerrechtliche Zurechnung von Normverletzungen gem. den ARSIWA ist begrifflich von einer politischen und technischen Zurechnung (meist als politische oder technische »Attribution« umschrieben) zu differenzieren.[659] Unter einer politischen Attribution wird eine politische Zurechnung verstanden, mittels derer ein anderer Staat öffentlich für ein Fehlverhalten verantwortlich gemacht wird, ohne dass dies zwangsläufig rechtliche Folgen hat.[660] Vielmehr soll dadurch Fehlverhalten signalisiert und politischer Druck aufgesetzt werden.[661] Bei der technischen Attribution geht es, basierend auf spezifischen technischen Indikatoren, um die Eruierung des Ursprungs eines Cyberangriffs. Diese wird oftmals durch IT-Experten und Sicherheitsfirmen durchgeführt. Die technische Attribution bei Cyberangriffen ist unerlässlich, um den Urheber ausfindig zu machen und nachzuweisen.[662] Ohne technischen Nachweis, dass ein bestimmter Akteur hinter einem Angriff steht, kommt folglich auch die eine Verantwortlichkeit begründende rechtliche Zurechnung an einen Staat an ihre Grenzen.[663] Die technische Beweisbarkeit ist somit zentral für die Bejahung rechtlicher Verantwortlichkeiten.[664] Allerdings stellen sich im Cyberkontext, wie bereits erwähnt, erhebliche (technische) Beweisschwierigkeiten, um staatliche und nichtstaatliche Akteure hinter Angriffen zu identifizieren.[665] Die weitreichende Anonymität bei Cyberangriffen stellt eine erhebliche Herausforderung beim Ausfindigmachen eines Urhebers sowie eines verantwortlichen Territoriums dar.[666] Gerade bei DDoS-Angriffen, die von breiten Botnetzen ausgehen und teilweise willkürliche IP-Adressen als Brückenkopf verwenden, ist es schwierig, mit Sicherheit festzustellen, wer der tatsächliche Urheber eines Angriffs

659 Mikanagi/Mačák, S. 53 Fn. 9 m.V.a. Huang, S. 43.

660 Broeders/De Busser/Pawlak, S. 9 ff. m.w.V.; Egloff/Wenger, S. 1.

661 Siehe z.B. in: US National Cyber Strategy 2018, S. 21. Zu diesbezüglichen Beispielen nachfolgend unter IV.B.2.e).

662 Roguski, S. 13.

663 Harrison Dinniss, S. 99 ff.; Walter, S. 687; Woltag, S. 28 ff., S. 87. Eingehender zur Rückverfolgungsproblematik: Schulze, S. 36 ff.

664 Lahmann, S. 262; Wilmshurst et al., S. 968.

665 Eingehender zur Schwierigkeit, Angriffe einem Staat nachzuweisen anhand eines konkreten Falles: Mikanagi/Mačák, S. 52 ff. Ferner zur Anonymität: Goldsmith, S. 136.

666 Lahmann, S. 262.

ist.[667] Im Cyberkontext ist es zudem oft nicht möglich, ohne die Kooperation des potenziell verantwortlichen Staates die rechtlich relevanten Beweise zu erlangen.[668]

Des Weiteren enthalten Schadprogramme meist keine Hinweise auf den Urheber, und sollten sie solche enthalten, können sie gefälscht sein.[669] Somit können sich staatliche Akteure hinter vermeintlich privaten Urhebern verstecken und private Akteure können Angriffe von staatlichen Infrastrukturen aus lancieren.[670] Die involvierten Akteure können also (willentlich) den Anschein erwecken, dass ein bestimmter Staat oder eine Gruppe hinter einem Angriff steht.[671] Dies könnte durch falsch ausgerichtete Gegenangriffe zu Konflikten und politischen Spannungen führen, während die wahren Urheber unbekannt bleiben. Das Tallinn Manual 2.0 erwähnt etwa das Beispiel, in dem 2013 Cyberangriffe darauf hindeuteten, dass das NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) offizielle ukrainische Webseiten manipuliert hätte. Auf diese Angriffe folgten vermeintliche Gegenangriffe von ukrainischen Regierungs-IP-Adressen auf die Webseiten der NATO CCDCOE, die estnischen Verteidigungskräfte und das Militär weiterer NATO-Staaten.[672] Experten vermuteten aber, dass es sich weder bei den IP-Adressen im Rahmen der Angriffe auf die Ukraine noch auf die Webseite der NATO CCDCOE um die wahren Urheber handelte.[673]

Angesichts der schwierigen technischen Attribution kann man festhalten, dass eine rechtliche Zurechnung von Cyberangriffen zu einem Staat nach den völkerrechtlichen Massstäben sehr schwierig ist. So werden im Hinblick auf zeitnahe Nachweise staatlicher Organeigenschaft oder *de facto*-Organeigenschaft bei spezifischen Angriffen regelmässig Unsicherheiten bestehen bleiben.[674] Ähnlich wird man auch die bei privaten Akteuren hochangesetze, effektive Kontrolle eines Staates über Cyberangriffe nur schwer technisch beweisen

667 Evron, S. 121 ff, insb. S. 123 f.; Harrison Dinniss, S. 100; Tikk/Kaska/Vihul, S. 23. Ähnlich: Tallinn Manual 2.0, S. 91 R15 C14.

668 Mikanagi/Mačák, S. 67. Ferner: Brunner/Dobrić/Pirker, S. 102 ff.

669 Heckman et al., S. 72 ff.

670 Vgl. Tallinn Manual 2.0, S. 91 R15 C13 ff.

671 Tallinn Manual 2.0, S. 91 R15 C15.

672 Tallinn Manual 2.0, S. 91 R15 C15.

673 Tallinn Manual 2.0, S. 92 R15 C15. Eingehender zu den unübersichtlichen Urheberkonstellationen bei den Cyberangriffen i.Z.m. dem Ukraine-Konflikt um 2013: Baezner/Robin, Information Warfare, S. 11 ff.

674 Mikanagi, S. 1026; Schulze, S. 141 f.

können.[675] Für eine erfolgreiche Beweiserbringung werden daher neben technischen auch weitere, für den Gesamtkontext relevante Aspekte wie die geopolitischen Umstände berücksichtigt werden müssen.[676] Hinsichtlich des insgesamt für die rechtliche Zurechnung erforderlichen Beweismasses besteht dabei Klärungsbedarf. Das erforderliche Beweismass für eine erfolgreiche Zurechnung im Kontext der Staatenverantwortlichkeit ist explizit nicht Gegenstand der ARSIWA,[677] und internationale Gerichte vertreten diesbezüglich unterschiedliche Ansätze.[678] So gibt es im Gegensatz zum sog. »*beyond reasonable doubt*«-Standard internationaler Straftribunale[679] keine klaren Beweiskriterien seitens des IGH.[680] Obschon gewisse Tendenzen zu verzeichnen sind,[681] besteht daher weiterhin Klärungsbedarf hinsichtlich des für die Zurechnung erforderlichen Beweismasses, den dabei zu berücksichtigenden Faktoren sowie dahingehend, ob eine Pflicht besteht, bei der (politischen oder rechtlichen) Zurechnung Beweise erbringen zu müssen.[682] Dies ist jedoch Gegenstand anderweitiger Debatten und soll vorliegend nicht weiter ausgeführt werden.[683] Grundsätzlich sind jedoch all jene Cyberangriffe, bei denen die erforderliche

675 Mikanagi, S. 1026; Schulze, S. 142.

676 Mikanagi, S. 1026. Baezner/Robin, Information Warfare, S. 11 verweisen für die Zurechnung auf die *cui bono*-Logik, bei der es um die Würdigung des jeweils erlangen (politischen) Vorteils hinter Angriffen geht. Ferner: Tallinn Manual, S. 92 R15 C16.

677 Mikanagi/Mačák, S. 64 m.V.a. ARSIWA-Kommentar, Kapitel III(4) und ARSIWA-Kommentar, Kapitel V(8).

678 Dazu m.w.V.: Mikanagi/Mačák, S. 64 ff. Eingehend zu den unterschiedlichen Beweismassen der Attribution: Broeders/De Busser/Pawlak.

679 Reflektiert im Art. 66 des Römer-Statuts des Internationalen Strafgerichthofs. Zu den unterschiedlichen Funktionen verschiedener Zurechnungsstandards: Jacobs, S. 1143.

680 Mikanagi/Mačák, S. 64; Teitelbaum, S. 124; Riddell/Plant, S. 125 f.; Roscini, Evidentiary Issues, S. 227. Ähnlich: Kerschischnig, S. 305.

681 Mikanagi/Mačák, S. 65 m.V.a. Benzing, S. 1382, S. 1403; Brunner/Dobrić/Pirker; Gattini, S. 889 ff.; Riddell/Plant, S. 80, S. 123. Dazu auch: Roscini, Evidentiary Issues, S. 227 ff.

682 Roguski, S. 14 mit der Frage, ob es eine Pflicht gibt, Beweise zu erbringen, wenn ein Cyberangriff öffentlich an einen Staat (politisch) attribuiert wird. Zu den Unklarheiten des rechtlichen Beweismasses im Kontext der Selbstverteidigung und der Staatenverantwortlichkeit: Lahmann, S. 70 ff. und S. 79 ff. Schmitt ist hingegen der Ansicht, dass »*reasonable certainty*« ausreichend ist, um (auch fälschlich ausgerichtete) Gegenmassnahmen zu rechtfertigen: Schmitt, Countermeasures Response Option, S. 727. Allerdings bestätigt er, dass eine nicht genügend begründete Würdigung eines Verstosses einen reagierenden Staat selbst verantwortlich machen kann: S. 726.

683 Das Konzept der Attribution und die damit verbundenen Schwierigkeiten im Cyberkontext haben generell bereits zu Debatten geführt: Tsagourias, S. 229 ff.; Jensen, Tallinn Manual 2.0, S. 750 u.a. m.V.a. Newman, Wired vom 24.12.2016.

Organeigenschaft oder die hohe Schwelle der effektiven Kontrolle nicht gegeben oder nicht nachgewiesen werden können, aus rechtlicher Sicht einem Staat nicht zurechenbar. Für solche Cyberangriffe würden folglich keine völkerrechtlichen Verantwortlichkeiten für Staaten begründet. Solange also aufgrund von Beweis- und Rückverfolgungschwierigkeiten keine völkerrechtlichen Verantwortlichkeiten und dadurch keine Rechtsfolgen ausgelöst werden können, werden Völkerrechtsnormen wie das Interventionsverbot wohl wenig Wirkung entfalten können.[684] Angesichts dieser Zurechungsschwierigkeiten ist gem. SCHULZE über alternative Ansätze nachzudenken.[685] In diesem Zusammenhang wird in der Lehre verschiedentlich die zunehmende Bedeutung von Due Diligence-Normen im Cyberkontext betont.[686] MIKANAGI/MAČÁK sehen Due Diligence als einen möglichen Alternativweg zur völkerrechtlichen Zurechnung, um rechtliche Verantwortlichkeiten von Staaten etablieren zu können (dazu näher sogleich unter III.B.2.c).[687]

v. Zunahme von Akteuren ohne klares Haftungssubstrat

Wie vorangehend erläutert, werden staatliche Verantwortlichkeiten für Völkerrechtsverstösse grundsätzlich nicht für private Handlungen begründet,[688] ausser die Voraussetzungen einer effektiven Kontrolle oder der genannten Zurechnungsmöglichkeiten gem. den ARSIWA sind gegeben.[689] Demgemäss gelten das Gewalt- und Interventionsverbot grundsätzlich nur für Staaten und ihnen zurechenbare Akteure.[690] Aus völkerrechtlicher Sicht problematisch ist also, dass im Cyberraum der Radius an Akteuren zunimmt, die ohne klares Haftungssubstrat handeln.[691] Gleichzeitig können für einen angegriffenen Staat die auf seinen *domaine réservé* wirkenden Effekte dem Zwang einer Interventionsverbotsverletzung gleichkommen, auch wenn diese Angriffe von nichtstaatlichen Akteuren lanciert werden. Dies wäre bspw. der Fall, wenn private Gruppierungen politische Prozesse zwangsmässig beeinflussen und ma-

684 JENSEN, Tallinn Manual 2.0, S. 778.

685 SCHULZE, S. 142.

686 MIKANAGI/MAČÁK, S. 71 ff.; JENSEN, Tallinn Manual 2.0, S. 778.

687 MIKANAGI/MAČÁK, S. 71 ff. Ähnlich: DELERUE, Cyber Operations, S. 374, der Due Diligence als mögliches »Palliativ« zur Attributionsproblematik sieht.

688 DIGGELMANN/HADORN, S. 270; SEIBERT-FOHR, S. 40 ff.

689 ARSIWA-Kommentar, insb. Art. 8; DIGGELMANN/HADORN, S. 269 f.; DÖRR, S. 642 ff., insb. S. 653; SCHULZE, S. 55; WOLF, S. 62 f.

690 TIKK/KASKA/VIHUL, S. 32.

691 DIGGELMANN/HADORN, S. 269. Ähnlich im Kontext anderer transnationaler Schädigungsmöglichkeiten durch Private wie z.B. durch private Unternehmen: SEIBERT-FOHR, S. 39.

nipulieren. Letzteres Phänomen wird insb. unter dem Stichwort des »patriotischen Hackings« diskutiert.[692] Patriotisches Hacken ist darauf ausgerichtet, politische Ziele zu verfolgen, indem Druck auf Autoritäten ausgeübt oder die Öffentlichkeit beeinflusst wird.[693]

Da privat lancierte und keinem Staat zurechenbare Cyberangriffe nicht unter das Völkerrecht fallen, wären diese grundsätzlich vor dem Hintergrund regulärer Cyberkriminalität zu betrachten.[694] Das für Cyberkriminalität einschlägige internationale Regelwerk ist die Budapest-Konvention von 2001,[695] deren Wortlaut relativ offen formuliert ist und motivationsneutral interpretiert werden kann.[696] Der primäre regulatorische Fokus der Budapest-Konvention ist laut TIKK/KASKA/VIHUL allerdings auf ökonomisch motivierte Angriffe gerichtet, wie bspw. Angriffe auf private Unternehmen mit dem Ziel von Lösegeldforderungen.[697] Damit sei unklar, inwiefern und wie Cyberkriminalitätsnormen politisch motivierte Angriffe erfassen. Dieser Betrachtungsweise von TIKK/KASKA/VIHUL zufolge bewegen sich patriotische Hacker daher in rechtlichen Graubereichen, da sie weder im Völkerrecht noch im Strafrecht im regulatorischen Fokus sind.[698] TIKK/KASKA/VIHUL sprechen sich folglich dafür aus, dass die Rechtslage geklärt werden und patriotische Hacker unter nationale und internationale Strafrechtsnormen fallen sollen, da von ihnen ein Schädigungspotenzial für Gesellschaft, Sicherheit und die öffentliche Ordnung ausgehe.[699] Im Hinblick auf die Erfassung nichtstaatlicher Akteure, die innere Angelegenheiten von Staaten beeinflussen ohne die Verantwortlichkeit eines Staates zu begründen, besteht somit grundsätzlicher Klärungsbedarf.[700] Denn

692 BUSSOLATI, S. 104 ff.; TIKK/KASKA/VIHUL, S. 31 f. m.H.

693 TIKK/KASKA/VIHUL, S. 31.

694 TIKK/KASKA/VIHUL, S. 32.

695 Siehe Abkürzungsverzeichnis.

696 TIKK/KASKA/VIHUL, S. 32. Gemäss HINKLE geht die Konvention von einem ähnlichen Grundgedanken wie das Interventionsverbot aus und verbietet illegale Systembeeinträchtigungen unabhängig der Motive. Unabhängig davon, wie man die Konvention interpretiert, kommt es bei der strafrechtlichen Erfassung von Cyberangriffen letztlich auf die Umsetzung der Mitgliedstaaten an. Die Normen der Budapest-Konvention verpflichten die Staaten, nationale Regelungen aufzustellen und verweisen somit jeweils auf die nationalen Regime. Siehe HINKLE, S. 16.

697 TIKK/KASKA/VIHUL, S. 31 f.

698 TIKK/KASKA/VIHUL, S. 32.

699 TIKK/KASKA/VIHUL, S. 32.

700 Dazu, dass gerade Vorfälle wie diejenigen in Estland aufzeigten, dass strafrechtliche Normen und Kooperationen im Cyberkontext gestärkt werden sollen: TIKK/KASKA/VIHUL, S. 28 ff.

solange privates Handeln nicht einem Staat zurechenbar ist, wird man auf nationale und internationale (Straf-)Rechtsgrundlagen zurückgreifen müssen. Obschon international keine grundsätzliche Pflicht besteht, spezifische nationalrechtliche Normen zu etablieren, könnten solche Normen u.U. auf ein völkerrechtskonformes Verhalten vor dem Hintergrund der Due Diligence-Pflicht hinweisen (siehe sogleich unter c)).[701]

c. Völkerrechtliche Sorgfaltspflicht (Due Diligence)

i. Grundidee der völkerrechtlichen Due Diligence

Gemäss der historisch gewachsenen, völkerrechtlichen Sorgfaltspflicht (sog. Due Diligence) sind Staaten grundsätzlich verpflichtet, sicherzustellen, dass ihr Territorium nicht für Zwecke genutzt wird, die die Rechte anderer Staaten verletzen.[702] Für einen Staat können dieser Sorgfaltspflicht zufolge indirekte Verantwortlichkeiten entstehen, wenn er von seinem Territorium ausgehende, schädigende Aktivitäten nicht verhindert.[703] Es geht um eine grundsätzlich als Gewohnheitsrecht anerkannte[704] Pflicht eines Staates, mit der den Umständen nach gebotenen Sorgfalt Verletzungen fremdstaatlicher Rechte,[705] von denen er Kenntnis hat, vom eigenen Territorium aus zu verhindern.[706] Für das Bestehen dieser Sorgfaltspflicht zentral ist das wegweisende Urteil des IGH im Korfu Kanal-Fall von 1949, das diese umschreibt als: »*every State's obligation*

701 Woltag, S. 110. Ähnlich: Sklerov, S. 62.

702 Delerue, Cyber Operations, S. 353 m.w.V.; Coco/Dias, S. 771 ff.; Mikanagi/Mačák, S. 71 u.a. m.V.a. ILA Study Group on Due Diligence 2016, S. 5 f.; Schmitt, Grey Zones, S. 11; Schulze, S. 142 ff.; Wolf, S. 462 ff.

703 Woltag, S. 95 m.w.V.

704 Gemäss Schulze, S. 143 handelt es sich um eine völlkergewohnheitsrechtliche Pflicht wohingegen Woltag eine gewohnheitsrechtliche Etablierung ablehnt und von einem generellen Rechtsprinzip ausgeht: Woltag, S. 110. Gemäss Crawford, State Responsibility, S. 217 ff. und S. 226 ff. lässt sich eine Verhinderungspflicht für Staaten aus Art. 23 der Draft Articles von 1996 und des späteren Art. 14(3) ARSIWA (i.V.m. Art. 2 ARSIWA; siehe ARSIWA-Kommentar, Art. 2(4) ableiten; vgl. ARSIWA-Kommentar, Art. 14(14). Das Konzept war zudem Gegenstand einer Reihe von Schieds- und Gerichtsentscheiden vor dem IGH oder dem ITLOS. Eingehender dazu: Peters/Krieger/Kreuzer, Dissecting the Leitmotif, S. 1 m.w.V.

705 Dabei sind das nationale Recht verletzende Handlungen wie transnationale Cyberkriminalität grundsätzlich nicht umfasst. Solche Handlungen sind Gegenstand von Vereinbarungen für Strafverfolgungskooperationen: Tallinn Manual 2.0, S. 34 R6 C15, ferner S. 75 ff. R13.

706 Schulze, S. 143.

not to knowingly allow its territory to be used for acts contrary to the rights of other States.«[707] In jenem Fall wurden in den albanischen Küstengewässern mit hoher Wahrscheinlichkeit mit Wissen der albanischen Behörden durch (mutmasslich) Private Minen gelegt, durch die britische Schiffe beschädigt wurden und britische Seeleute ums Leben kamen.[708] Albanien hatte es gem. IGH versäumt, Drittstaaten vor den in ihren Gewässern befindlichen Minen zu warnen und sich dadurch verantwortlich gemacht.[709] Der IGH sah die pflichtwidrige Unterlassung darin, dass Albanien die zumutbaren Verhinderungsmöglichkeiten wissentlich nicht wahrgenommen hatte.[710] Die Kenntnis über die Verletzungen durch die betreffenden Aktivitäten stellt ein für die Begründung der Pflicht konstitutives Element dar.[711] Die Auseinandersetzung des IGH mit sorgfaltsrechtlichen Fragen bei einer Verletzung durch Unterlassen im Korfu Kanal-Fall hatte einen wesentlichen Einfluss auf den späteren (und auch gegenwärtigen) Umgang mit sorgfaltspflichtsrechtlichen Fragen bei transnationalen Schädigungen.[712] Gerade bei transnationalen Phänomenen wie Cyberangriffen, globalen Umweltverschmutzungen oder terroristischen Akten werden solche völkerrechtlichen Konstellationen wohl weiter an Relevanz gewinnen.[713]

Im Grunde geht es um eine sorgfaltspflichtsrechtliche Unterlassung[714] eines Staates, die bei erfolgreicher Zurechnung Gegenmassmahmen rechtfertigen kann.[715] Rechtlich wird eine Unterlassung nur dann relevant, wenn eine Pri-

707 IGH, Korfu Kanal-Urteil, S. 22. Dieser Grundsatz ist in weiteren Entscheiden widerspiegelt. Siehe u.a.: IGH, Bosniengenozid-Urteil, §430; IGH, Nuklearwaffen-Gutachten, §29; (unter Bezugnahme auf das Korfu Kanal-Urteil) IGH, Zellstofffabriken-Fall, §101; IGH, Grenzgebiets- und San Juan Strassenbau-Urteil, §104, §153, §168. Zum Bestehen dieser Sorgfaltspflicht u.a.: Dörr, S. 653 f. (unter expliziter Erwähnung von Schutz- und Verhinderungspflichten in Bezug auf Schädigungen durch die Nutzung von Computersystemen); Fitzmaurice, S. 138 f.; Mikanagi, S. 1022 ff.; Woltag, S. 103 je m.w.V.

708 IGH, Korfu Kanal-Urteil; Diggelmann/Hadorn, S. 270. Ausführlicher zum erforderlichen Beweismass für die Unterlassung gem. IGH: Del Mar, S. 98 ff.

709 IGH, Korfu Kanal-Urteil, S. 22 f.; Crawford, State Responsibility, S. 218.

710 Fitzmaurice, S. 136; Woltag, S. 105.

711 IGH, Korfu Kanal-Urteil, S. 22; Tallinn Manual 2.0, S. 40 R6 C37.

712 Siehe dazu u.a.: Dupuy/Hoss, S. 225 ff.; Heathcote, State Omissions, S. 295 ff.

713 Zu einer eingehenden Abhandlung der Bedeutung der Due-Diligence in den verschiedenen Bereichen: Krieger/Peters/Kreuzer.

714 Crawford, State Responsibility, S. 217 f.; Tallinn Manual 2.0, S. 43 R7 C2; Woltag, S. 95.

715 Schmitt, Grey Zones, S. 11.

märpflicht missachtet wird.[716] Die für Sorgfaltspflichten relevante Intensität, die Art der erforderlichen Schädigung sowie die konkreten Pflichten sind im Einzelnen allerdings umstritten[717] und variieren je nach Kontext.[718] Die Rolle und die Funktion (und daher die Schutzausrichtung) der Due Diligence unterscheiden sich somit von Regime zu Regime.[719] Trotz der vermeintlichen Ähnlichkeit des Prinzips in verschiedenen Völkerrechtsbereichen hat es im Einzelnen verschiedene Ausrichtungen: Im Bereich der Menschenrechte geht es bspw. um Minimalerfordernisse und die Konturen von positiven Schutzpflichten von Staaten, die anhand von (privaten vs. öffentlichen) Interessenabwägungen (unter Berücksichtigung der Verhältnissmässigkeit) abgewogen werden.[720] Im internationalen Wirtschaftsrecht hingegen geht es bspw. um sorgfaltspflichtsrechtliche Risikominimierungen, indem rechtliche, umweltbezogene und/oder soziale Abklärungen getätigt werden müssen, um transnationale Schädigungen zu vermeiden.[721] In dieser Dissertation ist für die von Cyberangriffen ausgehenden Risiken insb. das Konzept des Korfu Kanal-Urteils und damit die Verhinderung transnationaler Verletzungen *fremdstaatlicher Rechte* massgebend. In diesem Kontext geht es grundsätzlich um Rechte, zu deren Beachtung ein Staat gegenüber einem anderen Staat verpflichtet ist.[722] So ist ein Staat bspw. verpflichtet, nicht zwangsweise in die inneren Angelegenheiten eines anderen Staates zu intervenieren oder diesen gewaltsam zu schädigen.[723]

Eine Verantwortlichkeit durch pflichtwidriges Unterlassen gem. dem Due Diligence-Prinzip ist analytisch von der völkerrechtlichen Zurechnung staatlichen oder privaten Handelns an einen Staat gem. Art. 4–11 ARSIWA zu unterscheiden.[724] Obschon Verletzungen (durch Cyberangriffe bspw.) im Einzelfall völker-

716 Crawford, State Responsibility, S. 218; Crawford, Brownlie's Principles, S. 541. Due Diligence ist grundsätzlich jeweils an eine Primärnorm gebunden: Tallinn Manual 2.0, S. 32 R6 C6. Allerdings kann Due Diligence nicht nur als Sekundär-, sondern auch als Primärnorm relevant werden: Peters/Krieger/Kreuzer, Dissecting the Leitmotif, S. 6 ff.

717 Tallinn Manual 2.0, S. 36 R6 C25 m.V.a. den Trail-Smelter-Schiedsspruch, S. 1963. Dazu u.a. auch: Jensen, Tallinn Manual 2.0, S. 744.

718 Peters/Krieger/Kreuzer, Risk Management Tool, S. 138 ff.

719 Peters/Krieger/Kreuzer, Risk Management Tool, S. 132.

720 Peters/Krieger/Kreuzer, Risk Management Tool, S. 132.

721 Peters/Krieger/Kreuzer, Risk Management Tool, S. 133.

722 Tallinn Manual 2.0, S. 34 R6 C15.

723 Die Experten im Tallinn Manual einigten sich darauf, dass sich eine Sorfgaltspflicht generell auf den Anwendungsbereich von Völkerrechtsverletzungen (»*internationally wrongful acts*«) bezieht: Tallinn Manual 2.0, S. 34 R6 C17.

724 ARSIWA-Kommentar, Kapitel II (4); Hessbruegge, S. 265 ff.; Woltag, S. 96.

rechtlich einem Staat nicht gem. ARSIWA zugerechnet werden können, kann dennoch eine Verantwortlichkeit für diesen resultieren, wenn die betreffenden Angriffe von seinem Territorium aus einen anderen Staat schädigen und er dies wissentlich nicht mit den ihm zumutbaren Mitteln verhindert.[725] Dies ist mitunter ein Grund, weshalb Due Diligence, wie bereits vorangehend erwähnt, oftmals als möglicher Alternativweg zur völkerrechtlichen Zurechnung gem. ARSIWA gesehen wird.[726]

ii. Cyberangriffe und Due Diligence

Die Frage, ob eine völkerrechtliche Due Diligence-Pflicht im Cyberkontext gilt, ist innerhalb der Staatengemeinschaft umstritten.[727] Einige Staaten verkennen eine solche Pflicht, vereinfacht gesagt, mit dem Argument, dass der Cyberraum eine neue Domäne sei, für die eine solche Pflicht erst noch etabliert werden müsse.[728] Die UN GGE 2013 und 2015 haben durch ihre Umschreibung in §13(c) »*States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*« immerhin anerkannt, dass eine solche Sorgfaltspflicht zwischen Staaten bestehen soll.[729] Dabei, und dies ist zu betonen, lehnen sich die als nicht-bindend qualifizierten[730] Formulierungen bewusst oder unbewusst (bzw. laut Akande/Coco/Dias explizit oder implizit) an diejenige des IGH im Korfu Kanal-Fall an.[731] Die Experten des Tallinn Manu-

725 Roscini, Cyber Operations, S. 40; Schulze, S. 143; Woltag, S. 110.

726 Delerue, Cyber Operations, S. 374; Mikanagi/Mačák, S. 71 ff.

727 Siehe: Schmitt, Grey Zones, S. 11, der darauf verweist, dass gewisse Staaten die Anwendbarkeit der Due Diligence im Cyberraum ablehnen. Zu verschiedenen Ansichten ausgewählter Staaten zur Due Diligence siehe auch: Roguski, S. 11 f. Das Vereinigte Königreich und die USA sind gem. Roguski Beispiele, die das Due Diligence-Prinzip im Cyberkontext nicht anerkennen. Sklerov, S. 62 z.B. sieht eine solche Verhinderungspflicht im Cyberbereich als gewohnheitsrechtlich anerkannt. Einige Staaten sprechen sich für die Anwendung des Prinzips aus: Siehe: UN Doc. A/76/135 (2021), u.a. (Schweiz) S. 91, (Japan) S. 48, (Niederlande), S. 59.

728 So bspw. die Argumentationsweise Israels und Neuseelands. Siehe dazu: Akande/Coco/Dias, EJIL Blog vom 05.01.2021.

729 UN Doc. A/RES/68/98 (2013), §20; UN Doc. A/RES/70/174 (2015), §13(c) bzw. §27, §28(e). Ähnlich in: OEWG, finaler Bericht vom 10.03.2021, §31. Die Experten im Tallinn Manual erachten die Umschreibung »*should*« als *lex ferenda* widerspiegelnd: Tallinn Manual 2.0, S. 31 R6 C3.

730 Im UN GGE 2015 Rapport wird die betreffende Bestimmung als Empfehlung und in dem Sinne als nicht-bindende Norm verstanden: UN Doc. A/RES/70/174 (2015), §13(c), ferner §13(f).

731 Akande/Coco/Dias, EJIL Blog vom 05.01.2021. Ähnlich: Mikanagi/Mačák, S. 71.

als 2.0 hingegen anerkennen eine sorgfaltspflichtsrechtliche Verantwortung eines Staates als *lex lata*, wenn schädigende Cyberangriffe von in seiner Hoheitsgewalt[732] oder in seinem Territorium befindendlichen Cyberinfrastukturen ausgehen.[733] Der Staat müsse, wenn es ihm (technisch) möglich sei, einschreiten, wenn er von den jeweiligen Cyberaktivitäten Kenntnis hat.[734] Welche Handlungen von welchem Staat dabei konkret erforderlich sind, um schädigende Handlung zu unterbinden, bleibt es dabei im betreffenden Fall zu würdigen.[735]

Gemäss Tallinn Manual handelt es sich grundsätzlich allerdings um die verfügbaren und zumutbaren Mittel innerhalb der souveränen Vorrechte, die ein vernünftig handelnder Staat unter den gleichen oder ähnlichen Umständen einsetzen würde.[736] Dies hängt im Grunde von der (technischen) Aufstellung des betreffenden Staates ab: das heisst den ihm intellektuell und finanziell verfügbaren Ressourcen und den institutionellen Möglichkeiten, Massnahmen zu ergreifen oder die Kenntnis über schädigende Aktivitäten in seinen Cyberinfrastrukturen zu haben.[737] Beispielsweise ist es einem Staat grundsätzlich möglich, IP-Adressen, von denen für einen anderen Staat schädigende Cyberangriffe ausgehen, (zumindest indirekt via Anweisung des betroffenen privaten Netzwerkanbieters) zu blockieren.[738] Andererseits wird es einem Staat wohl weniger möglich sein, auf komplexe und dynamische Cyberangriffe zu reagieren, die (mitunter) von seinem Territorium ausgehen.[739]

Im Rahmen der Due Diligence stellt sich eine wesentliche Herausforderung gerade in der schwierigen Lokalisierbarkeit von Cyberangriffen. Cyberangriffe gehen i.d.R. nicht klar von einem Territorium aus, sondern durchqueren mittels verschiedener Netzwerkknoten meist mehrere Staatsterritorien oder gehen gar von mehreren Territorien gleichzeitig aus. Eine sich in Staat C befindende Hackergruppe kann einen Cyberangriff von Staat A auf Staat B

732 Das Tallinn Manual anerkennt eine extraterritoriale Verantwortlichkeit, wenn sich staatliche Cyberinstrastrukturen ausserhalb des Territoriums befinden, die er kontrolliert: Tallinn Manual 2.0, S. 33 R6 C9 ff. Ferner auch: Tallinn Manual 2.0, S. 31 R6 C3.

733 Tallinn Manual 2.0, S. 30 R6. Dazu auch: MIKANAGI/MAČÁK, S. 72; SCHMITT, Grey Zones, S. 11.

734 Tallinn Manual 1.0, S. 28 R5 C10; Tallinn Manual 2.0, S. 43 R7 C1; näher dazu u.a. auch HEINTSCHEL VON HEINEGG, Territorial Sovereignty, S. 7 ff.; WOLTAG, S. 110.

735 Tallinn Manual 2.0, S. 43 R7 C1, S. 46 R7 C12.

736 Tallinn Manual 2.0, S. 47 R7 C16.

737 Tallinn Manual 2.0, S. 47 R7 C16. Siehe dazu z.B. IGH, Bosniengenozid-Urteil, §430 f.; IGH, Teheraner Geiselfall, §63 ff.; IGH, Kongo-Urteil, §301.

738 Tallinn Manual 2.0, S. 47 R7 C16.

739 Tallinn Manual 2.0, S. 47 R7 C17.

lancieren, indem sie sich in dessen Cyberinfrastrukturen hackt[740] oder Schadprogramme physisch vor Ort einschleust (Bsp. Stuxnet). Gemäss SCHULZE beschränkt sich dabei die Verhinderungspflicht auf den Staat, von dem der Cyberangriff ursprünglich ausgeht (im Beispiel wäre dies Staat C). Demzufolge würden Drittstaaten (hier Staat A), durch deren Netzwerkinfrastruktur Angriffe lanciert oder weitergeleitet werden, nicht für Verletzungen verantwortlich.[741] Die Experten des Tallinn Manuals sehen dies anders: Ihrer Ansicht nach verletzt ein Drittstaat (wie Staat A) ebenfalls das Due Diligence-Prinzip, wenn er über eine pflichtwidrige Nutzung seiner Infrastrukturen Bescheid weiss und keine ihm verfügbaren Mittel ergreift, um die schädigenden Aktivitäten (und somit die Verletzung) zu stoppen.[742] Staat C beginge laut Tallinn Manual, wenn ihm das Handeln der Hackergruppe als staatliches Handeln gem. den ARSIWA zuzurechnen ist, die Verletzung direkt – und nicht durch Unterlassen.[743] Demzufolge würde die Frage einer Verantwortlichkeit (von Transitstaaten) grundsätzlich auch eine allfällige Weiterverbreitung von kompromittierten Infrastrukturen aus betreffen, mittels der weitere Staaten beschädigt werden können. Die Expertengruppe des Manuals diskutierte auch den Fall, in dem Cyberangriffe lediglich durch einen anderen Staat durchgehen (z.B. via Glasfaserkabel) und nicht von spezifischen Cyberinfrastrukturen dieses Staates aus lanciert werden. Sie einigten sich darauf, dass strikt rechtlich gesehen auch ein Transitstaat an das Due Diligence-Prinzip gebunden sei, wenn er erstens Kenntnis von den durchlaufenden Cyberangriffen hat, die die erforderliche Intensität einer Völkerrechtsverletzung aufweisen, und zweitens ihm adäquate Massnahmen zur Verfügung stehen, um die verletzenden Angriffe zu stoppen.[744] Dabei geht es nicht um eine absolute Verhinderungspflicht, sondern jeweils um das Ergreifen angemessener, verfügbarer Beendigungsmassnahmen.[745]

Eine weitere Schwierigkeit ist im Rahmen der Due Diligence die Frage, ab wann man überhaupt von der Kenntnis eines Staates ausgehen bzw. diese erwarten kann. Die meisten Cyberangriffe – neben DDoS-Angriffen – bleiben, wie bereits erwähnt, oft (lange) unbemerkt in einem Computersystem und

740 Tallinn Manual 2.0, S. 32 R6 C8.

741 SCHULZE, S. 144.

742 Tallinn Manual 2.0, S. 32 R6 C8.

743 Tallinn Manual 2.0, S. 42 R6 C 44 f.

744 Tallinn Manual 2.0, S. 33 R6 C13.

745 Ausführlicher dazu: Tallinn Manual 2.0, S. 43 ff. R7, insb. S. 45 R7 C7 f. m.V.a. IGH, Bosnien-genozid-Urteil, §431.

werden verschlüsselt übertragen.[746] Rechtlich wird die Kenntnis nicht bereits durch den Fakt angenommen, dass ein Cyberangriff vom eigenen Territorium ausgeht.[747] Man muss von der in den Umständen geboteten Sorgfalt des Einzelfalles ausgehen.[748] Die Experten im Tallinn Manual nehmen das Wissen um einen schädigenden Cyberangriff an, wenn der Staat nach dem natürlichen Verlauf der Dinge objektiv gesehen von diesem hätte wissen müssen. Als Beispiel werden öffentlich bekannte Schadprogramme, technische Sicherheitslücken (z.B. die 2014 entdeckte Sicherheitslücke »*Heartbleed*«) und DDoS-Angriffe erwähnt, da über diese eine grundsätzliche Kenntnismöglichkeit bestehe.[749] Die Kenntnis über von einem Territorium ausgehende Schädigungen und Schadprogramme ist grundsätzlich auch bei einer Notifizierung des betreffenden Staates[750] oder bei einem zwischenstaatlichen Informationsaustausch anzunehmen. Eine komplette Überwachung der eigenen Infrastrukturen ginge allerdings zu weit[751] und würde insb. nicht zu jedem nationalen Rechtssystem passen. Solche Massnahmen müssen nämlich jeweils mit den weiterhin geltenden, nationalen und internationalen Individualrechten abgewogen werden.[752] Eine generelle präventive Verhinderungspflicht wird, wie bereits erwähnt, auch von den Experten des Tallinn Manuals abgelehnt.[753] Die Expertengruppe hielt dabei z.B. im Zusammenhang mit Transitstaaten fest, dass es generell sehr unwahrscheinlich sei, dass diese Kenntnis über in ihrem Territorium befindliche Kabel durchquerende Cyberangriffe haben, die sie (im Stadium ihrer Durchquerung) als völkerrechtsverletzend einstufen können.[754] Hinzu komme, dass der Grossteil der Internetkommunikation via Cyberinfrastrukturen privater Internetanbieter erfolgt. Auch wenn Schadprogramme entdeckt würden, hänge es von der nationalen Rechtslage ab, ob private Inter-

746 Tallinn Manual 2.0, S. 33 R6 C14.

747 Vgl. IGH, Korfu Kanal-Urteil, S. 18; Woltag, S. 110.

748 Schulze, S. 144; Woltag, S. 104.

749 Tallinn Manual 2.0, S. 41 R6 C39 f.

750 Woltag, S. 104.

751 Woltag, S. 104.

752 Woltag, S. 104.

753 Ausführlicher dazu: Tallinn Manual 2.0, S. 45 R7 C8. Allerdings ist die Abgrenzung von zumutbarer Kenntnisnahme und zumutbaren Massnahmen zu präventiven Massnahmen z.T. fliessend: vgl. Woltag, S. 98.

754 Tallinn Manual 2.0, S. 33 R6 C14.

netanbieter dazu verpflichtet seien, diese den Behörden zu melden.[755] Damit würde eine Verantwortlichkeit für Transitstaaten in der Praxis oft bereits an der ersten Voraussetzung – der (fehlenden) Kenntnis – scheitern.[756]

Schliesslich ist die Reichweite der Sorgfaltspflicht und der damit verbundenen Verantwortlichkeit auch eine Frage der Verhältnismässig- und Zumutbarkeit.[757] So könnten wahrscheinlich ein Grossteil von Cyberangriffen selbst auch bei gegebener Kenntnis des Staates nicht oder nur mittels unverhältnismässiger Massnahmen beendet werden.[758] Für die Verantwortlichkeit eines Staates durch ein pflichtwidriges und wissentliches Unterlassen muss eine verhältnismässige und zumutbare Möglichkeit der Verhinderung oder Minimierung eines Risikos gegeben gewesen sein, die nicht wahrgenommen wurde.[759] Im Beispiel von DDoS-Angriffen, die automatisiert von einem breiten Netz ausgehen, um einen anderen Staat zu schädigen, müsste man bspw. essentielle Teile des Internets abkoppeln, um die Angriffe zu stoppen.[760] In solchen Fällen müssten Art und Umfang des (potenziellen) Schadens durch die DDoS-Angriffe als auch durch die Abkopplung des Internets bewertet werden, um zu beurteilen, ob eine Massnahme angemessen – also verhältnismässig und zumutbar – ist.[761]

Insgesamt gehört gem. Tallinn Manual 2.0 die Errichtung von nationalen CERTs (Computersicherheits-Ereignis- und Reaktionsteams), von nationalen Sicherheitsstrategien und Melderegulierungen für Unternehmen zu den Beispielen für adäquate, verhältnismässige und zumutbare Massnahmen, um Cyberschäden zu vermeiden oder deren Risiken zu minimieren.[762] CERTs sind institutionalisierte Kontaktstellen, die für die zwischenstaatliche Kommunikation im Zusammenhang mit schädigenden Cyberaktivitäten in den von ihnen beaufsichtigten Netzwerken zuständig sind.[763] Obschon *bis dato* (zumindest

755 Tallinn Manual 2.0, S. 33 R6 C14.

756 Tallinn Manual 2.0, S. 33 R6 C14.

757 SCHULZE, S. 144; WOLTAG, S. 107, 110 f.

758 SCHULZE, S. 144.

759 WOLTAG, S. 106 f.

760 Tallinn Manual 2.0, S. 49 R6 C25. Ähnlich: SCHULZE, S. 144, der als unverhältnismässige Massnahme das Beispiel einer kompletten Abkoppelung des Internets erwähnt.

761 Vgl. Tallinn Manual 2.0, S. 49 R6 C25.

762 Tallinn Manual 2.0, S. 46 R7 C12.

763 WOLTAG, S. 104.

ausserhalb der EU[764]) kein expliziter rechtlicher Rahmen für einen solchen Informationsaustausch besteht, haben viele Staaten bereits gewisse Informationsaustauschmechanismen durch nationale CERTs etabliert.[765] Neben nationalen CERTs gibt es weitere relevante, oft mit Staaten zusammenarbeitende Informationsaustauschplatformen.[766] Die Schweiz hat zudem mit der Melde- und Analysestelle Informationssicherung des Bundes MELANI eine mittlerweile innerhalb des Nationalen Zentrums für Cybersicherheit (NCSC) angegliederte Institution errichtet, um einerseits Informationen mit dem Privatsektor auszutauschen und andererseits die Öffentlichkeit über gemeldete Sicherheitslücken zu informieren.[767] Obschon CERTs und Meldestellen alleine wohl nicht ausreichen, um schädigende Cyberaktivitäten effektiv zu vermeiden oder zu unterbinden, handelt es sich um geeignete und grundsätzlich einem Staat zumutbare Minimalstandards im Hinblick auf nationale Netzwerksicherheitsstrukturen.[768]

Im Cyberkontext sprechen gerade die schwierige territoriale Lokalisierbarkeit von Schädigungsquellen und die Weiterverbreitungsmöglichkeiten von Cyberangriffen für einen zwischenstaatlichen Warn- und Informationsmechanismus. Durch einen solchen können nämlich einerseits Informationen über schädliche Cyberaktivitäten und andererseits Informationen zu den Ur-

764 Für EU-Staaten besteht mit der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.08.2013 über Angriffe auf Informationssysteme zusammen mit der Empfehlung des Rates vom 25.06.2001 über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität (2001/C 187/02) eine rechtliche Grundlage für zunehmend institutionalisierte Kooperationsformen.

765 SCHULZE, S. 120 m.w.V. Ausführlicher zu CERTs: WOLTAG, S. 104 f. Gemäss WOLTAG wird die Etablierung nationaler CERTs, die rund um die Uhr verfügbar sind, als organisatorische »*best practice*« in dieser Hinsicht angesehen: WOLTAG, S. 110. Zum nationalen CERT der Schweiz siehe: Swiss Government Computer Emergency Response Team (GovCERT), abrufbar unter: <https://www.govcert.admin.ch/#> (zuletzt besucht: März 2023).

766 So z.B. das »Malware Information Sharing Project (MISP) und Weitere: MISP, Open Source Threat Intelligence Platform and Open Standards For Threat Information Sharing, abrufbar unter: <https://www.misp-project.org/communities/> (zuletzt besucht: März 2023). Für eine verbesserte technische Attribution und Kooperation wurde etwa auch ein Netzwerk von unabhängigen IT-Laboren vorgeschlagen, die getrennt voneinander die technischen Aspekte eines Cyberangriffs analysieren: MÄDER, NZZ vom 28.03.2021.

767 Näheres zur Melde- und Analysestelle MELANI, die gemeinsam mit dem nationalen Computer Emergency Response Team (GovCERT) als technische Fachstelle in das Nationale Zentrum für Cybersicherheit (NCSC) integriert ist, siehe: NCSC, abrufbar unter: <https://www.ncsc.admin.ch/ncsc/de/home.html> (zuletzt besucht: März 2023).

768 WOLTAG, S. 106.

sprungssystemen ausgetauscht werden, um Schäden überhaupt minimieren zu können. Und zwar nicht nur zwischenstaatlich, sondern – da die grosse Mehrheit der Internetserviceanbieter privat ist – eben gerade auch zwischen Staaten und dem Privatsektor.

iii. Nichtstaatliche Akteure und Due Diligence

Grundsätzlich geht es, wie vorangehend aufgezeigt, im Rahmen der Staatenverantwortlichkeit um Völkerrechtsverletzungen durch Staaten oder ihnen zurechenbare Akteure.[769] Das Handeln unabhängiger Privater löst im Völkerrecht grundsätzlich also *keine* Staatenverantwortlichkeit aus.[770] Im Zusammenhang mit der Due Diligence-Verpflichtung können Staaten allerdings auch für transnationale Schädigungen unabhängiger Privater verantwortlich werden, wenn sie Kenntnis davon sowie verhältnismässige und zumutbare Mittel dagegen gehabt hätten.[771] Obschon nichtstaatliche Akteure nicht *per se* Völkerrecht verletzen, können private Handlungen für einen Staat daher u.U. dennoch völkerrechtlich relevant werden. Wie z.B. anhand des patriotischen Hackings aufgezeigt wurde, können private Hacker bspw. auf politische Prozesse oder die Wirtschaft eines Staates Einfluss nehmen und dadurch dem Zwang einer Interventionsverbotsverletzung nahekommen. Angesichts solcher Gefahren für Staaten zeichnen sich insgesamt in verschiedenen international-rechtlichen Bereichen zunehmend staatliche Pflichten zum Umgang mit privaten Akteuren ab (wie bspw. betreffend Umweltschädigungen durch transnationale Unternehmen).[772]

Ein Staat kann grundsätzlich also in zwei Konstellationen für transnationale Verletzungen durch Private verantwortlich werden: Wenn die Handlungen ihm gem. Art. 8 bis 11 ARSIWA zurechenbar sind (wie im vorangehenden Abschnitt erläutert) oder wenn der Staat die ihm sorgfaltspflichtsrechtlich zumutbaren und notwendigen Massnahmen zur Verhinderung oder Beendigung der ihm bekannten Verletzung nicht ergriffen hat.[773] Demzufolge hängen die rechtliche Zurechung privater Handlungen gem. den ARSIWA und die staatliche Sorg-

769 Tallinn Manual 2.0, S. 35 R6 C20.

770 Diggelmann/Hadorn, S. 270; Hessbruegge, S. 265 ff.; Seibert-Fohr, S. 40.

771 Tallinn Manual 2.0, S. 35 R6 C21.

772 Siehe Krieger/Peters/Kreuzer zu verschiedenen Bereichen, in denen Due Diligence diskutiert wird. Aufgegriffen wird u.a. der Bereich des internationalen Umwelt- und Seerechts, verschiedene Bereiche internationaler Sicherheit und des internationalen Wirtschaftsrechts.

773 Woltag, S. 96 m.V.a. ARSIWA-Kommentar, Kapitel II (4).

faltspflicht zur Verhinderung von Verletzungen durch Private eng zusammen, während sie, wie bereits erwähnt, analytisch zu unterscheiden sind.[774] Beispielsweise ist ein Staat nicht *per se* verantwortlich, wenn Private eine Botschaft besetzen. Hatte der Staat jedoch nicht alle zumutbaren Massnahmen zur Verhinderung einer solchen Besetzung oder für die Befreiung derselben ergriffen, kann er aufgrund der Verletzung des Due Diligence-Prinzips verantwortlich gemacht werden.[775] Anders wäre die Situation, in der Angriffe aufgrund genügenden Zusammenhangs einem Staat zuzurechnen sind oder sie durch staatliche Organe ausgeführt werden. In solchen Konstellationen würde ein Staat direkt für die jeweilige Verletzung (z.B. des Interventionsverbots) verantwortlich.[776] Folglich bezieht sich die Due Diligence-Pflicht *de facto* überwiegend auf Handlungen nichstaatlicher Akteure, bei denen der geographische Handlungsursprung zwar bekannt ist, sie einem Staat jedoch nicht gem. ARSIWA zurechenbar sind.[777]

Im Zusammenhang mit der zunehmenden Möglichkeit von Einflussnahmen in innere Angelegenheiten von Staaten durch Private (was bis zum Beweis, dass ein Staat dahintersteht, angenommen werden muss), bietet das Due Diligence-Prinzip Chancen, das Haftungssubstrat zu erweitern. Es würde eine Rechtsgrundlage bieten, um transnationale Schädigungen nichtstaatlicher Akteure indirekt völkerrechtlich zu erfassen. Mit anderen Worten würde die Due Diligence durchaus eine grundsätzlich praktikable Alternative zu den restriktiven ARSIWA-Zurechnungsmöglichkeiten bieten.[778] Damit Estland bspw. bei den DDoS-Angriffen 2007 auf der Grundlage des Interventionsverbots Ansprüche oder Gegenmassnahmen gegenüber einem anderen Staat geltend hätte machen können, hätte nachgewiesen werden müssen, dass die Angriffe jenem Staat gem. ARSIWA zurechenbar sind.[779] Dies war entweder aufgrund mangelnden technischen Nachweises eines staatlichen Zusammenhangs mit den Angriffen oder aufgrund tatsächlicher Ausführung durch private Akteure nicht möglich.[780] Auf diesem Weg könnten Staaten einer direkten Verantworung für schädigendes (privates) Verhalten u.U. sogar bewusst ausweichen.[781]

774 ARSIWA-Kommentar, Kapitel II (4).

775 ARSIWA-Kommentar, Kapitel II (4) m.V.a. IGH, Teheraner Geiselfall.

776 Woltag, S. 99.

777 Wolf, S. 230; Woltag, S. 99. Der Korfu Kanal-Fall ist ein Beispiel dafür.

778 Mikanagi/Mačák, S. 74; Schulze, S. 148.

779 Woltag, S. 95.

780 Woltag, S. 95.

781 So könnten bspw. patriotische Hacker vorgebracht werden, um Verantwortlichkeiten auszuweichen: Phillips/Isachenkov, U.S. News vom 01.06.2017.

Gerade in solchen Fällen würde das Due Diligence-Prinzip eine Grundlage schaffen, dass Staaten nicht *per se* von der Verantwortung ausgeschlossen würden, sondern bei Kenntnis der Schädigung immerhin darlegen müssten, inwiefern ihnen keine vernünftigerweise zumutbaren Mittel dagegen zur Verfügung standen. Eine Nichtergreifung von zumutbaren und verhältnismässigen Möglichkeiten würde sie für die Verletzungen (*post facto*) verantwortlich machen. Zu den zumutbaren und verhältnismässigen Massnahmen eines Staates im Falle einer von seinem Territorium ausgehenden Verletzung würden wohl regelmässig (zumindest nachträgliche) Kooperationsbemühungen zu Investigations-, Schadensbegrenzungs- und Strafverfolgungszwecken mit dem verletzten Staat zählen. Dies illustriert das Potenzial dieser Verantwortlichkeitsregelung für ein internationales Risikomanagement und die damit verbundene Wichtigkeit, die Einzelheiten des Prinzips im Hinblick auf den Cyberkontext zu klären.[782]

iv. Zusammenfassung

Das Tallinn Manual geht in der Theorie von einer relativ weitgehenden Verantwortlichkeit durch sorgfaltspflichtwidriges Unterlassen aus – insb. im Hinblick auf Transitstaaten. Zu extensiv ausgelegte Verantwortlichkeiten von Drittstaaten würden angesichts der durch Cyberangriffe oder deren Weiterverbreitung oftmaligen Involvierung mehrerer Staatsgebiete einerseits die Gefahr implizieren, unbeteiligte Staaten zu Konfliktparteien zu machen und durch die potenzielle Bejahung einer Verletzung Gegenmassnahmen ermöglichen.[783] Dies impliziert ein grundsätzliches Eskalationspotenzial.[784] Dabei ist insb. im Zusammenhang mit Transitstaaten zu beachten, dass u.a. (auch temporäre) Blockierungen gewisser Datenpaketsknoten unvorhergesehene Änderungen der Route nach sich ziehen, womit beinahe unweigerlich unbeteiligte und weitgehend willkürlich Territorien miteinbezogen werden.[785] Andererseits könnte die Aussicht auf eine eigene Verantwortlichkeit Kooperation, Zusammenarbeit sowie proaktive nationale Bemühungen zur Verbesserung einer präventiv ange-

782 Vgl. Mikanagi/Mačák, S. 74 f. Zurückhaltender zur Anwendung von Due Diligence: Jensen/Watts, S. 1555 ff.

783 Ähnlich: Jensen/Watts, S. 1577: »*By presenting more opportunities for more States to allege more breaches of international law, due diligence potentially increases the frequency of States' resort to countermeasures and their accompanying potentially destabilizing effects*«.

784 Vgl. Jensen/Watts, S. 1577: »*Whether a refined duty of cyber diligence would cure or inflame the ills of cyberspace is still unclear*«.

785 Eingehender zur Wichtigkeit der Unterscheidung von Ursprungs- und Transitstaaten: Delerue, Cyber Operations, S. 362 f., S. 368 f.

legten Cybersicherheit begünstigen.[786] Beispielsweise durch Präventionsmassnahmen anhand von Melde- und Analysestellen, (internationale und nationale) Kooperationsmechanismen oder die Einführung nationaler Regelungen zu Sorgfaltspflichten privater Netzwerk-, Soft- oder Hardwareanbieter oder -vertreiber. Angesichts dessen, dass die Umsetzung der Netzwerksicherheit zu einem grossen Teil durch die Privatwirtschaft und den Zivilsektor (»*bottom-up*«) erfolgt, ist die Einbindung und Berücksichtigung jener Sektoren bei der Schaffung regulatorischer Anreize sinnvoll. Neben der nationalen ist für die technische Zurückverfolgung und Beendigung von Cyberangriffen auch eine internationale Kooperation unabdingbar. Ohne Kooperation des Ursprungsstaates ist eine Identifizierung des/der für die jeweiligen Cyberangriffe Verantwortlichen nämlich beinahe unmöglich.[787] Eine derartige Kooperation mit dem Ziel, Cyberangriffe möglichst zu verhindern oder – im Falle einer Schädigung – zu beendigen, würde nach vorliegend vertretener Auffassung ein verhältnismässiges, zumutbares und geeignetes Verhalten des Ursprungsstaates (»*diligent behavior*«) bedeuten.[788] Estlands Präsidentin ging in diesem Punkt sogar einen Schritt weiter und nahm den Standpunkt ein, dass Staaten zugunsten der Kooperation technische Instrumente entwickeln sollten, um den verletzten Staat bei der Identifizierung und Investigation von Cyberangriffen unterstützen zu können.[789] Das Due Diligence-Prinzip könnte sich somit nicht nur im Hinblick auf internationale Kooperation eignen, sondern auch darauf, dass auf nationaler Ebene öffentlich-private Partnerschaften im Technologiebereich gefördert werden könnten. Es könnte insgesamt ein Anreiz geschaffen werden, dass Staaten auf nationaler Ebene die Zusammenarbeit mit privaten Serviceanbietern und Techfirmen ausbauen, um schädigende Cyberaktivitäten zu unterbinden. Dies wiederum könnte die Cybersicherheit insgesamt erhöhen.

786 Schulze, S. 151 ff., 160 spricht sich für eine Beweislastumkehr bei staatlich oder zu staatlichen Zwecken betriebenen Netzwerkinfrastrukturen aus. Eine solche Beweislastumkehr könnte letztlich auch eine internationale Kooperation anstossen.

787 Woltag, S. 110.

788 Ebenso: Woltag, S. 110. Ähnlich kann auch im Falle eines bewaffneten Angriffs durch nichtstaatliche Akteure eine Pflicht des Ursprungsstaates zur Kooperation mit dem Zielstaat angenommen werden: Institute de Droit Internationale, Resolution on Self-Defense 2007, §10.

789 Siehe Kaljulaid, Eröffnungsrede CyCon 2019. Dazu auch: Schmitt, Just Security vom 10.06.2019.

Die Staaten haben bei der Umsetzung der Due Diligence ein Ermessen, die zu ihrem System passenden und adäquaten Massnahmen zu wählen.[790] Eine einzelfallbezogene Berücksichtigung der jeweils einem Staat zumutbaren und angemessenen Möglichkeiten bleibt daher möglich. Dabei werden subjektive und objektive Aspekte gewürdigt. Es besteht bspw. keine generelle Pflicht, dass Staaten die absolute Kenntnis über alle Aktivitäten innerhalb ihres Territoriums oder ihrer Cyberinfrastrukturen haben müssen.[791] Staaten werden zudem nicht explizit dazu verpflichtet, spezifische nationale Strafbestimmungen zu erlassen.[792] Die Abwesenheit von nützlichen Mechanismen könnte in einem Schadensfall, wie bereits erwähnt, u.U. dennoch ein Hinweis auf sorgfaltspflichtwidriges Verhalten sein.[793] Gänzlich von der Verantwortung wird sich ein Staat (u.a. im Hinblick auf Risiken minimierende Instrumente) somit nicht nehmen können, wenn für ihn vernünftige, objektiv zumutbare und verhältnismässige Mittel vorhanden gewesen wären. Trotz relativ flexibler Einzelfallbeurteilungsmöglichkeiten bestehen nämlich objektiv zumutbare Handlungsmöglichkeiten. So kann die Kenntnis einer vom eigenen Territorium ausgehenden Verletzung wohl objektiv als gegeben erachtet werden, sobald der Zielstaat den Ursprungsstaat darüber informiert.[794] Spätestens ab jenem Zeitpunkt wäre es dem Ursprungsstaat daher zumindest möglich zu kooperieren, um sich einer Verantwortlichkeit zu entziehen.

Es mag sein, dass Staaten dem Due Diligence-Prinzip generell eher zurückhaltend gegenüberstehen, da es ihnen Verantwortlichkeiten auferlegt[795] und gegebenenfalls Gegenmassnahmen gegen sie ermöglicht. Die den Staaten auferlegte Verantwortlichkeit erscheint jedoch nach vorliegend vertretener Ansicht nicht ungebührlich hoch. Von den Staaten wird nämlich nur das ihnen jeweils wissentlich und vernünftigerweise Zumutbare und Mögliche erwartet.[796] Zudem betrifft die Verantwortlichkeit nicht die Verhinderung eines jeden Cyberangriffs, sondern bezieht sich vor allem auf Vorkehrungen zur *Risikominimierung* von sicherheitspolitisch relevanten Cyberangriffen.[797] Indem am Zumutbaren und Möglichen angesetzt wird, sind grundsätzlich keine konkreten

790 Woltag, S. 110.
791 Dazu: Delerue, Cyber Operations, S. 359 f.
792 Woltag, S. 110.
793 Woltag, S. 110.
794 Woltag, S. 110.
795 Jensen, Tallinn Manual 2.0, S. 745.
796 Delerue, Cyber Operations, S. 374; Woltag, S. 110.
797 Vgl. dazu auch Kaljulaid, Eröffnungsrede CyCon 2019.

Resultate erforderlich, um die Voraussetzungen des Prinzips zu erfüllen.[798] Da völkerrechtlich relevante Cyberangriffe trotz angewandter, angemessener Sorgfalt oft erst nach Eintritt einer relevanten Schädigung bemerkt werden, wird die Due Diligence-Verantwortung im Cyberkontext zudem zu einem Grossteil Handlungen des Ursprungsstaates *nach* der Kenntnis eines Schadenseintritts[799] oder aber institutionalisierte Mechanismen zur Prävention von Schäden und der Risikominimierung betreffen. Im Hinblick auf die Verantwortlichkeit würde dies im Regelfall somit vordergründig Kooperations- und Beendigungsbemühungen betreffen. Absolute (präventive) Sicherheit wird im Cyberkontext unrealistisch bleiben, da laufend technische Umgehungsmöglichkeiten entstehen, die gerade auf neue, dem Opfer unbekannte Sicherheitslücken ausgerichtet sind. Die völkerrechtliche Due Diligence würde Staaten vielmehr dazu verpflichten, die vernünftigerweise erforderlichen Vorkehrungen und Rahmenbedingungen zu etablieren, um die Risiken völkerrechtlich relevanter, transnationaler Schädigungen zu minimieren. Das Verhältnismässigkeitsprinzip verhindert schliesslich, dass völkerrechtliche Sorgfaltspflichten die Handlungsfreiheit von Staaten in unzumutbarer Weise beschränken[800] und ungebührlich hohe Verantwortlichkeiten auferlegen.

Das Due Diligence-Prinzip bietet grundsätzlich eine völkerrechtliche Grundlage, um auf die Charakteristika von Cyberangriffen sowie die unübersichtlichen Akteurskonstellationen zu reagieren. Es würde zudem die grundsätzliche Möglichkeit für Staaten beschränken, die Anonymität im Cyberraum vorzuschieben und für ein sorgfaltspflichtsrechtliches Untätigbleiben keine Verantwortung übernehmen zu müssen. Da private und staatliche Akteure im Cyberkontext in unübersichtlicher Weise zusammentreffen, könnte man mit dieser Norm ein Gefäss schaffen, solche Sachverhalte rechtlich besser zu erfassen.

---

798 Zur Unterscheidung von Verhinderungserfolg und des Ergreifens aller vernünftiger und notwendiger Massnahmen: Crawford, State Responsibility, S. 227 f. m.w.V. Er unterscheidet in diesem Zusammenhang eine präventive Verhinderungspflicht vom Ergreifen der erforderlichen Sorgfaltspflicht. Ihm zufolge ist die Verhinderungspflicht keine Garantie, dass eine Verletzung nicht eintrifft. Vielmehr setze sie voraus, dass alle vernünftigerweise notwendigen Massnahmen ergriffen wurden, um sie zu verhindern. Vgl. dazu: ARSIWA-Kommentar, Art. 23(34), (6); IGH, Bosniengenozid-Urteil, §430: »*It is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide.*« Dazu ebenfalls: Peters/Krieger/Kreuzer, Risk Management Tool, S. 128 ff. Für den Cyberkontext: Delerue, Cyber Operations, S. 374.

799 Woltag, S. 110. Ähnlich Jensen, Tallinn Manual 2.0, S. 745.

800 Vgl. Woltag, S. 110.

Sollten sich Staaten vermehrt zum Due Diligence-Prinzip bekennen, könnte dies Unklarheiten (oder wie SCHMITT es nennt »Graubereiche«[801]) in seiner Geltung entgegenwirken, Voraussehbarkeit schaffen sowie gegenseitige Verantwortung und Kooperation begünstigen. Dabei werden die Anwendung und die Umsetzung des Prinzips im Cyberbereich weiter geklärt werden müssen.[802] Abzuwägen sind dabei einerseits das Interesse, unbeteiligte Staaten möglichst nicht in Konflikte zu ziehen und dadurch Stabilität zu wahren – und andererseits das Ziel, möglichst breite Kooperation sowie die Minimierung von Risiken anzustreben und Sanktionsgrundlagen für schwerwiegende, völkerrechtlich relevante Cyberangriffe (ausserhalb der *ius ad bellum*-Diskussion) zu schaffen, über die Kenntnis sowie zumutbare Verhinderungsmöglichkeiten bestanden.

Die Möglichkeit, private Handlungen einem Staat (unabhängig von den ARSIWA) anzurechnen, erweitert im Ergebnis den Radius des Anwendungsbereichs der völkerrechtlichen Staatenverantwortung. Gemäss einem Teil der Lehre kann darin, vereinfacht gesagt, eine strukturelle Verschiebung in der internationalen Ordnung gesehen werden.[803] Insgesamt betrachtet sind staatliche Sorgfaltspflichten für transnationale Verletzungen im Grunde allerdings, wie anhand des Korfu Kanal-Falles aufgezeigt wurde, nicht neu.[804] Die völkerrechtlichen Erwartungen in Bezug auf die Verhinderung transnationaler Schädigungen sind es folglich auch nicht. Der vorliegend vertretenen Auffassung nach sollte die völkerrechtliche Due Diligence angesichts der zunehmenden digitalen Einfluss- und Schädigungsmöglichkeiten anderer Staaten grundsätzlich also ernst genommen werden. Im Einzelnen sollte eine Sorgfaltspflichtsverletzung allerdings eher zurückhaltend bejaht werden, um internationale Verantwortlichkeiten nicht vorschnell anzunehmen. So sollten die Kenntnis sowie zumutbare und verhältnismässige Verhinderungsmöglichkeiten im Zweifel restriktiv angenommen werden. Diese sollten für den betreffenden Staat vielmehr in *substanzieller und realistischer* Weise gegeben sein. Bei der Würdigung der zumutbaren und verhältnismässigen Kenntnis- und Verhinderungsmöglichkeit sollte genügend Raum bestehen bleiben, um auf die individuellen (technischen) Möglichkeiten von Staaten eingehen zu können. Das

801 SCHMITT, Grey Zones, S. 11. Ihm zufolge impliziert es einen Graubereich, dass nicht alle Staaten eine solche Pflicht anerkennen.

802 Vgl. MIKANAGI/MAČÁK, S. 74 f.

803 Siehe dazu das Kapitel »*Due Diligence and Structural Change in the International Legal Order*«, in: KRIEGER/PETERS, S. 351 ff.; PETERS/KRIEGER/KREUZER, Risk Management Tool, S. 135.

804 AKANDE/COCO/DIAS, EJIL Blog vom 05.01.2021.

heisst, eine durch Sorgfaltspflichten ausgelöste, völkerrechtliche Verantwortlichkeit sollte nach vorliegend vertretener Ansicht bei Cyberangriffen zwar insgesamt möglich sein, doch im Einzelfall restriktiv angenommen werden.

Im Zusammenhang mit Cyberangriffen wird insb. die territoriale Anknüpfung der völkerrechtlichen Due Diligence-Norm eine Herausforderung bleiben.[805] Eine klare technische Zuordnung von Cyberangriffen an ein bestimmtes Territorium wird angesichts der globalen Vernetzung nämlich weiterhin schwierig sein. Obschon Cyberinfrastrukturen wie Server, Router, Kabel usw. grundsätzlich physisch einem Territorium oder einer Hoheitsgewalt zugeordnet werden können,[806] bleiben aufgrund der internationalen Interkonnektivität solcher digitaler Infrastrukturen -und Aktivitäten Schwierigkeiten bestehen. Es wird zu klären sein, ab wann extraterritoriale Schädigungen durch Cyberangriffe einem Territorium und damit einem Staat zugeordnet werden können – insb., wenn sie von mehreren Territorien gleichzeitig ausgehen. Hinzu kommt die bereits genannte Herausforderung, dass Schadprogramme automatisiert, aus der Ferne oder physisch in einem anderen Territorium eingeschleust werden können. Das heisst, Schadprogramme können zwar von einem bestimmten Territorium ausgehen, obschon diese in einem anderen Staat programmiert oder freigelassen wurden. In dieser Hinsicht werden künftig wohl auch sorgfaltspflichtsrechtliche Fragen in Bezug auf die zugrundeliegende Absicht der *Urheberschaft von Schadprogrammen* wichtiger werden, um einen (u.U. durch Due Diligence) verantwortlichen Ursprungsstaat zu eruieren.[807] Die alleinige Anknüpfung an ein Territorium wird zu einem gewissen Grad Kooperation begünstigen, aber kaum die gesamte Bandbreite an Cyberangriffsmöglichkeiten erfassen können.

805 Vgl. Wortlaut im Korfu Kanal-Fall: »*not knowingly allow their territory*«.

806 SCHULZE, S. 112 m.w.H.

807 Das Tallinn Manual berücksichtigt für die Zuordnung an die Souveränität eines Staates bspw. verschiedene Schichten des Cyberraums sowie die Akteure dahinter. Gemäss Tallinn Manual 2.0, S. 12 R1 C5 können Cyberangriffe der Souveränität eines Staates zugeordnet werden, wenn sie Objekte auf einem Territorium betreffen oder durch in dessen Hoheitsgewalt stehende Personengruppen ausgeübt werden. Es geht davon aus, dass physische, logische und soziale Schichten im Cyberraum enthalten sind. Erstere Schicht umfasst die physischen Netzwerkkomponenten (d.h. Hardware und andere Infrastrukturen wie Kabel, Router, Server und Computer). Zweitere Schicht besteht aus den Verbindungen, die zwischen Netzwerkgeräten bestehen und u.a. Datenaustausch zwischen den physischen Infrastrukturen ermöglichen. Die soziale Schicht umfasst die Akteure hinter Cyberangriffen: Tallinn Manual 2.0, S. 12 R1 C4.

IV. Cyberangriffe und Verhältnismässigkeit unilateraler Selbsthilfe

»Is the question of *level* of violence by regular forces not really an issue of *proportionality*, rather than a question of determining what is an armed attack?«[808]

In diesem Kapitel soll die auf eine bejahte Völkerrechtsverletzung folgende unilaterale Reaktion näher betrachtet werden. Die Anwendung des Rechts auf Selbstverteidigung nach Art. 51 UN-Charta sowie der völkerrechtlichen Normen der Staatenverantwortlichkeit auf Cyberangriffe werfen der Logik folgend nämlich die Frage auf, welches die rechtlichen Selbstverteidigungs- und Gegenmassnahmemöglichkeiten sind und wie weit sie gehen dürfen.[809] Dafür ist das Verhältnismässigkeitsprinzip relevant. Wichtig ist, dass dem Prinzip je nach Bereich, wie bereits unter II.B.3) erwähnt, unterschiedliche Bedeutungen zukommen. Wird ein bewaffneter Angriff nach Art. 51 UN-Charta bejaht, kommt die insb. zeitlich eng gefasste Verhältnismässigkeit des *ius ad bellum* zur Anwendung. Werden Normen der Staatenverantwortlichkeit wie das Interventions-, das Gewaltverbot oder das Due Diligence-Prinzip verletzt, ist das Verhältnismässigkeitsprinzip des Gegenmassnahmenrechts gem. ARSIWA einschlägig. Die Würdigung von Cyberangriffen hat somit nicht nur fundamentale Auswirkungen auf das Spektrum möglicher Reaktionen (militärische Selbstverteidigung vs. nicht-militärische Gegenmassnahmen), sondern auch auf die Art, Intensität und die Ausrichtung derselben. Wenn Cyberangriffe als bewaffnete Angriffe gem. Art. 51 UN-Charta statt als Normverletzungen innerhalb der Staatenverantwortlichkeit betrachtet werden, hat dies folglich

---

808 Higgins, S. 251.

809 Petkis, S. 1454.

erhebliche Konsequenzen auf das, was als verhältnismässig und was als unverhältnismässig, als gerechtfertigt und als ungerechtfertigt angesehen wird.[810] Die Abhandlung im vorangehenden Teil III.B. dieser Dissertation sollte demgemäss aufgezeigt haben, dass extensive oder restriktive Verständnisse von Art. 51 UN-Charta daher durchaus zentral sind, um das Spektrum möglicher Reaktionen festzulegen. Deeskalierend bleibt dabei eine *restriktive* Subsumierung von Cyberangriffen unter den Anwendungsbereich der Selbstverteidigung. Dadurch schliesst man nämlich im Voraus die Möglichkeit *kollektiver militärischer* Reaktionen aus.[811] Dies spricht folglich *gegen* die in diesen Teil einleitende Frage, ob das Mass militärischer Gewalt primär vor dem Hintergrund der Verhältnismässigkeit zu beantworten ist. Dahingehende Entwicklungen, den Anwendungsbereich von Art. 51 UN-Charta mit dem Argument auszuweiten, dass die Verhältnismässigkeit die Intensität und Art der Reaktion in »ausreichender« Weise einzuschränken vermag,[812] sind nach vorliegender Haltung daher mit grosser Zurückhaltung zu betrachten. Obschon die Bejahung eines bewaffneten Angriffs im Cyberkontext, wie vorangehend dargelegt wurde, in den überwiegenden Fällen folglich restriktiv erfolgen sollte,[813] muss es dennoch möglich bleiben, sich gegen schwerwiegende transnationale Gewalt wehren zu können.[814] Sollte eine gewaltsame Selbstverteidigung in einem konkreten Falle eines bewaffneten Angriffs tatsächlich die einzig effektive Massnahme sein, um die Existenz eines Staates zu schützen, muss sie daher insgesamt möglich, jedoch gleichzeitig verhältnismässig sein. Ähnlich hält die Mehrheit der Staaten weiterhin am Recht auf Selbstverteidigung bei Cyberangriffen fest.[815] Demzufolge kommt der Verhältnismässigkeit in jenen Konstellationen der vorliegenden Ansicht zufolge als letztes (gewalteindämmendes oder -legitimierendes) Rechtsventil grosse Bedeutung zu.

---

810 Siehe May, S. 14 f. in: Proportionality and "Cyberwar".

811 Ähnlich dazu: Schmitt, Countermeasures Response Option, S. 730.

812 Der Tendenz nach u.a. Petkis, S. 1452. Vgl. ferner die Ausführungen sogleich in Fn. 816.

813 Ähnlich: Lahmann, S. 112.

814 Vgl. zu dieser Gratwanderung: Kress, S. 603 f. Er anerkennt zwar die Tendenz des IGH, Gewalt, wenn nur möglich, *restrikiv* zuzulassen. Allerdings betrachtet er eine zu weitgehende Gewalteinschränkung als fraglich, wenn eine Gewaltanwendung die einzige effektive Verteidigungsmöglichkeit darstellt. Man dürfe nicht vergessen, dass bewaffnete Angriffe und massive transnationale Gewalt eine durchaus sehr ernstzunehmende Gefahr für (alle) Staaten darstellen.

815 Explizit halten u.a. die USA, die Niederlande und Estland sowie die in Roguski, S. 1 ff. untersuchten Länder am Recht auf Selbstverteidigung fest.

A. Verhältnismässigkeit und Selbstverteidigungsrecht

Sollte ein Cyberangriff als bewaffneter Angriff i.S.v. Art. 51 UN-Charta bejaht werden, muss eine darauffolgende Selbstverteidigungshandlung zwingend dem Erfordernis der Verhältnismässigkeit genügen. Dogmatisch ist die Qualifizierung eines bewaffneten Angriffs von der darauffolgenden Überprüfung der ergriffenen Selbstverteidigungsmassnahme im Lichte der Verhältnismässigkeit grundsätzlich zu unterscheiden.[816] Nichtsdestotrotz überschneiden sich diese Bereiche inhaltlich, indem insb. die Qualifizierung des Beginns und der Beendigung eines bewaffneten Angriffs sich auf die Frage nach der Verhältnis- und Notwendigkeit einer Selbstverteidigungshandlung auswirkt. Somit beeinflussen nicht nur unterschiedliche Ansichten der Verhältnismässigkeit, sondern auch bereits die Definition des Anwendungsbereichs eines bewaffneten Angriffs die rechtliche Würdigung, ob eine Selbstverteidigungshandlung verhältnismässig ist.[817] Die Bejahung einer antizipatorischen Selbstverteidigung impliziert bspw. ein extensives Verständnis davon, dass eine Verteidigung bereits im Vorfeld von konkreten Schäden notwendig (und damit verhältnismässig) sein kann. Nachfolgend sollen sich im Cyberkontext stellende Schwierigkeiten näher analysiert werden. Dazu soll vorerst die traditionelle Bedeutung der Verhältnismässigkeit bei der Selbstverteidigung aufgegriffen werden, um sie in einem zweiten Schritt auf den Cyberbereich anzuwenden.

---

816 Der IGH trennt (z.B. im IGH, Ölplattformen-Urteil) die Konzepte der Notwendig- und Verhältnismässigkeit dogmatisch von der Qualifizierung eines bewaffneten Angriffs, indem er die Notwendig- und Verhältnismässigkeit erst *nach* der Bejahung eines bewaffneten Angriffs nach Art. 51 UN-Charta berücksichtigt. In der Staatenpraxis hingegen sind die Notwendig- und Verhältnismässigkeit oft die *einzigen* Faktoren, die zur Würdigung der Rechtmässigkeit gewisser Handlungen herangezogen werden. Dadurch können Staaten in Sicherheitsratsdebatten doktrinalen Auseinandersetzungen darüber, ob der Anwendungsbereich der Selbstverteidigung weit oder eng zu verstehen ist, ausweichen. Siehe dazu: Gray, Use of Force, S. 163 f. m.w.V., S. 213 m.w.V.

817 Gray, Use of Force, S. 159.

1. Grundidee der *ius ad bellum*-Verhältnismässigkeit

a. Theoretische Grundlagen

Jede Selbstverteidigungshandlung auf einen bewaffneten Angriff gem. Art. 51 UN-Charta, unabhängig davon, ob sie kinetischer oder elektronischer Natur ist, unterliegt im internationalen Recht den Grundsätzen der Notwendig- und Verhältnismässigkeit.[818] Gemäss IGH gelten die Notwendig- und Verhältnismässigkeit als dem Art. 51 UN-Charta inhärente und damit gewohnheitsrechtliche Prinzipien.[819] Obschon ein grundsätzlicher Konsens darüber besteht, *dass* die Verhältnismässigkeit im *ius ad bellum* eingehalten werden muss, bestehen divergierende Verständnisse darüber, *wie* die Verhältnismässigkeit im Einzelnen auszulegen ist.[820] Grundsätzlich wird die Verhältnismässigkeit bei der Selbstverteidigung allerdings eng verstanden, indem die Massnahme auf die Beendigung und Abwehr eines bewaffneten Angriffs gerichtet sein muss[821] und keine Vergeltung oder Bestrafung sein darf (Sinn und Zweck der Selbstverteidigung).[822] Es gilt daher ein grundsätzliches Repressalienverbot.[823] Es ist dabei unklar (jedoch davon auszugehen), ob die Notwendigkeit einen Unteraspekt der Verhältnismässigkeit oder einen separaten Aspekt darstellt; einige Autoren unterscheiden die Konzepte theoretisch, indem sie teilweise ausschliesslich dem einen oder dem anderen Erfordernis folgen und andere wie-

818 *Dass* für eine legitime Selbstverteidigung die Prinzipien der Notwendig- und Verhältnismässigkeit eingehalten werden müssen, ist in der Lehre und innerhalb der Staatengemeinschaft weitgehend unbestritten: Gardam, Proportionality and Force, S. 391; Gray, Use of Force, S. 157 f. m.w.V.; Banks/Criddle, S. 74; Dinstein, War, Aggression and Self-Defence, S. 249 ff.; Randelzhofer/Nolte, S. 1425 ff. Für den Cyberkontext: Harrison Dinniss, S. 102; Hathaway et al., S. 849; Lahmann, S. 54. Die Erfordernisse werden oft i.Z.m. der Webster Formel des Caroline Falles angeführt: Jennings, S. 82 ff.

819 IGH, Nicaragua-Urteil, §176, §194; IGH, Nuklearwaffen-Gutachten, §41; IGH, Ölplattformen-Urteil, §74; IGH, Kongo-Urteil, §147; Kress, S. 568. Einige wenige Autoren lehnten den gewohnheitsrechtlichen Charakter (allerdings in der Vergangenheit) ab. So z.B. in 1947 Kunz, S. 872 ff.

820 Akande/Liefländer, S. 566.

821 Gray, Limits of Force, S. 140 ff.; Newton/May, S. 270; Nolte, A Response to Kretzmer, S. 290; Wicker, S. 35 ff.; Wilmshurst et al., S. 966. Contra: Kretzmer, 235 ff.

822 Gray, Use of Force, S. 159; Harrison Dinniss, S. 104; Lahmann, S. 54. Dazu auch: Randelzhofer/Nolte, S. 1425 ff.

823 IGH, Nuklearwaffen-Gutachten, §46; Diggelmann, Völkerrecht, S. 162 ff.; Dinstein, Computer Network Attacks, S. 107 f.; Gray, Use of Force, S. 160 u.a. m.V.a. die Declaration on Friendly Relations (UN Doc. A/RES/2625 (XXV), die Declaration on the Inadmissibility of Intervention (UN Doc. A/RES/36/103 (1981)).

derum handeln die beiden Elemente als ein gemeinsames Konzept ab.[824] Da die beiden Erfordernisse bei Selbstverteidigungshandlungen eng zusammenhängen und es fraglich bleibt, inwiefern sie tatsächlich getrennt betrachtet werden können, sollen sie vorliegend gleichermassen Erwähnung finden. Denn ist Gewaltanwendung nicht notwendig, kann sie laut GRAY nicht verhältnismässig sein und ist sie nicht verhältnismässig, ist es schwierig zu argumentieren, dass sie notwendig ist.[825] Auch der IGH geht von einer »dualen Kondition« der Notwendig- und Verhältnismässigkeit aus, die »gleichermassen auf Art. 51 UN-Charta Anwendung findet«.[826] Vorliegend sollen daher im Rahmen eines übergeordneten Verhältnismässigkeitsverständnisses (i.w.S.) einerseits die Notwendigkeit und andererseits die Verhältnismässigkeit i.e.S. unterschieden werden (die Herangehensweise ist inspiriert von der innerstaatlichen Verhältnismässigkeitsprüfung laut der Schweizerischen Bundesverfassung).

Gemäss dem Notwendigkeitsprinzip müssen Selbstverteidigungshandlungen notwendig sein, um einen bewaffneten Angriff abzuwehren[827] und um dadurch die Existenz des Staates zu schützen.[828] Die Notwendigkeit impliziert, dass keine milderen Mittel den Zweck des Abwehrens erfüllen hätten können oder diese bereits ausgeschöpft wurden.[829] Der sich verteidigende Staat darf also nicht mehr Gewalt anwenden als zur Existenzsicherung notwendig ist, und

824 Siehe z.B. IGH, Nuklearwaffen-Gutachten, (Gegenmeinung Richterin Higgins), §5; BETHLEHEM, S. 775 (beide Elemente in Prinzip 3 anführend); GARDAM, Necessity, Proportionality, S. 156 ff.; GREENWOOD, MPEPIL 2011, §26; NEWTON/MAY, S. 65. Ausführlicher dazu: AKANDE/LIEFLÄNDER, S. 566 ff.; GRAY, Use of Force, S. 159. Dies kann im Ergebnis zu verschiedenen Konklusionen führen, welche Handlungen letztlich als (un-)verhältnismässig gesehen werden. Siehe dazu ausführlicher nachfolgend.

825 GRAY, Use of Force, S. 159. Ähnlich zu den beiden Konzepten und dass beide für die Selbstverteidigung relevant sind: CORN, S. 79 ff., insb. S. 81, S. 83.

826 IGH, Nuklearwaffen-Gutachten, §41; KRESS, S. 568.

827 GREENWOOD, MPEPIL 2011, §27; HARRISON DINNISS, S. 102. Ferner dazu: AKANDE/LIEFLÄNDER, S. 566; DINSTEIN, War, Aggression and Self-Defence, S. 249 f.

828 Zumindest vertritt eine überwiegend in Kontinentaleuropa vorherrschende Ansicht diese Auffassung vom Sinn und Zweck der Selbstverteidigung. Siehe vorangehend unter III.B.1.a. und b.

829 DINSTEIN, Proportionality and Necessity, S. 57; HARRISON DINNISS, S. 103; WILMSHURST et al., S. 966 f.

es dürfen keine friedlichen Alternativen zur Verfügung stehen.[830] Stehen einem Staat gewaltlose Massnahmen zur Verfügung, um dasselbe Ziel zu erreichen, wäre eine gewaltsame Selbstverteidigungshandlung nicht gerechtfertigt.[831] Eine gewaltsame Selbstverteidigung darf demzufolge nur als letztmögliches Mittel eingesetzt werden.[832] Auch das Zielobjekt der Verteidigungshandlung kann in die Würdigung der Notwendigkeit einfliessen; so kann es u.U. gem. IGH als nicht notwendig erachtet werden, auf bestimmte Objekte oder Einrichtungen abzuzielen, wenn deren Angriff nicht der Abwehr dient.[833] Zudem rührt aus dem Notwendigkeitsprinzip, dass eine Selbstverteidigungshandlung zeitlich *während* eines Angriffs stattfinden muss,[834] da nach Beendigung desselben eine Verteidigung grundsätzlich nicht mehr zur Abwehr notwendig ist.[835] Es gibt allerdings extensive Ansichten, dass auch unmittelbar *bevorstehende* Gefahren das Recht auf Selbstverteidigung auslösen können.[836] Das Verhältnismässigkeitsprinzip soll nach jener Lesart bei existenziellen, unmittelbaren Gefahren die Anwendung von Gewalt nicht beschränken können, da die Möglichkeit einer gewaltsamen Abwehr auch in jenen Situationen als notwendig erachtet wird.[837] Wie weit in Abweichung vom Wortlaut von Art. 51

---

830 IGH, Ölplattformen-Urteil, (separate Meinung Richter Kooijmans), §62; Akande/Liefländer, S. 564, S. 567. Zu den einzelnen Elementen: u.a. IGH, Nicaragua-Urteil, §237. Ferner: Lahmann, S. 54; Green, S. 85; Greenwood, MPEPIL 2011, §27; Sloane, Cost of Conflation, S. 108 f. (»*An act is ad bellum disproportionate if the same ad bellum objective sought by force clearly could have been achieved by diplomacy or another nonviolent strategy at a roughly comparable, or even moderately greater, cost.*«).

831 Ago, S. 69; Harrison Dinniss, S. 103.

832 Als Beispiel friedlicher Alternativen würden diplomatische Verhandlungen gelten: Hathaway et al., S. 849.

833 Harrison Dinniss, S. 103 und Gray, Use of Force, S. 160 f. m.V. auf den Ölplattformen-Fall, in dem das Abzielen auf bestimmte Platformen als nicht notwendig angesehen wurde: IGH, Ölplattformen-Urteil, §73 ff. Contra: Taft, S. 295.

834 Harrison Dinniss, S. 103. Davon teilweise abweichend: Dinstein, War, Aggression and Self-Defence, S. 222 ff., S. 229 ff. Ihm zufolge muss das zeitliche Erfordernis flexibel angewandt werden. Solange eine Verteidigungshandlung nicht mit unangemessener Verzögerung erfolge, könne sie auch zeitlich *nach* einem Angriff erfolgen. Er verweist auf S. 252 darauf, dass bis zur Autorisierung des Sicherheitsrats, die notwendigen Massnahmen vorzunehmen, u.U. zu viel Zeit vergehen kann. Es besteht somit eine gewisse Kotroverse, unter welchen Umständen die Unmittelbarkeit gegeben ist: Gardam, Necessity, Proportionality, S. 149 ff.; Corten, Law against War, S. 485.

835 Siehe Ausführungen zur zeitlichen Komponente der Selbstverteidigung unter III.B.1.a.

836 Zum Beispiel die USA, UK und Israel: Gray, Use of Force, S. 227.

837 Gray, Use of Force, S. 227

UN-Charta auch unmittelbar vor oder nach einem Angriff ein Recht auf Selbstverteidigung besteht, ist allerdings vehement umstritten und Gegenstand epischer Debatten.[838]

Die Notwendigkeit wirft auch im Hinblick auf Selbstverteidigungsmassnahmen gegen nichtstaatliche Akteure Fragen auf. Würde die Selbstverteidigung gegen nichtstaatliche Akteure bejaht, würde diese nämlich ebenfalls dem Erfordernis der Verhältnismässigkeit i.w.S. und damit der Notwendigkeit unterliegen.[839] Militärische Selbstverteidigungshandlungen gegen nichtstaatliche Akteure auf dem Territorium eines anderen Staates sind dem Prinzip zufolge nur erlaubt, wenn der sich verteidigende Staat die Zustimmung des die Angreifer beherbergenden Staates dazu einholt und jener ungewillt oder nicht in der Lage ist zu agieren.[840] Es kann nicht notwendig (bzw. das mildeste Mittel) sein, die territoriale Integrität eines anderen Staates mit einer Selbstverteidigungshandlung zu verletzen, wenn Massnahmen mit der Einwillungen des Letzteren möglich gewesen wären.[841] Es kann in der Praxis durchaus schwierig sein zu beweisen, dass der die Angreifer beherbergende Staat nicht bereit oder in der Lage ist, bewaffnete Angriffe nichtstaatlicher Akteure gegen andere Staaten zu verhindern oder diesbezüglich zu kooperieren.[842] Vom Einholen der Einwilligung soll jedoch nur abgesehen werden dürfen, wenn dies die Wirksamkeit einer Massnahme erheblich untergraben oder das Risiko weiterer bewaffneter Angriffe erhöhen würde.[843] Der sich verteidigende Staat soll sich nicht so verhalten müssen, dass für die Abwehr des Angriffs notwendige und effektive Massnahmen unwirksam würden.[844] Dem die Angreifer beherbergenden Staat muss i.d.R. allerdings zumindest die Möglichkeit gegeben werden,

838 Diggelmann, Völkerrecht, S. 160. Dazu u.a. Bethlehem, S. 770 ff.; Dinstein, War, Aggression and Self-Defence, S. 222 ff., S. 229 ff., S. 252. Siehe bspw. die entgegenstehenden Positionen von Kretzmer, S. 235 und Nolte, A Response to Kretzmer, S. 283. Für den Cyberkontext u.a.: Roscini, World Wide Warfare, S. 120 ff.; Jensen, Critical National Infrastructure, S. 219.

839 Wie bereits unter III.B.1.a. und c. angeführt, ist umstritten, ob ein Recht auf Selbstverteidigung gegen nichtstaatliche Akteure erlaubt ist. Zur Verhältnismässigkeit der Selbstverteidigung gegen nichtstaatliche Akteure: Trapp, S. 141 ff.

840 Akande/Liefländer, S. 566; Lahmann, S. 62.

841 Akande/Liefländer, S. 566.

842 Zu den Schwierigkeiten und Abwägungen i.Z.m. dem erforderlichen Mass an Gewissheit: Deeks, S. 508 ff.

843 Bethlehem, S. 776, in Prinzip 12.

844 Akande/Liefländer, S. 566.

seine Pflicht wahrzunehmen, von seinem Territorium ausgehende Schädigungen zu unterbinden, bevor militärische Selbstverteidigungshandlungen gegen ihn eingeleitet werden.[845]

Das Element der Verhältnismässigkeit (i.e.S.) ergänzt die Logik der Notwendigkeit und verbietet Gewalt, wenn der Gesamtumfang und die Intensität derselben disproportional zur tatsächlichen Gefahr für den Staat ausfallen.[846] Es gibt verschiedene Auffassungen dazu, was im Einzelnen bei Selbstverteidigungshandlungen verhältnismässig ist.[847] Einer ersten Kategorisierung zufolge muss eine Verteidigungshandlung dem Angriff *quantitativ* entsprechen, um verhältnismässig zu sein.[848] Ein zweites Konzept impliziert, dass die Verteidigungshandlung keinen zum beabsichtigten und zulässigen *Ziel* unverhältnismässigen Schaden anrichten darf (sog. »funktionaler Ansatz«[849]).[850] So kann man in einigen Urteilen des IGH die Tendenz feststellen, dass der durch den Angriff verursachte Schaden und der Zweck der Reaktion verglichen werden.[851] Letzteres Verständnis von Verhältnismässigkeit verlangt im Grundsatz nicht, dass ein Angriff nur mit derselben Art oder Intensität von Gewalt abgewehrt werden darf.[852] Wenn vernünftigerweise mehr Gewalt erforderlich ist, um den ursprünglichen Angriff effektiv beenden zu können, könne diese Massnahme nicht als unverhältnismässig gelten.[853] Primär muss die Selbstverteidigungsmassnahme allerdings geeignet sein, um den Angriff zu beenden und abzuwehren.[854] Aufgrund der verbleibenden Vagheit des Prinzips geht man auch beim zweiten Ansatz allgemein davon aus, dass immerhin eine gewisse Vergleichbarkeit zwischen dem ursprünglichen Angriff und der Selbst-

845 Dazu i.Z.m. dem Cyberkontext: Couzigou, S. 14; Lahmann, S. 62.

846 Hathaway et al., S. 849; Lahmann, S. 54.

847 Akande/Liefländer, S. 566.

848 Vgl. IGH, Nicaragua-Urteil, §237; IGH, Ölplattformen-Urteil, §77 (Mehrheitsmeinung). Ruys, S. 110 f. (umschreibt diesen als »quantitativen Ansatz«); Kress, S. 587.

849 Dazu: Ruys, S. 112; Kress, S. 587 m.V.a. Ago, S. 69.

850 Akande/Liefländer, S. 567; Newton/May, S. 270 m.w.V.

851 IGH, Nuklearwaffen-Gutachten, §41 ff. (Mehrheitsmeinung); IGH, Kongo-Urteil, (separate Meinung Richter Kooijmans), §33 f.; Cannizzaro, Contextualizing Proportionality, S. 779, S. 792; Akande/Liefländer, S. 567.

852 Greenwood, MPEPIL 2011, §25, §28; Lahmann, S. 54 f.

853 Lahmann, S. 55; Randelzhofer/Nolte, S. 1426; Wicker, S. 44 ff.

854 Harrison Dinniss, S. 103 m.V.a. Ago, S. 69 §121.

verteidigungsmassnahme bestehen soll.[855] Eine offensichtliche Diskrepanz zwischen den beiden Massnahmen würde demzufolge als unverhältnismässig gelten.[856]

Die vorangehenden Ausführungen zeigen, dass die Kriterien für eine (un-)verhältnismässige Selbstverteidigung im Einzelnen unklar bleiben.[857] Dies impliziert eine beträchtliche Flexibilität in der Anwendung des Verhältnismässigkeitsprinzips, wodurch auch die Einzelfallwürdigung an Relevanz gewinnt.[858] Zudem hängen die Erfordernisse der Notwendigkeit und der Verhältnismässigkeit i.e.S. sowie auch die beiden Unterkonzepte der Verhältnismässigkeit i.e.S. (die quantitative Verhältnismässigkeit sowie die Verhältnismässigkeit zum Ziel) eng zusammen. Einige Autoren verstehen neben dem Konzept der Notwendigkeit auch die beiden Unterkonzepte der Verhältnismässigkeit (i.e.S.) als kumulative Voraussetzungen bzw. differenzieren sie nicht weiter.[859] Allerdings können sich die Konzepte im Einzelfall entgegenstehen: Gemäss Akande/Liefländer kann die Entscheidung für ein jeweiliges Konzept signifikante Auswirkungen für die normative (Nicht-)Legitimierung von Selbstverteidigungshandlungen haben.[860] Als Beispiel führen sie den Fall an, in dem die Gefahr einer Serie von Attentaten die Schwelle eines bewaffneten Angriffs erreicht und der bedrohte Staat annimmt, dass der bewaffnete Angriff nur gestoppt werden kann, wenn das die Attentäter beherbergende Land vollständig invadiert wird.[861] Wenn die erste Lesart, die der Notwendigkeit (»nicht mehr Schaden anrichten als nötig«), angenommen wird, besteht die Einschränkung darin, abzuwägen, ob dasselbe Ziel mit weniger militärischer Gewalt erreicht werden kann. Vertritt der betroffene Staat die Ansicht, dass eine Invasion notwendig ist, würde er dies folglich verneinen.[862] Würde man hingegen dem Konzept der Verhältnismässigkeit folgen, wonach die Selbstverteidigungshandlung quantitativ mit den Ausgangsschäden übereinstimmen müsste, dürfte der Staat nur das gleiche Mass an Gewalt anwenden. Daher wäre gem.

855 Lahmann, S. 55. Siehe Kress, S. 586 ff. zu einer eingehenderen Abhandlung der Verhältnismässigkeit durch den IGH. Der Rechtsprechung zufolge darf eine Verteidigung im Vergleich zum Angriff insgesamt nicht extensiv sein. Die genaue Schwelle zur Exzessivität bleibt letztlich jedoch vage.

856 Green, S. 96; Lahmann, S. 55.

857 Lahmann, S. 55; Green, S. 96; Kress, S. 590.

858 Vgl. Harrison Dinniss, S. 104.

859 Siehe z.B. Lahmann, S. 54 f.

860 Akande/Liefländer, S. 567 f.

861 Akande/Liefländer, S. 567 f.

862 Akande/Liefländer, S. 567.

jener Lesart eine vollständige Invasion eindeutig nicht gerechtfertigt.[863] Schliesslich wäre die Würdigung beim letzten (oft in der Praxis vorgebrachten) Konzept, das eine strikte Proportionalität der Reaktion zum angestrebten *Ziel* der Abwehr verlangt, nicht so klar. Die Abwägung des (drohenden) Schadens mit der (im Einzelfall als zulässig zu qualifizierende) Zielverfolgung implizieren eine komplexe Interessenabwägung.[864] Daraus ergibt sich gem. AKANDE/LIEFLÄNDER die Frage, welches Interesse unter den betreffenden Umständen des Einzelfalls überwiegen soll: Das Interesse an der Verhinderung oder Beendigung eines bewaffneten Angriffs (oder einer Gefahr) oder die Interessen, die durch den Einsatz massiver Gegengewalt verletzt werden?[865]

Während dem quantitativen Konzept der Verhältnismässigkeit zufolge eine Selbstverteidigungshandlung als unproportional gelten kann, könnte man dem Notwendigkeitsprinzip folgend ein ganz anderes Mass an Gewalt rechtfertigen. Ähnlich kann auch das dritte Konzept, je nach Abwägung der Interessen (sowie subjektiver Aufassung der Schädigung oder der Bedrohung) im Einzelfall u.U. eine weit über die ursprüngliche Handlung hinausgehende Gewalt rechtfertigen. Die Argumentation und die Entscheidung für ein Konzept der Verhältnismässigkeit ist folglich massgebend für das jeweilige Ergebnis.[866] Demzufolge bleibt das Verhältnismässigkeitsprinzip im Zusammenhang mit der Selbstverteidigung insgesamt vage, und es ist schwierig, es in der Praxis kohärent anzuwenden.[867] Die Einzelfallwürdigung verschafft hier nicht nur sinnvollen Spielraum, sondern birgt auch das erhebliche Missbrauchspotenzial, im Einzefall dem (strategisch) jeweils passenderen Konzept zu folgen. AKANDE/LIEFLÄNDER und BETHLEHEM sprechen sich daher für eine Klärung des Prinzips aus.[868] Sie unterstreichen die Notwendigkeit objektiv anwendbarer, rechtlicher Kriterien, um staatliches Verhalten überprüfen zu können.[869] Dies erscheint insb. angesichts der Wichtigkeit der involvierten Interessen bei möglichen Selbstverteidigungshandlungen sinnvoll.

863 AKANDE/LIEFLÄNDER, S. 568.

864 AKANDE/LIEFLÄNDER, S. 568.

865 AKANDE/LIEFLÄNDER, S. 568.

866 AKANDE/LIEFLÄNDER, S. 568.

867 AKANDE/LIEFLÄNDER, S. 569.

868 AKANDE/LIEFLÄNDER, S. 570; BETHLEHEM, S. 774.

869 AKANDE/LIEFLÄNDER, S. 570 m.V.a. BETHLEHEM, S. 774 unterstreichen »*the need for legal principles that are ›capable of objective application‹*«.

b. Beeinflussung des Prinzips durch Staatenpraxis und *opinio iuris*

Durch die verbleibende Vagheit des Verhältnismässigkeitsprinzips und dem damit verbundenen Ermessensspielraum gewinnen Staatenpraxis und *opinio iuris* für Auslegungsfragen an Bedeutung.[870] Staatenansichten verschaffen dem Verhältnismässigkeitsprinzip allerdings nicht nur Klärung, sondern fordern die vagen Grenzen (un-)verhältnismässiger Selbstverteidigung auch wiederholt heraus.

GRAY bietet einen Überblick über die Folgen einer extensiven Auslegung der Verhältnismässigkeit gewisser Staaten beim Recht auf Selbstverteidigung.[871] Vorliegend sollen nur einige beispielhafte Ausschnitte aus den in ihren Abhandlungen besprochenen Fällen herangezogen werden, um die inhärenten Interpretationsspielräume und die unterschiedlichen Argumentationsmöglichkeiten zu illustrieren. Die Auseinandersetzung mit den Folgerungen des IGH im Ölplattformen-Urteil vom 6. November 2003 enthält dazu einige Beispiele. Zusammengefasst hatte in jenem Fall der Iran am 2. November 1992 aufgrund von Angriffen auf und der Zerstörung von kommerziellen Ölplattformen eines nationalen iranischen Ölunternehmens einen Prozess gegen die USA eingeleitet. Die USA machten ihrerseits ihr Recht auf Selbstverteidigung geltend, wonach diese Massnahmen für sie notwendig gewesen seien, um essenzielle Sicherheitsinteressen zu schützen.[872] Der IGH hat in seinem Urteil mitunter allerdings entschieden, dass es, wie bereits erwähnt, unter Umständen (im Rahmen der Verhältnismässigkeitsprüfung) nicht notwendig ist, auf gewisse Objekte und Einrichtungen abzuzielen, wenn diese nicht die direkten Quellen eines Angriffs sind und nicht dem Zwecke der Abwehr dienen.[873] Damit hat der IGH ein Recht auf Selbstverteidigung im Ergebnis verneint.[874] In der Folge hat TAFT, der damalige Rechtsberater des US-Aussendepartements,

---

870 Insbesondere auch im Hinblick auf die mögliche Etablierung von Gewohnheitsrecht durch Staatenpraxis und *opinio iuris*: vgl. Art. 38(1)(b) IGH-Statut. Zum potenziellen Einfluss der Staatenpraxis und *opinio iuris* bei Graubereichen (im Cyberkontext): SCHMITT, Grey Zones, S. 20. Näher zu Staatenpraxis und der Etablierung von Gewohnheitsrecht: KAMMERHOFER, Kelsenian Perspective, S. 62 ff.

871 Siehe dazu: GRAY, The Limits of Force, S. 101 ff.; GRAY, Use of Force, S. 227 ff. sowie die Ausführungen zur Notwendigkeit im vorangehenden Abschnitt.

872 IGH, Ölplattformen-Urteil, §1 ff., §36 ff., §51.

873 IGH, Ölplattformen-Urteil, §76, wonach das Abzielen auf bestimmte Objekte mit der Abwehr in Verbindung stehen muss; GRAY, Use of Force, S. 160 f.; KRESS, S. 589.

874 IGH, Ölplattformen-Urteil, §125.

explizit statuiert, dass diese Ansichten des IGH weder die Staatenpraxis widerspiegelten noch von den relevanten Regierungen (wie den USA) unterstützt würden.[875] Aus seiner Sicht war es für die USA notwendig, sich zu ihrem Schutz mit Gewalt gegen die Angriffe des Irans zu wehren. Die zusätzliche Anforderung, dass *nur bestimmte Ziele angegriffen* werden dürften, sei nicht praktikabel und würde das Recht auf Selbstverteidigung untergraben.[876] Indem bei einer Beschränkung auf bestimmte Plattformen die »legitimen« Ziele beiden Konfliktparteien bekannt seien, werde die Verteidigungsmassnahme ihrer Effektivität entleert, da der Gegner jenes Ziel verschieben oder sich dort unangreifbar machen könne. Des Weiteren betonte Taft, dass Intensität und Art einer Selbstverteidigungshandlung nicht beschränkt seien, sondern die Verhältnismässigkeit vielmehr an der jeweiligen *Gefahr* gemessen werden müsse.[877] Damit folgt er weniger einem quantitativen Vergleich, sondern vielmehr der mit grösserem Ermessen verbundenen Abwägung zwischen der Reaktion und dem Ziel, eine (wiederum zu definierende) Gefahr abzuwehren. Hinzu kommt die Haltung, dass auch auf *künftige* Gefahren reagiert werde bzw. dass jeweils geprüft werden müsse, ob ein betreffender Angriff Teil einer Angriffsserie sei, die man abwehren müsse.[878] Dadurch wird einerseits die Notwendigkeit weit verstanden, indem es als notwendig erachtet wird, bevorstehende Schäden abwehren zu können und den Eintritt von Schädigungen nicht abwarten zu müssen. Andererseits resultiert daraus, dass die Verhältnismässigkeitsabwägung so zwischen tatsächlich erfolgter, gewaltsamer Reaktionshandlung und dem aus einer unmittelbar bevorstehenden Gefahr potenziell resultierendem, *künftigem* Schaden erfolgt. Diese Ansichten unterstreichend statuierte Taft, dass die USA ihrerseits weiterhin dem folgen werden, was sie in diesen Punkten als »korrekte Auslegung des Völkerrechts verstehen«.[879] Die Ansicht der USA zur Verhältnismässigkeit ist vom Gedanken geprägt, dass Ein-

875 Taft, S. 300, S. 304. Eingehender zur US-Haltung i.Z.m. dem Ölplattformen-Urteil: Gray, Use of Force, S. 160 f.; Ochoa-Ruiz/Salamanca-Aguado, S. 499 ff.

876 Taft, S. 304.

877 Taft, S. 305.

878 Taft, S. 305 u.a. m.V.a. Schachter, International Law, S. 154. Es handelt sich dabei um die sog. Ereigniskumulationstheorie (im Englischen: »*accumulation of events theory*«). Siehe dazu u.a. Kretzmer, S. 244; Tams, Use of Force, S. 359 ff. Ausführlicher dazu: Gray, Use of Force, S. 227.

879 Taft, S. 306. Eingehender zur Gegenmeinung der USA im Ölplattformen-Urteil u.a. unter Erwähnung der Notwendigkeit siehe die Widerklage vom 23.06.1997: International Court of Justice, Case Concercing Oil Platforms, Counter-Memorial and Counter-Claim submitted by the United States of America, 23 June 1997.

schränkungen von Reaktionsmöglichkeiten Angreiferstaaten »erheblich und in gefährlicher Weise befähigen würden«, bewaffnete Angriffe zu lancieren, ohne dass sie eine Verteidigungshandlung auf ihre Angriffe befürchten müssten.[880]

Ein weiteres Beispiel, in dem die USA sich explizit auf die Notwendig- und Verhältnismässigkeit einer Selbstverteidigungshandlung bezogen, steht im Zusammenhang mit den terroristischen Angriffen vom 11. September 2001 (9/11). Vereinfacht gesagt wurde eine militärische Verteidigung in jenem Fall als notwendig erachtet, um sich gegen die Angriffe bzw. die damit verbundenen Gefahren zu verteidigen.[881] Da eine Selbstverteidigung auf die Abwehr oder die Beendigung eines bewaffneten Angriffs gerichtet sein muss, stellt sich in jenem Zusammenhang allerdings die Frage, ob militärische Gewalt in einem solchen Fall *überhaupt* zur Abwehr geeignet und damit notwendig ist. Gray umschreibt dies als »the limits *of* force«.[882] Zumindest müsste man ab jenem Zeitpunkt die Notwendigkeit einer militärischen Massnahme in Frage stellen, ab dem unklar wird, ob man einen Gegner mit dieser Strategie überhaupt »abwehren« oder »besiegen« kann.[883] Militärische Gewalt muss, wie bereits angeführt, zur Beseitigung einer Gefahr in einem konkreten Angriff notwendig und im Verhältnis zur »Gefahr« verhältnismässig sein. Je länger eine militärische Operation dauert, desto mehr müsste man folglich ihre ursprüngliche Legitimation zur Selbstverteidigung (bzw. ihre Notwendigkeit) in Frage stellen.[884] Kann ein Gegner – in jenem Fall waren es nichtstaatliche Akteure – überhaupt mit militärischen Mitteln besiegt werden?[885] Gray argumentiert dahingehend, dass kontraproduktive und ungeeignete militärische Massnahmen unter Umständen *rechtlich* relevant werden.[886] Wenn ein Gegner und von ihm ausgehende bewaffnete Angriffe mit herkömmlicher militärischer Gewalt nicht

880 Taft, S. 306.

881 Eingehender dazu: Gray, The Limits of Force, S. 113 ff., inbs. S. 115 ff.; Gray, Use of Force, S. 159, S. 227 ff. m.V.a. UN Doc. S/RES/1368 (2001); UN Doc. S/RES/1373 (2001). Ferner dazu: Sapiro, S. 602.

882 Zu den Grenzen von Gewaltanwendungen: Gray, Limits of Force, S. 101 ff.

883 Gray, Use of Force, S. 231. Ähnlich: Münkler, S. 241.

884 Die sich auf die Sicherheitsratsresolution UN Doc. S/RES/1368 (2001) beziehende Operation Enduring Freedom in Afghanistan hielt dreizehn Jahre an (bis zum 28.12.2014) und der militärischen Präsenz in Afghanistan wurde erst zwanzig Jahre später ein Ende gesetzt. Dazu: Gray, Use of Force, S. 231; Steinvorth, NZZ vom 14.04.2021.

885 Münkler, S. 187 ff., S. 241. Gemäss Gray ging die Operation über das ursprüngliche Argument der Selbstverteidigung in den Sicherheitsratsresolutionen UN Doc. S/RES/1368 (2001) und UN Doc. S/RES/1373 (2001) hinaus, womit sie ohne ausdrückliche UN-Grundlage fortgesetzt wurde: Gray, Use of Force, S. 231.

886 Gray, Use of Force, S. 231 m.w.V.; Gray, The Limits of Force, S. 101 ff.

abwehrbar und die damit ausgelösten Folgeschäden insgesamt nicht gerechtfertigt sind, müsste man rechtlich gesehen folglich auch die Notwendig- und Verhältnismässigkeit militärischer Gewalt in solchen Konstellationen absprechen. In der Praxis kann es sodann mit fortwährendem Konflikt sehr schwierig sein, eine Verteidigung von einer Vergeltung zu unterscheiden.[887] Zudem ist die Verhältnismässigkeit im Hinblick auf Selbstverteidigungsmassnahmen gegen nichtstaatliche Akteure jeweils zusätzlich kritisch zu hinterfragen.[888] Solange dem die nichtstaatlichen Akteure beherbergenden Staat vor dem Ergreifen einer militärischen Aktion keine Möglichkeit gegeben wird, selbst aktiv zu werden und dieser nicht die Erlaubnis erteilt, in seinem Territorium militärisch vorzugehen, müsste die Verhältnismässigkeit einer Selbstverteidigungsmassnahme streng juristisch gesehen – zumindest der Theorie zufolge – verneint werden.[889] Vor dem Hintergrund der Verhältnismässigkeit wäre in einer solchen Konstellation die Selbstverteidigungsmassnahme grundsätzlich nicht gem. Art. 51 UN-Charta gerechtfertigt.[890]

Die (jeweils subjektive) Wahrnehmung und Definition einer Gefahr wird im Ergebnis die Würdigung von dem, was als notwendig und verhältnismässig eingestuft wird, immer beeinflussen. Bereits im Nicaragua-Urteil hatten die USA argumentiert, dass es ihnen selbst vorbehalten sein müsse, über die Notwendigkeit ihrer Selbstverteidigung zu entscheiden, da dies eine subjektive Angelegenheit sei.[891] Die unterschiedlichen Argumentationsmöglichkeiten, die fundamental divergierende praktische Folgen nach sich ziehen, widerspiegeln letzlich die Massgeblichkeit von Interpretationsspielräumen internationaler Normen. Letztlich wird jeder internationale Konflikt von einem inhärenten Spannungsverhältnis geprägt sein: Und zwar demjenigen zwischen dem Bedürfnis eines Staates, öffentliche Sicherheitsinteressen möglichst zu verteidigen und dem unter Umständen entgegenstehenden Interesse der internationalen Gemeinschaft, militärische Gewalt, wenn nur möglich, einzuschränken.[892]

887 Gray, Use of Force, S. 160, S. 205. Ferner: Wicker, S. 48 f.

888 Dazu u.a.: Heinze, S. 95.

889 Vgl. die vorangehenden Ausführungen und Verweise u.a. auf Akande/Liefländer, S. 566.

890 Heinze, S. 95.

891 Das war auch die richterliche Gegenmeinung von Richter Schwebel: IGH, Nicaragua-Urteil, (Gegenmeinung Richter Schwebel), §69 ff. Dazu: Gray, Limits of Force, S. 132.

892 Vgl. Dazu: Ochoa-Ruiz/Salamanca-Aguado, S. 499 ff.

Unabhängig davon, ob man der US-amerikanischen Haltung folgt, kann man festhalten, dass diese den völkerrechtlichen Diskurs mitgestaltet und beeinflusst.[893] Nicht nur wurde die grundsätzliche Möglichkeit einer Selbstverteidigung gegen nichtstaatliche Akteure eröffnet,[894] sondern es wurden auch die zeitlichen Schranken der Selbstverteidigung sowie die Beschränkung zulässiger Ziele in Frage gestellt.[895] Da die Staatenpraxis weiterhin eine prominente Rolle im Völkerrecht spielt, werden diese Aspekte wohl auch im Hinblick auf den Umgang mit Gefahren (und mit nichtstaatlichen Akteuren) im Cyberkontext Auswirkungen haben.[896]

c. Zwischenfazit

Im Ergebnis beeinflussen die Staatenpraxis sowie die *opinio iuris* das Völkerrecht massgeblich. Durch die Etablierung von Gewohnheitsrecht können grundsätzlich neue Grenzen definiert und damit potenziell auch künftige Entscheidungen legitimiert werden. Dies insb. angesichts der grundsätzlichen Absenz von Normenhierarchien im Völkerrecht.[897]

Wie aufgezeigt, sind die Konzepte der Verhältnismässig- und Notwendigkeit zu vage, um starre, vordefinierte Grenzen zu setzen, und sie lassen dementsprechend erheblichen Raum für Interpretation.[898] Dieser Spielraum ist mitunter erwünscht, um das Prinzip flexibel zu halten und im Einzelfall Interessenabwägungen vornehmen zu können.[899] Innerhalb dieses Spielraums erscheint die Diskussion zur Verhältnismässigkeit jedoch weitgehend polarisiert: Staaten, die angegriffen werden, neigen (zumindest *ad hoc*) zu extensiven Ansichten, während andere, unbeteiligte Staaten tendenziell zu einer restriktiveren Handhabung des Prinzips aufrufen.[900] Letztlich werden somit nicht nur

893 Näher dazu: GRAY, Use of Force, S. 205 ff.

894 Ausführlicher zur Verhältnismässigkeit bei gewaltsamer Selbstverteidigung gegen Terrorismus: WICKER, S. 61 ff.

895 Dazu u.a.: WICKER, S. 64.

896 Siehe dazu: LAHMANN, S. 62 m.w.V.

897 DÖRR, S. 580. Eingehender zur Theorie und Praxis von Völkerrechtsquellen: ROBERTS/SIVAKUMARAN, S. 89 ff.

898 Zu inhärenten Interpretationsspielräumen bei der Anwendung von Völkerrecht: KAMMERHOFER, Kelsenian Perspective, S. 121 ff., S. 124.

899 WICKER, S. 7. Vgl. dazu GARDAM, Proportionality and Force, S. 412: »*It appears that the endless flexibility of the principle is both its strength and its weakness*«.

900 Siehe z.B. die sich gegenüberstehenden Ansichten in: UN Doc. S/PV 5493 (2006); UN Doc. S/PV 5511 (2006). Ausführlicher dazu: GRAY, Use of Force, S. 227 ff.

objektiv-restriktive, sondern eben auch extensive, aus Affektsituationen entspringende Haltungen, die Etablierung und Weiterentwicklung von Völkerrecht mitprägen und damit beeinflussen, wie Konflikte insgesamt geführt oder bestenfalls gelöst werden. Es stellt sich die Frage, ob die Meinung von »Gefahren« betroffener Staaten in einem konkreten Fall mehr ins Gewicht fallen sollte. Verdienen sie aufgrund ihrer erhöhten Betroffenheit mehr Gehör für ihre (Sicherheits-)Interessen? Rührt umgekehrt eine restriktive Handhabung von Prinzipien vielleicht auch etwas von einer privilegierten, »sicheren« und von einer Gefahr distanzierten Position? Letztlich – und dies ist wichtig für eine balancierte Herangehensweise – wird es in jedem Konflikt um Abwägungen gehen. Eine zu restriktive Ansicht, militärische Gewalt, wenn immer möglich einzuschränken, scheint *in abstracto* zwar erstrebenswert, wäre gleichzeitig jedoch zu weitgehend, wenn von einem Staat in einem akuten Angriffsfall pauschal und ausnahmslos verlangt würde, diplomatische Lösungen zu suchen, wenn jener solche Lösungen nicht sieht.[901] Retrospektiv lässt sich teilweise ein Sachverhalt nüchterner betrachten als dies in einer akuten Bedrohungslage möglich gewesen wäre. Dies zeigt die Schwierigkeit, starre juristische Vorgaben für jeden Fall vorzusehen. Damit kommt man in der Praxis nicht um eine Würdigung der konkreten Umstände des jeweiligen Einzelfalles herum.[902] Von diesen, dem Völkerrecht praktisch innewohnenden Spannungsverhältnisse einmal abgesehen, lässt sich folgendes dennoch festhalten: Unabhängig der jeweils zugrundeliegenden, subjektiv berechtigten oder nicht berechtigten Gründe geht mit einer *extensiven* Auslegung des Verhältnismässigkeitsprinzips die grundsätzlich machteindämmende Wirkung desselben eher verloren. Extensive Interpretationen kurbeln Gewaltspiralen in der Praxis wohl eher an, als dass sie diese abkühlen.[903] Zudem bleibt es vorliegend zu betonen, dass es beim Verhältnismässigkeitsprinzip eben gerade nicht darum geht, keine Verteidigung zu ermöglichen, sondern keine *übermässige*.[904] Eine Verteidigung soll nicht *per se* verwehrt werden, sondern es soll vielmehr gewürdigt werden, inwieweit und unter welchen Bedingungen militärische Massnahmen notwendig und verhältnismässig sind, um einen Angriff zu *beenden*.

901 Kress, S. 588 (m.V.a. IGH, Ölplattformen-Urteil, §76) sowie S. 589.

902 Wilmshurst et al., S. 967.

903 Ähnlich: Gray, The Limits of Force, S. 101 ff.

904 Siehe die Ausführungen zur Verhältnismässigkeit unter II.B.3. und IV.A.

Eine der wesentlichen Herausforderungen im Zusammenhang mit dem Verhältnismässigkeitsprinzip wird es folglich bleiben, dass die Interpretationen desselben jeweils sehr subjektiv geprägt sind.[905] Dieser Umstand ist vor dem Hintergrund dieser Dissertation besonders hervorzuheben, da es bei der vorliegenden Thematik um *unilateral* getroffene Massnahmen geht. Es ist am jeweiligen Staat zu entscheiden, ob er mit gewaltsamer Selbstverteidigung handeln soll oder nicht.[906] Gemäss WICKER warf die nachfolgende Aussage von Hersch Lauterpacht sogar die Frage auf, ob nicht nur die Entscheidung zur Selbstverteidigung an sich, sondern darüber hinaus auch die Würdigung der getroffenen Massnahme dem betroffenen Staat überlassen werden soll:[907] »*(recourse to self-defence) must be a matter for the judgement of the State concerned. For if recourse to it were conditioned by a previous authorization of a law-administering agency, then it would no longer be self-defence; it would be execution of a legal decision. Self-defence is incapable of being defined in advance, and it must therefore be left to the State concerned to decide in each individual case whether the circumstances justify recourse to war in self-defence*«.[908] Wird diese Ansicht dahingehend verstanden, einem Staat zu ermöglichen, die Legalität seiner eigenen Handlungen (u.a. anhand der Verhältnismässigkeit) zu beurteilen, ist sie mit grosser Vorsicht zu betrachten, wenn nicht abzuweisen.[909] Die vorangehend aufgezeigten Beispiele zeigen, wie wichtig die Unterscheidung von subjektiver Überzeugung und objektiven Kriterien ist.[910] Zwar muss ein Staat im Rahmen der unilateralen Selbsthilfe ausnahmsweise gerade keine rechtliche Bewilligung des Sicherheitsrats zur Selbstverteidigung abwarten. Dennoch würde die Ermächtigung eines Staates, nicht nur

905 Vgl. FRANCK, Proportionality, S. 716: »*It is said about the principle of proportionality that, like beauty, it exists only in the eye of the beholder*.« Er sieht diese Aussage zwar als plausibel, kommt im Ergebnis jedoch zum Schluss, dass dies nicht stimme, da sich durch die Anwendung des Prinzips durchaus klare (objektive) Anhaltspunkte herauskristallisier haben: S. 718.

906 Vgl. WOLTAG, S. 181; ZEMANEK, MPEPIL 2013, §2.

907 WICKER, S. 50.

908 LAUTERPACHT, S. 179.

909 WICKER, S. 50. Ähnlich argumentierte Richter Schwebel in seiner Gegenmeinung im Nicaragua-Fall dahingehend, dass die Beurteilung davon, ob eine Selbstverteidigung notwendig ist dem betreffenden Staat (in jenem Fall den USA) vorbehalten bleiben müsse: IGH, Nicaragua-Urteil, (Gegenmeinung Richter Schwebel), §69 ff. Der IGH teilte die Gegenmeinung von Richter Schwebel im Nicaragua-Urteil allerdings nicht, indem er die Würdigung der Notwendigkeit einer Selbstverteidigung als eine objektive erachtete. Dazu auch: GRAY, Limits of Force, S. 133.

910 WICKER, S. 51.

selbst darüber zu entscheiden *ob*, sondern auch *wie* er auf einen (aus seiner Sicht) bewaffneten Angriff reagieren möchte, den eigenen Ermessenspielraum wohl übermässig ausweiten.[911] Ein Angegriffener wird in einer konkreten Angriffssituation wohl regelmässig für eine extensive Handhabung von Verteidigungsmöglichkeiten plädieren. Aus subjektiver Sicht eines Angegriffenen wird meist das Gefühl vorherrschen, dass eine von ihm getroffene Abwehr sich aufdrängte und notwendig war, und es ist fraglich, ob ein Staat *post facto* sein eigenes Verhalten als völkerrechtswidrig qualifizieren wird. Eine zu weitgehende Subjektivität hat letztlich das Potenzial, die machteindämmende Funktion des Verhältnismässigkeitserfordernisses zu untergraben und dieses in politisch-strategische Bereiche zu verlegen,[912] statt als rechtliches Prinzip zu stärken.

Aus den erwähnten Gründen ist die Beurteilung der Legalität einer Selbstverteidigungsmassnahme durch unbeteiligte Drittpersonen sehr wichtig. Gemäss WICKER ist es unentbehrlich, dass Drittparteien die Rechtmässigkeit einer Selbstverteidigungsmassnahme *post facto* (und aufgrund objektiver Kriterien)[913] beurteilen können sollen: »*The individual state necessarily decides whether or not to use force in self-defence but the propriety of its decision is to be determined by the* UN. *It is true that self-defence, under general international law, is a right and not a duty but whether a State is correct in referring to self-defence is to be determined by law, especially since it is one of the main purposes and functions of international law, to determine the legality of a State's actions.*«[914] Wenn jeder Staat selbst darüber entscheiden könnte, wann und in welchem Ausmass er militärische Gewalt anwenden darf, würde das die gewalteindämmende Funktion des Völkerrechts untergraben. Um dem erheblichen Gewicht der Staatenpraxis entgegenzuwirken, ist es somit besonders wichtig, dass unbeteiligte, objektive Staaten ihre Meinungen (*opinio iuris*) weiterhin äussern und der nüchterne, wissenschaftliche Diskurs sowie IGH-Urteile herangezogen werden. Ähnlich hat der IGH in seinem Ölplattformen-Urteil festgehalten, dass die Würdigung der Notwendigkeit einer Selbstver-

911 WICKER, S. 51.

912 WICKER, S. 67 m.V.a. KAIKOBAD, S. 318.

913 Er schlägt dazu in seinem Kapitel 3 einen objektiven Verhältnismässigkeits-Test vor: WICKER, S. 205 ff.

914 WICKER, S. 52 m.w.V. Ähnlich: SCHACHTER, Rule of Law, S. 266: »*If (…) each State remained free to decide for itself when and to what extent it may use force, the legal restraint on force would virtually disappear*«.

teidigungsmassnahme eine strikte und objektive sei.[915] Bei dieser Frage gäbe es keinen Ermessensspielraum (»*no room for any measure of discretion*«).[916] Daher wird ein Staat seine militärischen Handlungen vor der internationalen Staatengemeinschaft weiterhin rechtfertigen müssen, und es wird ihm vermittelt, dass er nicht unilateral über sein Verhalten *und* die Verhältnismässigkeit desselben entscheiden kann. Die Stärkung objektiv-rechtlicher Aspekte des Verhältnismässigkeitsprinzips ist dabei gerade auch im Hinblick auf den Cyberkontext von Relevanz. So scheint es unumgänglich, dass auch künftig die subjektive Auffassung von Bedrohungen und Verletzlichkeiten durch Cyberangriffe (oder andere Gefahren) zwischen den Staaten variieren wird. Sehr digital aufgestellte Staaten sind letztlich nämlich tatsächlich viel angreifbarer und verletzbarer als weniger digitale Staaten,[917] womit sich Subjektivitäten und ungleiche Bedrohungsstrukturen wohl weiterziehen werden.

2. Verhältnismässige Selbstverteidigung gegen Cyberangriffe?

a. *Ius ad bellum*-Verhältnismässigkeit bei Cyberangriffen

Die Konzepte der Notwendig- und der Verhältnismässigkeit gelten im Rahmen der Selbstverteidigung grundsätzlich gleichermassen für den Cyberkontext wie sie dies im herkömmlichen Kontext tun.[918] Die beiden Elemente werden dabei zumindest im Tallinn Manual 2.0 kumulativ verstanden: »*Proportionality addresses the issue of how much force, including use of cyber force, is permissible once force is deemed necessary*«.[919]

Die Verhältnismässigkeit setzt auch im Cyberkontext weder voraus, dass der sich verteidigende Staat dieselben Waffen[920] einsetzen muss wie der Angreifer, noch beschränkt sie Verteidigungshandlungen auf das eigene Territorium.[921] Der Verteidigerstaat kann daher gem. Tallinn Manual grundsätzlich die ihm

915 IGH, Ölplattformen-Urteil, §73 (seine Haltung im Nicaragua-Urteil bestätigend). Dazu: Gray, Limits of Force, S. 133.

916 IGH, Ölplattformen-Urteil, §73. Dazu: Harrison Dinniss, S. 102; Gray, Limits of Force, S. 132 f.

917 Zegart, TED vom 29.06.2015.

918 Siehe: Tallinn Manual 2.0, S. 348 ff., R72 f., sowie S. 347, R71 C23. Ähnlich: U.S. International Strategy for Cyberspace 2011, S. 14; Hathaway et al., S. 849.

919 Tallinn Manual 2.0, S. 349 R72 C5.

920 Tallinn Manual 2.0, S. 348 R72 C2, C5.

921 Harrison Dinniss, S. 104.

verfügbaren, geeigneten Cyber- oder nicht-Cybermittel anwenden, solange die Reaktion zur Abwehr insgesamt »verhältnismässig« sei[922] und nicht eskaliere.[923] Demnach könnten Cyberangriffe laut Tallinn Manual grundsätzlich bei Erfüllung der Voraussetzungen eines bewaffneten Angriffs i.S.v. Art. 51 UN-Charta (in Übereinstimmung mit der Verhältnismässigkeit) zu kinetischen Reaktionen und umgekehrt ein traditioneller Angriff zu Cybergegenmassnahmen führen.[924] Zudem könnten militärische Reaktionen mit andersartigen Mitteln wie ökonomischen oder diplomatischen Sanktionen kombiniert werden.[925]

Gesamthaft betrachtet hat das Tallinn Manual ähnlich der vorangehend unter IV.A.1.b. angeführten US-amerikanischen Haltung einen tendenziellen Fokus auf der Notwendigkeit, einen Angriff (bzw. eine Gefahr) abzuwehren, statt auf einem quantitativen Vergleich der beiden Massnahmen.[926] Dies ist im Kern vergleichbar mit dem mit einem grösseren Ermessensspielraum verbundenen Verhältnismässigkeitskonzept, dass Verteidigungshandlungen jeweils am Ziel, eine Gefahr zu beseitigen, gemessen werden müssen. Diese Argumentation belässt, wie im vorangehenden Abschnitt IV.A.1. aufgezeigt, einen erheblichen Spielraum, die zu beseitigende Gefahr sowie die auf dem Spiel stehenden Interessen zu definieren. Gemäss Tallinn Manual könnten in diesem Sinne je nach Situation unterschiedliche Intensitäten von Gewalt als notwendig erachtet werden, um sich erfolgreich i.S.v. Art. 51 UN-Charta verteidigen zu können.[927] Es sei demzufolge kontextabhängig, ob mehr oder weniger Gewalt ausreichend sei.[928] Die Verhältnismässigkeit setze daher nicht zwingend eine friedliche Reaktion auf einen bewaffneten Angriff voraus.[929] Damit das Recht auf Selbstverteidigung seiner Bedeutung nicht entleert werde, müsse es einem angegriffenen Staat, dem keine friedlichen Massnahmen zur Verfügung stehen, möglich sein, zu gewaltsamen Mitteln zu greifen, um seine Interessen zu verteidigen.[930] Aus den ergänzenden Ausführungen der Lehre wird allerdings geschlossen, dass die Intensität einer Gegenhandlung auch im Cyberkontext

922 Harrison Dinniss, S. 104; Jensen, Cyber Deterrence, S. 800.

923 Hathaway et al., S. 849; Jensen, Cyber Deterrence, S. 800.

924 Tallinn Manual 2.0, S. 349 R72 C5.

925 Tallinn Manual 2.0, S. 349 R72 C2.

926 Siehe: Tallinn Manual 2.0, S. 349 R72 C5.

927 Tallinn Manual 2.0, S. 349 R72 C5. Ähnlich: Greenwood, MPEPIL 2011, §28; Lahmann, S. 55; Randelzhofer/Nolte, S. 1426.

928 Tallinn Manual 2.0, S. 349 R72 C5.

929 Tallinn Manual 2.0, S. 350, R72 C6.

930 Tallinn Manual 2.0, S. 349 R72 C3; Lahmann, S. 64; Keber/Roguski, S. 416.

quantitativ nicht klar disproportional sein darf.[931] Das heisst, das quantitative Abwägen der beiden Massnahmen soll gewissermassen als äusserste Schranke dienen.

Wie im traditionellen Kontext auch, dürfen keine zur Gewaltanwendung alternativen milderen Massnahmen zur Verfügung stehen.[932] Eignen sich also passive defensive Cybergegenmassnahmen wie Firewalls oder automatische Früherkennungsprogramme[933], um einen Cyberangriff im Rahmen von Art. 51 UN-Charta zu beenden oder zu verhindern, würden darüber hinausgehende aktive Cybergegenmassnahmen regelmässig als unzulässig kategorisiert.[934] Ähnlich wären den Experten des Tallinn Manuals zufolge kinetische Massnahmen unzulässig, wenn aktive Cybermassnahmen unterhalb der Gewaltverbotsschwelle genügen, um einen Angriff abzuwehren.[935]

Zusammengefasst hat sich die Expertengruppe folglich darauf einigen können, dass die völkerrechtliche Verhältnismässigkeit im Cyberbereich einerseits die Notwendigkeit einer Abwehr (mildestes Mittel) voraussetzt sowie andererseits die Angemessenheit der Massnahme, um eine Gefahr oder Schädigung abzuwehren (Zweck-Mittel-Relation).[936] Das Erfordernis der *Geeignetheit* einer Massnahme wird im Tallinn Manual nicht explizit statuiert. Der vorliegenden Ansicht nach impliziert, wie vorangehend unter IV.A.1. angeführt, das Ziel der Abwehr eines Angriffes allerdings auch, dass die getroffene Massnahme über-

931 Vgl. Hathaway et al., S. 849; Harrison Dinniss, S. 104; Green, S. 96; Greenwood, MPEPIL 2011, §28; Jensen, Cyber Deterrence, S. 800; Lahmann, S. 55.

932 Tallinn Manual 2.0, S. 349 R72 C3. Dieser Ansicht ist grundsätzlich auch die Lehre: Lahmann, S. 63; Roscini, Cyber Operations, S. 89.

933 Zu automatisierten Erkennungsprogrammen: Denning, Information Warfare, S. 361 ff.

934 Tallinn Manual 2.0, S. 349 R72 C3. Ebenso: Lahmann, S. 63; Stein/Marauhn, S. 8.

935 Tallinn Manual 2.0, S. 349 R72 C3.

936 Tallinn Manual 2.0, S. 349 R72 C3.

haupt dazu geeignet sein muss. Die Grundidee der Selbstverteidigung, dass sie auf die Abwehr einer Gefahr bzw. eines Angriffs gerichtet sein muss (gewissermassen ihre »raison d'être«), unterstreicht dieses implizite Erfordernis.[937]

Im Folgenden sollen die einzelnen Aspekte der Verhältnismässigkeit völkerrechtlicher Selbstverteidigungsmassnahmen nach Art. 51 UN-Charta bei Cyberangriffen näher beleuchtet werden. Insbesondere der Einsatz aktiver digitaler Verteidigungsmassnahmen gegen Cyberangriffe gem. Art. 51 UN-Charta erweist sich vor dem Hintergrund der Verhältnismässigkeit als sehr komplex[938] bzw. als wesentlich komplexer als es u.a. im Tallinn Manual zur Geltung kommt. Die Möglichkeit digitaler Verteidigungshandlungen wie bspw. Hackbacks erweitert nämlich nicht nur das Spektrum potenziell verhältnismässiger[939], sondern nach vorliegend vertretener Ansicht ebenso potenziell unverhältnismässiger Reaktionen. Zu erinnern ist, dass unter Hackback *per definitionem* grundsätzlich »Hacking« zu verstehen ist, das ein Eindringen in fremde Systeme impliziert.[940] Obschon dies nicht zwingendermassen in jedem Fall notwendig ist, muss ein Staat offensive Cyberkapazitäten besitzen, um digitale Gegenangriffe lancieren zu können. Zu diesem Zweck wird ein Staat entdeckte technische Sicherheitslücken in Software oder Hardware i.d.R. nicht offenlegen, um sich diese für Hackbacks vorzubehalten.[941] Hinzu kommt die Vielzahl an möglichen Effekten eines Cyber(gegen-)angriffs sowie, dass ein digitales Zurückschlagen zu unvorhergesehenen, unter Umständen physischen Effekten ausserhalb des angegriffenen Computersystems führen kann.[942] So z.B., wenn sich ein Schadprogramm unkontrolliert weiterverbreitet und/oder unbeteiligte (kritische) Infrastrukturen trifft, die lediglich als Brückenkopf oder paketvermittelnde Router für den ursprünglichen Angriff dienten.[943] Da

937 Siehe die Argumentationslinie des IGH, der (wie vorangehend erwähnt) im Ölplattformen-Urteil, §76, das Abzielen auf bestimmte Objekte als nicht notwendig erachtete, da diese nicht mit der Abwehr in Verbindung standen. Dies impliziert, dass eine Massnahme gewissermassen zur Abwehr geeignet sein muss. Zu ähnlichen Argumentationslinien in der Lehre, dass eine Verteidigungsmassnahme auf die Beseitigung einer Gefahr gerichtet sein muss: Nolte, A Response to Kretzmer, S. 290; Newton/May, S. 270 m.V.a. Jennings, S. 89. Ferner auch: Banks/Criddle, S. 89 f.: »military action is permissible in response to cyber attacks only if such action is strictly necessary *and narrowly tailored* to prevent grave and imminent harm« (Kursivsetzung durch die Autorin).

938 Lahmann, S. 64.

939 Jensen, Cyber Deterrence, S. 800.

940 Lahmann, S. 279.

941 Baumgärtner et al., Der Spiegel vom 24.08.2018; Lahmann, S. 279.

942 Dewar, Active Cyber Defense, S. 5.

943 Lahmann, S. 64.

solche Folgen im Voraus oft schwer kalkulierbar sind, könnte unter Umständen auch ein grundsätzlich als verhältnismässig erachteter Hackback sich letztlich als unverhältnismässig erweisen.[944]

b. Notwendigkeit einer Selbstverteidigung

Das Erfordernis der Notwendigkeit wirft im Cyberkontext die Frage auf, wann und inwiefern eine Selbstverteidigungshandlung auf einen Cyberangriff notwendig ist. Um diese Frage zu beantworten ist es vorerst zentral, definieren zu können, wann der Cyberangriff unmittelbar bevorstehend ist, wann er beginnt und wann er beendet ist. Denn wie unter III.B.1.a. angeführt, ist die Ausübung des Selbstverteidigungsrechts grundsätzlich auf einen frühestmöglichen und spätestzulässigen Zeitpunkt beschränkt.[945] Die Frage, von wann bis wann ein bewaffneter Angriff gem. Art. 51 UN-Charta gegeben ist, ist dogmatisch somit nicht nur für die Bejahung des bewaffneten Angriffs an sich von Relevanz, sondern auch für die Prüfung des Notwendigkeitserfordernisses: Denn das Zurückschlagen auf abgeschlossene Angriffe ist streng gesehen nicht mehr notwendig, um diese abzuwehren. Ähnlich muss die Notwendigkeit einer aktiven Selbstverteidigungsmassnahme für *bevorstehende* Schädigungen durch Cyberangriffe sehr gut begründet werden können.[946] Die zeitliche Herausforderung bei Cyberangriffen stellt sich somit sowohl bei der Definierung eines bewaffneten Angriffs als auch bei der darauffolgenden Würdigung der Verhältnismässig- und Notwendigkeit einer Selbstverteidigungsmassnahme. Die Würdigung der Verhältnismässigkeit einer Selbstverteidigungshandlung hängt deshalb, wie bereits erwähnt, auch mit der vorangehenden Definition eines bewaffneten Angriffs zusammen, und umgekehrt beeinflusst das Verständnis des Notwendigkeitserfordernisses auch die Bedeutung der Selbstverteidigung als Abwehrrecht (oder dessen Ausweitung).[947] Da nach vorliegender Auffassung das Recht auf Selbstverteidigung einen bewaffneten Angriff mit destruktiven physischen Schäden und/oder Toten voraussetzt,[948] werden vorliegend der Beginn und das Ende eines Cyberangriffs im Rahmen von Art. 51 UN-Charta

944 Lahmann, S. 64; Roscini, Cyber Operations, S. 90. Ähnlich: Aldrich, S. 258 auf die Unkontrollierbarkeit aktiver Gegenmassnahmen verweisend.

945 Diggelmann/Hadorn, S. 262; Kammerhofer, Restrictivist Rules, S. 629 m.V.a.

946 Es besteht kein klarer Konsens innerhalb der Staatenpraxis, ab welchem Zeitpunkt konkret eine Selbstverteidigungshandlung als notwendig erachtet wird: Lahmann, S. 55; Randelzhofer/Nolte, S. 1421 ff.

947 In Bezug auf eine mögliche zeitliche Ausweitung des Anwendungsbereichs: Lahmann, S. 55.

948 Zu den Voraussetzungen des bewaffneten Angriffs siehe vorangehend unter III.B.1.a.

an dessen *physischen* Schäden gemessen. Denn ohne klar messbare physische Schäden würde man sich der vorliegenden Ansicht zufolge nicht im Anwendungsbereich eines bewaffneten Angriffs nach Art. 51 UN-Charta bewegen.

In einem ersten Schritt sollen die Phasen von Cyberangriffen näher aufgegriffen werden, um zu eruieren, ab und bis wann man sich bei Cyberangriffen überhaupt im Bereich einer legitimen Selbstverteidigung befindet. Mit anderen Worten: von wann bis wann davon auszugehen ist, dass Cyberangriffe im Gange sind. Darauffolgend sollen nur in Bezug auf die zur Selbstverteidigung infrage kommenden Kategorie *anhaltender* Cyberangriffe die weiteren Erfordernisse des mildesten Mittels sowie der Geeignetheit aufgegriffen werden. Wichtig zu betonen ist, dass das beschränkte Zeitfenster grundsätzlich gleichermassen für traditionelle und für digitale Selbstverteidigungshandlungen gilt. Die Verhältnismässigkeitsprüfung von Art. 51 UN-Charta bezieht sich dabei grundsätzlich auf den Einsatz *offensiver* Selbstverteidigungsmassnahmen und nicht passiver Massnahmen. Passive (digitale) Verteidigungsmassnahmen, mittels derer nicht in ein fremdes System eingedrungen oder ein solches beschädigt wird, sind mangels Effekten an fremden Systemen gem. vorliegender Ansicht nicht vor dem Hintergrund von Art. 51 UN-Charta zu betrachten, sondern gegebenenfalls gem. anderweitig relevanter Rechtsgrundlagen.[949]

i. Unmittelbar bevorstehender und beginnender Cyberangriff: Unklare Schäden

Wie beschrieben, vertritt ein Teil der Lehre und der Staaten die Ansicht, dass es notwendig sein müsse, sich bereits gegen einen *unmittelbar bevorstehenden* Angriff oder gegen eine davon ausgehende Gefahr wehren zu können und einen Eintritt der Schädigung nicht abwarten zu müssen, da ansonsten das Recht auf Selbstverteidigung verwehrt würde.[950]

---

[949] Dies schliesst allerdings, wie vorangehend unter III.A.4. erwähnt, eine Anwendbarkeit anderweitiger Rechtsregime nicht aus.

[950] Tallinn Manual 2.0, S. 349 R72 C3. Ähnlich ist Jensen im Cyberkontext für eine antizipatorische Möglichkeit, sich mit aktiver Cyberverteidigung auf Cyberangriffe (auch von nichtstaatlichen Akteuren) gegen kritische Infrastrukturen wehren zu können, auch wenn sie noch keinen bewaffneten Angriff darstellen: Jensen, Critical National Infrastructure, S. 239 f. Ähnliche rechtliche Fragen sind im Hinblick auf die zunehmende Entwicklung automatisierter digitaler Verteidigungsmittel absehbar, die in »Echtzeit« (was bei Cyberangriffen gegebenfalls noch keine physischen Effekte impliziert) eingesetzt würden: vgl. u.a. Jensen, Critical National Infrastructure, S. 231. Dazu auch: Harrison Dinniss, S. 91 ff., insb. S. 93; Lahmann, S. 63.

Eine rechtliche Herausforderung bei Cyberangriffen ist es folglich, zu bestimmen, wann der für den Anwendungsbereich der Selbstverteidigung relevante Angriff beginnt: Ist bspw. ein Schadprogramm im System, sind jedoch (noch) keine kinetischen Schäden ausgelöst worden, fragt sich, ob der Cyberangriff bereits im Gang oder noch unmittelbar bevorstehend ist. Je nach Argumentation befindet man sich dann in der Diskussion antizipatorischer oder »herkömmlicher« Selbstverteidigung. In diesem Zusammenhang zu betonen ist jedoch, dass bei Cyberangriffen, die noch keine physischen Schäden ausgelöst haben, grundsätzlich unklar ist, ob und in welchem Masse die zu erfolgenden physischen Effekte überhaupt eintreffen werden. Eine konkrete, für das Selbstverteidigungsrecht relevante »Cybergefahr« im Vorfeld konkreter Schäden zu definieren ist daher eine Herausforderung. Es ist extrem schwierig genau festzustellen, welche konkreten (physischen) Effekte von einem (unmittelbar bevorstehenden oder bereits begonnenen) Cyberangriff ausgehen werden.[951] Anders als bei herkömmlichen Angriffen sind die tatsächlich ausgelösten Effekte oder Schäden eines Cyberangriffs teilweise erst Wochen oder Monate später ersichtlich. So ist meist auch dem Urheber des Angriffs bis zur Entdeckung nicht klar, ob etwas »Nützliches« aus dem Angriff resultiert,[952] oder resultieren wird. Dies trifft insb. zu, wenn Daten gesammelt werden müssen. So kann es unter Umständen Jahre dauern, bis die beabsichtigten Informationen erfolgreich operationalisiert werden können.[953] Wenn z.B. durch Früherkennungssysteme Systembeeinträchtigungen oder Schadprogramme entdeckt werden, ist es technisch sehr schwierig abzuschätzen, welche mittelbaren physischen Schäden bzw. ob überhaupt physische Schäden ausgelöst werden.

In der Lehre wurde die Frage aufgeworfen, wie (und ob) das Notwendig- und Verhältnismässigkeitsprinzip Staaten beschränken sollte, auf Cyberangriffe zurückschlagen zu können, *bevor* das Gesamtbild und die kinetischen Effekte bekannt sind.[954] Gemeint ist auch hier nicht die Beschränkung passiver Verteidigungsmechanismen, sondern aktiver, offensiver Selbstverteidigungshandlungen. Einerseits würde gem. Petkis ein Zuwarten auf das Eintreffen von Schäden das Selbstverteidigungsrecht unnütz machen (ähnlich der US-amerikanischen Argumentation bei der antizipatorischen Selbstverteidigung).[955] Andererseits stellt sich die Frage, wie weit man die Notwendigkeit einer Ver-

951 Petkis, S. 1440. Ähnlich dazu: Lahmann, S. 63; Roscini, Cyber Operations, S. 79 ff.

952 Petkis, S. 1448.

953 Petkis, S. 1448.

954 Petkis, S. 1449.

955 Petkis, S. 1449.

teidigung überzeugend begründen (und beweisen) kann, wenn das in jenem Zeitpunkt noch nicht eingetroffene Gesamtbild unklar ist. Für eine allfällige Bejahung antizipatorischer Selbstverteidigung müssten unmittelbar eintreffende physische Effekte konkret und mit Sicherheit voraussehbar sein, was, wie erläutert, zeitnah sehr schwierig ist.

Die Fragen nach dem Beginn eines Cyberangriffs sowie der Absehbarkeit unmittelbarer Schäden stellen sich auch im Hinblick auf die sog. Ereigniskumulationstheorie (im Englischen: »*accumulation of events theory*«) und bei einer Weiterverbreitung von Schadsoftware. Denn auch bei jenen Szenarien geht es im Grunde um die Gefahr einer *bevorstehenden* Schädigung. Bejaht man die Notwendigkeit von Selbstverteidigungshandlungen im Vorfeld konkreter Schäden, würde man sich auch bei der Problematik von Weiterverbreitungen theoretisch im Feld antizipatorischer Verteidigung bewegen. Aufgrund ihrer Umstrittenheit ist es nicht nur rechtlich, sondern durch die dazukommende schwierige Voraussehbarkeit von Effekten bei Cyberangriffen auch faktisch extrem schwierig, die Notwendigkeit einer antizipatorischen Selbstverteidigung überzeugend zu begründen. Die schwierige Vorhersehbarkeit kausaler Schäden bei Cyberangriffen erschwert die Debatte um (antizipatorische) Selbstverteidigungshandlungen daher wesentlich.

Vor dem Hintergrund des Notwendigkeitserfordernisses sollte eine dahingehende Argumentation, auf Cyberangriffe ohne konkrete physische Schädigungen zurückschlagen zu können – wenn überhaupt – mit äusserster Zurückhaltung in Betracht gezogen werden. Die Notwendigkeit kann im Rahmen von Art. 51 UN-Charta – wenn überhaupt – *nur* bei einer jeden Moment eintretenden Zerstörung mit Verletzten oder Toten und keiner alternativen Handlungsmöglichkeit (»*leaving no choice of alternative means*«) bejaht werden.[956] Im Cyberbereich wird eine solche Gewissheit kausaler und schwerwiegender physischer Schäden im Voraus wohl selten der Fall sein. Durch eine dahingende Argumentation, dass völkerrechtliche Selbstverteidungsmassnahmen gegen (Cyber-)angriffe notwendig sein müssen, bevor konkrete Schädigungen eingetroffen sind, könnte die strittige Doktrin umgangen werden, ob Selbst-

[956] JENNINGS, S. 82.

verteidigung extensiv (antizipatorisch) oder restriktiv verstanden werden muss. Es könnte argumentiert werden, dass eine gewaltsame Verteidigung notwendig und deshalb gerechtfertigt war.[957]

Gemäss der vorliegend vertretenen Auffassung sollte man sich strikt am Anwendungsbereich der herkömmlichen Selbstverteidigung orientieren – gerade angesichts der schwierigen Abschätzbarkeit von durch Cyberangriffe ausgelösten Schäden sowie angesichts der vehement umstrittenen Zulässigkeit antizipatorischer Selbstverteidigung. Vor dem Hintergrund herkömmlicher Selbstverteidigung befindet man sich grundsätzlich also regelmässig ausserhalb des Anwendungsbereichs von Art. 51 UN-Charta, solange keine physischen Schäden eingetroffen sind und keine Menschenleben unmittelbar auf dem Spiel stehen. Da man sich in solchen Konstellationen somit ausserhalb des Anwendungsbereichs von Art. 51 UN-Charta befindet, wäre juristisch gesehen folglich eine Selbstverteidigungshandlung auch nicht notwendig. Demzufolge befindet man sich beim grossen Teil der Cyberangriffe bis zum Eintreffen physischer Schäden ausserhalb einer gerechtfertigten Selbstverteidigung. Diese Restriktivität wird vorliegend bewusst vertreten, zumal die rechtliche Beschränkung nur den Bereich aktiver, offensiver Verteidigungsmassnahmen betrifft und daher passive Massnahmen zulässt, die gegebenenfalls frühentdeckte Schadprogramme auf dem eigenen Computersystem neutralisieren und/oder Schäden minimieren können.

ii. Nach Beendigung eines (Cyber-)Angriffs: Abänderung der Selbstverteidigung zur Vergeltung

Neben der Definierung einer unmittelbaren, konkreten Cybergefahr stellt sich auch die Frage, wann ein Cyberangriff beendet ist. Ist ein Angriff beendet, erweist sich eine Selbstverteidigungshandlung als nicht mehr notwendig. Wie unter III.A.3.b. ausgeführt, werden trojanische Pferde, Viren und Würmer i.d.R. erst *nach Eintritt* einer für die Selbstverteidigung relevanten Schädigung entdeckt. Zudem ist es oft sehr schwer, innerhalb eines absehbaren Zeitrahmens zuverlässig davon ausgehen zu können, dass eine Schädigung durch einen Cyberangriff ausgelöst wurde und es sich um keinen Systemfehler handelt.[958] Hinzu kommt, dass es auch im Falle kinetischer Schäden extrem schwierig sein

957 Vgl. GRAY, Use of Force, S. 163 f., die im herkömmlichen Kontext darauf verweist, dass die dogmatische Unterscheidung des bewaffneten Angriffs und der Verhältnismässigkeit in der Staatenpraxis oft verschwimmt, indem die Notwendigkeit oft als einziger Faktor zur Beurteilung der Legitimität einer Massnahme herangezogen wird.

958 LAHMANN, S. 272 f. (u.a.).

kann, *post hoc* zu eruieren, welche Informationen oder Softwaremanipulationen für welchen Schaden ursächlich und kausal waren bzw. inwiefern mittelbare Schäden überhaupt von einem konkreten Schadprogramm ausgingen.[959] Zum Zeitpunkt der Entdeckung eines Schadprogrammes könnte sich dieses bereits auf verschiedene Weise reproduziert und weiterverbreitet sowie bereits ein unbekanntes Volumen an Daten kopiert haben.[960]

Dennoch wird teilweise argumentiert, dass Staaten ein Recht auf Hackbacks oder auf den Einsatz anderweitiger offensiver Cyberselbstverteidigungsmassnahmen haben sollen, obschon der ursprüngliche Angriff beendet sei.[961] Eine dahingehende Argumentation würde streng gesehen allerdings dem Verhältnismässigkeitserfordernis der Selbstverteidigung nicht standhalten.[962] Denn zum Zeitpunkt, in dem ersichtliche kinetische Effekte eintreffen, ist der für eine Selbstverteidigung relevante Cyberangriff i.d.R. beendet, da die Schädigung bereits eingetroffen ist.[963] Jener (sowie der vorliegenden) Ansicht nach wäre damit das Zeitfenster verhältnismässiger Selbstverteidigungshandlungen geschlossen.[964] Ist die Schädigung beendet, ist eine auf den beendeten Angriff gerichtete Selbstverteidigungshandlung zur Abwehr nicht mehr notwendig. Würde man auf solche Angriffe mit militärischen Selbstverteidigungshandlungen reagieren, würde man sich nicht verteidigen, sondern vielmehr neue Schädigungen *ex post* auslösen[965] und dadurch neue Angriffe lancieren. Hinzu kommt, dass die technische Zurückverfolgung des Urhebers sowohl bei DDoS-Angriffen als auch bei trojanischen Pferden, Viren und Würmern jeweils eine gewisse Zeit beansprucht. Daher bleiben der wahre Angreifer und/oder der allenfalls rechtlich verantwortliche Staat oft (lange) unbekannt.[966] Digitale und nicht-digitale Verteidigungsmassnahmen gegen den Angreiferstaat würden damit zeitlich ohnehin erst *nach* der Notwendigkeit seiner Abwehr möglich. Das in der Praxis somit überwiegende zeitliche Zurückliegen eines Angriffs spricht daher gegen einen Einsatz von Selbstverteidigungsmassnahmen auf (beendete) Cyberangriffe. Eine Reaktion auf beendete Angriffe würde der (zu-

959 Vgl. Petkis, S. 1448.

960 Vgl. Newton/May, S. 271.

961 Halberstam, S. 204; Petkis, S. 1454.

962 Petkis, S. 1454.

963 Petkis, S. 1448.

964 Petkis, S. 1455 m.V.a. das Bsp. des Cyberangriffs auf Sony Pictures im Dezember 2014.

965 Diggelmann/Hadorn, S. 265.

966 Diggelmann/Hadorn, S. 265. Banks sieht die rechtzeitige Urheberzurechnung von Cyberangriffen als eine der grössten Herausforderungen für deren Regulierung: Banks, S. 165.

mindest hauptsächlich in Europa vertretenen[967]) Grundidee der Selbstverteidigung zuwiderlaufen, wonach diese nur unter restriktiven zeitlichen Schranken *während* eines Angriffs zulässig ist. Es gibt keinen ersichtlichen Grund, weshalb man im Cyberkontext länger zurückschlagen können sollte als im herkömmlichen Kontext[968] – insb., da man dadurch den Charakter der Selbstverteidigung von einem Abwehr- zu einem Vergeltungsrecht abändern würde.[969] Vergeltung ist *per definitionem* nicht notwendig für die Abwehr oder Beendigung eines Angriffs. Die Grundhaltung, Reaktionen auf abgeschlossene Schädigungen zu erlauben, wäre vielmehr – und dies ist nachfolgend relevant – der »Kompensationslogik« des Gegenmassnahmenrechts verpflichtet.[970] Gewaltsame Selbsthilfe ist nur zur Beendigung eines Angriffs erlaubt, nicht zur kompensatorischen gewaltsamen Schädigung.[971]

Schwieriger zu definieren wäre das Ende eines Cyberangriffs in jenen Fällen, in denen Schädigungen durch Fehlprogrammierungen oder Blockierungen (z.B. durch DDoS-Angriffe) *anhalten* bzw. wenn sich Schadprogramme entsprechend (automatisiert) weiterverbreiten. Indem bei DDoS-Angriffen – anders als bei Würmern oder Viren – der Schadenseintritt mit dem Angriff meist zusammenfällt, ist fraglich, ob man DDoS-Angriffe im Moment der Schädigung als bereits beendet betrachten sollte. Solange physische Destruktionen und (Personen-)Schäden durch Systembeeinträchtigungen nicht anhalten, bewegt man sich streng gesehen ausserhalb des Anwendungsbereichs von Art. 51 UN-Charta. Eine Notwendigkeit eines Gegenangriffes auf DDoS-Angriffe oder bei einer Weiterverbreitung von Schadprogrammen könnte man folglich nur in jenen Konstellationen sehen, in denen eine Blockierung oder Manipulation anhält (siehe nachfolgend). Auch in jenen Konstellationen spricht letztlich dennoch die erforderliche Zeit für eine technische Zurückverfolgung gegen die Beantwortung zurückliegender DDoS-Angriffe durch Selbstverteidigungshandlungen.

---

967 Zu den unterschiedlichen Verständnissen des Selbstverteidigungsrecht siehe vorangehend unter: III.B.1.b.

968 Petkis, S. 1456.

969 Diggelmann/Hadorn, S. 264. Bei einigen US-amerikanischen Autoren ist eine Tendenz zu erkennen, die Selbstverteidigung als Bestrafung (und Abschreckung) zu sehen: siehe z.B. Jensen, Critical National Infrastructure, S. 239: »*An active component to CND must be available to deter and punish an intruder*«.

970 Diggelmann/Hadorn, S. 265; O'Connell, Cyber Security, S. 205. Ausführlicher zum Gegenmassnahmenrecht siehe nachfolgend unter IV.B.

971 Diggelmann/Hadorn, S. 264.

Insgesamt bleibt es schwierig, mit Sicherheit die für Art. 51 UN-Charta relevanten Kausalzusammenhänge sowie den Beginn und das Ende von Cyberangriffen festzulegen. Der hier vertretenen Ansicht nach sollte sowohl der Beginn als auch das Ende eines für die Selbstverteidigung gem. Art. 51 UN-Charta relevanten Cyberangriffs folglich an den jeweils eingetroffenen, anhaltenden physischen Auswirkung gemessen werden. Und dies, auch wenn im System befindliche Schadprogramme (oder der Ursprungscomputer) bereits zuvor oder danach entdeckt werden oder sich weiterverbreiten. Im Ergebnis sprechen sowohl die vielen Unklarheiten bei Cyberangriffen und deren schwer absehbaren Schädigungen als auch die dogmatischen Debatten zum frühestmöglichen und spätestzulässigen Zeitpunkt der Selbstverteidigung dafür, die Notwendigkeit eng zu fassen.

iii. Während eines Cyberangriffs: Geeignetheit und mildestes Mittel

Die Gegenwärtigkeit eines für Art. 51 UN-Charta relevanten Cyberangriffs kann, wie bereits erwähnt, höchstens bei DDoS-Angriffen oder bei durch Schadprogramme ausgelösten Softwaremanipulationen, die anhaltend physische Zerstörungen und/oder Tote nach sich ziehen, festgestellt werden. Dies wäre bspw. denkbar, wenn durch DDoS-Angriffe kritische Infrastrukturen blockiert oder deren Kontrollsysteme manipuliert würden, was mittelbar zu anhaltenden physischen Zerstörungen führen könnte: z.B. bei einer anhaltenden Blockierung von Fluginformationen, die zu Kollisionen von Flugzeugen führt oder bei Blockierungen von Spitälern, die Tote fordern.

Bejaht man die Gegenwärtigkeit eines Cyberangriffs gem. Art. 51 UN-Charta, muss die entsprechende Selbstverteidigungshandlung des Weiteren das auf die Abwehr gerichtete, mildeste Mittel sein,[972] um den rechtlichen Erfordernissen der Notwendigkeit zu entsprechen.

Das Tallinn Manual 2.0 und die Lehre haben die Tendenz, digitale Verteidigungsmassnahmen als mildestes Mittel zu verstehen. Aktive und passive Cybergegenmassnahmen werden oft zusammengefasst, indem Letztere ausgeschöpft werden müssen, bevor kinetische oder aktive Cyberhandlungen eingesetzt werden dürfen.[973] Ein Teil der Lehre ist der Ansicht, dass nicht nur passive, sondern auch aktive Cyberverteidigungshandlungen wie Hackbacks kinetischen Angriffen vorgehen sollen, wenn sie »ausreichen«, um die Gefahr

[972] Petkis, S. 1454.

[973] Tallinn Manual 2.0, S. 349 R72 C3. Ähnlich: Petkis, S. 1440.

abzuwenden.[974] In jenen Fällen sei die Anwendung kinetischer Gewalt nicht gerechtfertigt.[975] Demzufolge werden Hackbacks im Vergleich zu traditioneller Gewalt oft als ein milderes Mittel gesehen.[976] Obschon man durch das Verhältnismässigkeitsprinzip nicht dazu angehalten sei, friedlich (»*in-kind*«) zu reagieren, sei es schwieriger, eine kinetische Massnahme zu rechtfertigen.[977] Insgesamt liegt daher in der Lehre ein Fokus auf der Frage der Legitimität *kinetischer* Selbstverteidigung, da sie grundsätzlich vergleichsweise schnell zur Eskalation führen könne.[978] Ohne dass vorliegend kinetische Reaktionen und die von ihnen ausgehenden Problematiken verharmlost werden sollen, drängt sich allerdings auch zunehmend die Frage nach der Verhältnismässigkeit *digitaler* Verteidigungsmassnahmen auf. Insbesondere, da wie unter II.B.2. angeführt, bereits einige Staaten digitale Gegenangriffe als Reaktionsmöglichkeiten auf Cyberangriffe betrachten.[979]

Um sowohl kinetische als auch digitale Verteidigungsmassnahmen lancieren zu können, muss man vorab wissen, gegen wen oder gegen welchen Computer diese zu erfolgen haben. Auf welches Ziel darf man abzielen, um einen durch Cyberangriffe ausgelösten »bewaffneten« Angriff in geeigneter Weise sowie als mildestes Mittel gem. Art. 51 UN-Charta abzuwehren? Indem Urheberhinweise in Schadprogrammen regelmässig gefälscht oder die IP-Adressen Dritter benutzt werden können, um auf falsche Fährten zu führen, ist es, wie bereits erwähnt, sehr schwer, zeitnah den »wahren« Urheber hinter einem Angriff zu eruieren.[980] Dieser Einbezug (allenfalls gezielter) Infrastrukturen Dritter kann dabei sogar an sich als politische Strategie eingesetzt werden.[981] Auch wenn man es also schafft, das Computersystem zu eruieren, von dem die betreffenden Angriffe ausgehen (bei DDoS-Angriffen müsste dies das Kontrollsystem sein, von dem die Befehle an alle Computer ausgehen), besteht das reale Risiko, dass man auf den »falschen Angreifer« zurückschlägt und, dass man über die Natur des Akteurs (staatlich, nichtstaatlich oder ein falscher

974 Lahmann, S. 64.

975 Stein/Marauhn, S. 9.

976 Siehe u.a. Condron, S. 410; Halberstam, S. 204, die offensive Cybergegenangriffe als »*in-kind response*« umschreiben. Ähnlich: Jensen, Critical National Infrastructure, S. 231; Sklerov, S. 25. Ferner: Rid, Cyberwar and Peace, S. 77 ff.

977 Petkis, S. 1440.

978 Siehe u.a. Libicki, S. 110; Jensen, Critical National Infrastructure, S. 230.

979 Vgl. Halberstam, S. 204 f. Eingehender zu nationalen Cyberstrategien und -Ansichten als auch zum zunehmenden Aufbau digitaler Cyber-Kapazitäten: Kerschischnig, S. 90 ff.

980 Harrison Dinniss, S. 105.

981 Harrison Dinniss, S. 105.

Staat) hinweggetäuscht wird. Erlaubt man ein kinetisches oder digitales Zurückschlagen auf Computersysteme (oder auf den betreffenden Staat, in dem sich diese Computersysteme befinden), von denen ein Angriff ausgeht, muss man folglich damit rechnen, nicht mit Sicherheit den eigentlichen Urheber (physisch) zu schädigen, sondern möglicherweise einen grundsätzlich unbeteiligten Dritten.[982]

Bei digitalen (Gegen-)Angriffen besonders ist, dass – anders als bei kinetischen Waffen – Folgeschäden schwer absehbar sind. Daher würde man regelmässig (eventualvorsätzlich) in Kauf nehmen, bei Dritten verschiedene Arten von physischen und nicht-physischen Schäden auszulösen. Obschon ein sofortiger digitaler Gegenschlag (unter Umständen auch gegen ein kompromittiertes Computersystem) geeignet sein könnte, einen anhaltenden Angriff zu neutralisieren, bleibt es fraglich, ob eine *militärische* Massnahme das jeweils mildeste Mittel ist. Führt ein militärischer Gegenschlag beim betreffenden System zu Schäden, würde man nämlich dadurch gegebenenfalls einen anderen Staat in seinen inneren Angelegenheiten (gewaltsam) verletzen. Auch wenn das Zurückschlagen auf kompromittierte Computer unter Umständen dem Zweck der Abwehr dienen könnte, muss man nicht nur aus rechtlicher, sondern auch aus staatlich-strategischer Sicht im Hinterkopf behalten, dass gewaltsame, militärische Massnahmen immer auch eine international-politische Komponente mit sich bringen. Hinzu kommt, dass sich die zur Verteidigung eingesetzten Schadprogramme wiederum auf weitere Systeme weiterverbreiten, dadurch noch mehr Unbeteiligte treffen und zu weiteren Kollateralschäden und (völker-)rechtlichen Verletzungen führen können.[983] Gemäss der hier vertretenen Auffassung sollte aus völkerrechtlicher Sicht die Inkaufnahme von möglicherweise kontraproduktiven Kollateralschäden in einem unbeteiligten Drittstaat nur als *ultima ratio* in Betracht gezogen werden dürfen, wenn keine alternativen milderen Mittel zur Verfügung stehen.[984] Dies gerade in Anbetracht dessen, dass digitale Gegenschläge oftmals Schüsse in das unüber-

[982] Eine eingehendere Betrachtung kinetischer Reaktionen soll Gegenstand anderweitiger Auseinandersetzungen sein, da diese den vorliegenden Rahmen sprengen würde. An dieser Stelle soll lediglich auf die erwähnte Problematik einer (zeitnahen) adäquaten, technischen und rechtlichen Zurechnung eines Cyberangriffs an einen Staat hingewiesen werden.

[983] Vgl. Ashford, ComputerWeekly vom 15.11.2013. Dazu ausführlicher nachfolgend unter den Ausführungen zur Verhältnismässigkeit i.e.S.

[984] Diese Folgerung lehnt sich an das Ölplattformen-Urteil des IGH an, in welchem das Abzielen militärischer Verteidigungsmassnahmen auf irrelevante Objekte als nicht notwendig erachtet wurde. Siehe dazu vorangehend unter IV.A.1.

sichtliche, weltweite Netz sind, während sie zugleich wenig Garantie einer effektiven Abwehr bieten.[985] Angesichts potenzieller politischer Implikationen durch (anonyme) Gegenschläge wäre es in solchen Konstellationen wohl jeweils milder, den betreffenden Staat, von dessen Computern die schädigenden Angriffe ausgehen, in einem ersten Schritt darüber zu informieren und dadurch sein eigenes Tätigwerden anzuordnen. Sollte dazu die Zeit fehlen oder sollte der informierte Staat nichts unternehmen, bestünde immer noch die passive Möglichkeit, eigene Computersysteme auszuschalten und relevante Funktionen auf Parallelsysteme zu leiten oder Schadprogramme auf dem eigenen System zu neutralisieren, bevor sich offensive Gegenschläge aufdrängen. Um diese Abwägungen im Einzelfall zu beurteilen, muss man letzlich allerdings abwägen, welche Schäden ein Ausschalten eines Systems (wie bspw. ein grossflächiges Ausschalten des Internets oder das Blockieren vieler IP-Adressen) wiederum zur Folge hätte und ob Parallelsysteme verfügbar sind. Im kinetischen Kontext ist es ähnlich fraglich, auf welches Ziel man unter Einhaltung des Erfordernisses des mildesten Mittels eine Selbstverteidigung richten würde, ohne unter Umständen »den Falschen« zu treffen. Dies betrifft mitunter auch die Frage, welches Mass an Gewissheit über den Urheber sowie (im digitalen und kinetischen Kontext) über potenzielle (physische) Folgeschäden an fremdstaatlichen Computerinfrastrukturen erforderlich ist.[986] Somit ist sowohl beim Einsatz kinetischer als auch digitaler militärischer Gewalt Zurückhaltung geboten. Fraglich ist daher insgesamt, ob aktive Verteidigung angesichts regelmässig verfügbarer, passiver Alternativen das mildeste Mittel ist. Zu grundsätzlich tauglichen milderen Mittel zählen nämlich auch die Möglichkeit diplomatischer Verhandlungen, der Retorsion und nicht-militärischer Gegenmassnahmen.[987] Daher werden wohl regelmässig gewaltlose und/oder passive digitale Mittel auf dem eigenen Computersystem abseits von offensiven Verteidigungsmassnahmen zur Verfügung stehen.

985 Dewar, Active Cyber Defense, S. 7 f.

986 Das Mass der Zurechnungsstandards, der entsprechenden Sorgfalts- und Beweiserbringungspflicht ist relativ unklar: Roguski, S. 14 f.

987 Banks/Criddle, S. 74.

Letztlich bleibt fraglich, ob sich digitale Gegenschläge grundsätzlich überhaupt eignen, um einen Angriff zu beenden und abzuwehren.[988] Indem die vorliegenden Ausführungen Kategorien offensiver Verteidigungsmittel betreffen, fallen, wie bereits an mehreren Stellen angeführt, digitale Massnahmen darunter, die das eigene System verlassen und (neben der technischen Zurückverfolgung) dazu auch programmiert werden müssen. Dies benötigt regelmässig viel Zeit.[989] Vor diesem Hintergrund ist es sehr schwierig zu argumentieren, dass ein digitaler Gegenschlag zur Abwehr geeignet ist, *post facto* einen bereits zurückliegenden Angriff abzuwehren.

Die gegenwärtige Tendenz, dass Staaten vermehrt auf aktive Cyberselbstverteidigung setzen wollen, ist der vorliegenden Ansicht nach ernst zu nehmen. Insbesondere dürfen Sinn und Zweck einer Selbstverteidigung im Rahmen von Art. 51 UN-Charta, auf die Abwehr und die Beendigung eines Angriffs abzuzielen, nicht verkannt werden.[990] Sowohl militärische digitale als auch nicht-digitale Selbstverteidigungshandlungen erscheinen im Ergebnis nur gerechtfertigt, wenn man damit die zur Selbstverteidigung legitimierenden physischen Schädigungen in geeigneter Weise beenden kann und diese Massnahmen im jeweiligen Fall erforderlich, mitunter also die mildesten zur Verfügung stehenden Mittel sind. Schliesslich wird man um eine Einzelfallbetrachtung nicht herumkommen, mittels derer die spezifischen Fakten der jeweiligen Vorfälle und insb. *auch der nicht-digitale Gesamtkontext* gewürdigt werden müssen.[991]

[988] Es gibt verschiedene Ansichten zur Geeignetheit von Hackbacks zur Abwehr: Harrison Dinniss; Jensen, Cyber Deterrence, S. 800 sprechen sich eher dafür aus, dass digitale Gegenmassnahmen, vereinfacht gesagt, am »effektivsten« seien. Ähnlich: Stein/Marauhn, S. 9. Petkis ist aufgrund der zeitlichen Komponente eher dagegen. Allerdings führt Petkis mit der Operation Buckshot Yankee (2008) ein Beispiel eines auf die Neutralisierung ausgerichteten und demnach verhältnismässigen digitalen Gegenschlags an: Petkis, S. 1456 mit den entsprechenden Verweisen. Ferner zur Neutralisierung von Angriffen durch aktive Cyberverteidigung: Kesan/Hayes, S. 474 f. m.w.V.

[989] Mäder/Sansano, Interview mit Süssli und Vuitel, NZZ vom 06.01.2021.

[990] Siehe ausführlicher dazu vorangehend unter IV.A.1.a.

[991] Lahmann, S. 64; Randelzhofer/Nolte, S. 1420, insb. §46.

c. Verhältnismässigkeit (i.e.S.): Zweck-Mittel-Relation und Intensität

Erwiese sich eine Selbstverteidigungsmassnahme auf einen bejahten bewaffneten Angriff gem. Art. 51-UN-Charta in Übereinstimmung mit den vorangehenden Voraussetzungen als notwendig, muss man prüfen, ob diese insgesamt verhältnismässig ist. Gemeint ist das im Cyberkontext überwiegend vertretene Erfordernis der Angemessenheit einer Massnahme zum Ziel der Abwehr[992] sowie die äusserste Schranke keiner »klar disproportionalen« Schädigung. Vor dem Hintergrund einer angemessenen Zweck-Mittel-Relation spielt auch die Frage mit, ob der Einsatz gewaltsamer Massnahmen *überhaupt* zielführend ist.[993] Damit gemeint ist, ob gewaltsame Massnahmen nicht nur ungeeignet für die Abwehr, sondern sogar kontraproduktiv sein können.[994] Dabei spielen insb. unbeabsichtigte Effekte militärischer Einsätze eine Rolle, die nicht nur politisch, sondern auch rechtlich relevant werden können.[995] Da es sich bei der Verhältnismässigkeit i.e.S. jeweils um Abwägungen der involvierten Interessen und Umstände handelt, sollen im Folgenden für den Cyberkontext einige Beispiele Erwähnung finden. Diese sollen die mit einer solchen Interessenabwägung verbundenen Schwierigkeiten in Bezug auf Cyberangriffe illustrieren.

i. Baku–Tiflis–Ceyhan Pipeline

Am 5. August 2008 haben Dokumentationen zufolge Cyberangriffe zur Explosion der Baku–Tiflis–Ceyhan Pipeline in der Nähe der Stadt Refahiye in Anatolien geführt.[996] Ein Schadprogramm konnte via Sicherheitslücken in der Kommunikationssystemssoftware der Überwachungskameras in das Kontrollsystem der Pipeline eindringen und dieses manipulieren.[997] Diese Manipulation führte zu einem Überdruck beim durch die Leitung fliessenden Rohöl,

---

992 Wicker, S. 40 ff. m.w.H. Ähnlich i.Z.m. aktiver Cyber-Verteidigung: Denning, Active Cyber Defense, S. 111.

993 Dazu vor dem Hintergrund herkömmlicher militärischer Massnahmen und anhand konkreter Beispiele: Gray, Limits of Force, S. 109.

994 Gray, Limits of Force, S. 109 und S. 112 m.V.a. die »Balance of Consequences« in: UN Doc. A/59/565 (2004), S. 58 §207(e).

995 Zu konkreten militärischen Einsätzen, die zu rechtlich relevanten, unbeabsichtigten Konsequenzen geführt haben: Gray, Limits of Force, S. 109 ff. Mitunter erwähnt Gray die US-amerikanische Invasion des Iraks 2003 oder die humanitäre Operation im Kosovo 1999, die neben Kurzzeit- auch Langzeitfolgen und »Nebeneffekte« nach sich zogen.

996 Corner, World Pipelines vom 12.12.2014; o.V., Homeland Security News Wire vom 17.12.2014.

997 Robertson/Riley, Bloomberg News vom 10.12.2014.

was in der Folge die Explosion auslöste.[998] Dies zog nicht nur ein schwer unter Kontrolle zu bringendes Feuer nach sich,[999] sondern es wurden auch 30'000 Barrel Öl in unmittelbarer Nähe eines Grundwasserleiters verschüttet, was zu beträchtlichen Umweltschäden in Anatolien führte.[1000] Die Angriffe fanden im selben Monat (August 2008) wie diejenigen auf Georgien statt, was jedoch erst Ende 2014 herausgefunden wurde.[1001] Davor ging man von technischen Fehlern aus.[1002] Es wird ein Zusammenhang mit dem russisch-georgischen Konflikt vermutet.[1003]

Der Vorfall ist nicht nur in Bezug auf die Intensität der durch die Manipulation einer kritischen Infrastruktur ausgelösten *physischen* Effekte erwähnenswert. Der springende Punkt für die hiesige Debatte ist, dass die Türkei ein wohl *unbeabsichtigtes* Ziel dieses Cyberangriffs wurde.[1004] Es handelte sich mit überwiegender Wahrscheinlichkeit um einen Nebeneffekt einer Cyberoperation, die im Grunde auf ein anderes Ziel ausgerichtet war. Wie unter III.A.3.b. beschrieben, können sich Schadprogramme u.U. nämlich unkontrolliert über ein Zielsystem weiterverbreiten. Somit wurde ein grundsätzlich unbeteiligter Drittstaat in unbeabsichtigter Weise von den Effekten eines mit einem kinetischen Angriff vergleichbaren Cyberangriffs getroffen. Dies zeigt, dass durch das Element der Unkontrolliertheit der Radius an Zielen (auch für physische Schäden) zunimmt. Vor dem Argument der Verhältnismässigkeit würde eine pauschale Beschädigung von unbeteiligten Drittstaaten, die nicht auf eine Abwehr gerichtet ist, schwer standhalten: Es ist (wie vorangehend aufgezeigt) fraglich, ob es notwendig und i.e.S. verhältnismässig ist, einen Drittstaat anzugreifen, um einen Angriff eines anderen Staates abzuwehren. Führt ein digita-

998 Lahmann, S. 7.

999 Robertson/Riley, Bloomberg News vom 10.12.2014.

1000 Lahmann, S. 65.

1001 Lahmann, S. 7.

1002 O.V., Homeland Security News Wire vom 17.12.2014.

1003 Robertson/Riley, Bloomberg News vom 10.12.2014.

1004 Lahmann, S. 65. Lahmann kategorisiert diesen Angriff auf ebendieser Seite als schwerwiegender als Stuxnet und argumentiert, dass er die Schwelle eines bewaffneten Angriffs gem. Art. 51 UN-Charta erreichen könnte. Allerdings sei das Element der für eine Selbstverteidung erforderlichen *Absicht* eines bewaffneten Angriffs fraglich.

ler Gegenschlag schliesslich zu physischen Schäden, kommt er einem kinetischen Abzielen auf ungerechtfertigte Objekte sehr nahe und würde unter die der Idee nach zu vermeidenden Kollateralschäden fallen.[1005]

ii. »Eternal Blue«, »WannaCry« und »NotPetya«

Im Frühling 2017 kam beim sog. »Shadow Brokers«-Vorfall ans Licht, dass über einen Zeitraum von acht Monaten etwa ein Gigabyte an hochgefährlichen Daten der Nationalen Sicherheitsbehörde der USA (im Englischen: National Security Agency. Fortan: NSA) kopiert worden waren.[1006] Darunter war auch »Eternal Blue«, ein auf eine sog. Zero-Day-Sicherheitslücke abzielendes Schadprogramm.[1007] Zero-Day-Lücken sind, wie bereits unter II.B.1.a. erwähnt, den Herstellern unbekannte Sicherheitslücken in spezifischen Softwareprotokollen. Dadurch können Schadprogramme (u.a. via Internet) grundsätzlich in jeden von dieser Lücke betroffenen Computer eingeschleust werden, bevor weder die Hersteller noch die Nutzer des betreffenden Computersystems die Zeit haben, diese Lücke zu schliessen.[1008] Dies dehnt das von diesen unbekannten Lücken ausgehende Schädigungspotenzial zusätzlich aus, da diese nicht geschützt werden können, während Angreifer einen Vorsprung für deren Ausnutzung haben. Das Schadprogramm Eternal Blue zielte auf eine Zero-Day-Sicherheitslücke in einem Microsoftprogramm (das Vorgängerprogramm von Microsoft 8) ab. Dieses Schadprogramm mit den darin enthaltenen Informationen zur betreffenden Sicherheitslücke führte in der Folge zu hohen Schäden (vorerst in Baltimore und weiteren US-Gebieten).[1009] Da im Zeitpunkt der Freilassung des Schadprogramms Microsoft noch nichts von der Sicherheitslücke wusste, konnten die Entwickler diese nicht schliessen. Nachdem das Programm also in Umlauf gebracht wurde, konnte es sich rasant verbreiten. Gravierend in jenem Fall war, dass – indem Microsoft *weltweit* verwendet wird – unzählige weitere Computer genau diese Sicherheitslücke aufwiesen. Letztlich – und dies ist für die hiesige Veranschaulichung wichtig – konnten sich

1005 An dieser Stelle soll an das IGH, Ölplattformen-Urteil, §76 erinnert werden, wonach das Abzielen auf gewisse Plattformen, die nicht der Abwehr dienten, als nicht verhältnismässig (i.w.S.) angesehen wurde.

1006 Brewster, Forbes vom 12.05.2017; Gallagher, Ars Technica vom 28.05.2019; Goodin, Ars Technica vom 14.04.2017.

1007 Lahmann, S. 11. Dazu auch: Clarke/Knake, Fifth Domain, S. 17 ff.

1008 Greenberg, Wired vom 22.08.2018. Eingehender dazu: Greenberg, Sandworm, S. 1 ff.; S. 163 ff.

1009 Dazu: Gallagher, Ars Technica vom 28.05.2019; Greenberg, Sandworm, S. 163 ff.; Lahmann, S. 280, S. 13; Perlroth/Shane, New York Times vom 25.05.2019.

auch weitere Schadprogramme dank dieser nicht offengelegten Sicherheitslücke exponenziell weiterverbreiten. Darunter waren auch die später unter dem Namen »WannaCry« und »NotPetya« bekannt gewordenen Cyberangriffe.[1010] Diese Angriffe stellten eine Serie von ökonomisch verheerenden Cyberangriffen im Jahr 2017 dar, die weltweit zu hoch bezifferten Schäden führten.[1011]

Um das Ausmass zu veranschaulichen: Durch das sich im Mai 2017[1012] verbreitende Schadprogramm WannaCry wurden innert kürzester Zeit etwa 230'000 Computer in mehr als 150 Ländern infiziert.[1013] Die Cyberangriffe führten zu Schäden in Milliardenhöhe und brachten durch das Blockieren von IT-Systemen mehrerer Spitäler weltweit Menschenleben in Gefahr.[1014] Im Dezember jenes Jahres haben die USA und weitere Staaten öffentlich Nord-Korea als für den Angriff verantwortlich erklärt.[1015] NotPetya verbreitete sich grundsätzlich ebenfalls global.[1016] NotPetya wurde zeitweise als »der verheehrendste Cyberangriff der Geschichte« bezeichnet, da durch die automatisierte und willkürliche Verbreitung des Schadprogrammes Schäden in der Höhe von über 10 Milliarden USD entstanden.[1017] Für die vorliegende Thematik interessant ist, dass die massiven Folgen nicht zwingend durch die Programmierer beabsichtigt oder voraussehbar gewesen waren und wohl wesentlich über das Ziel hinausgingen – oder in den Worten Greenbergs: »*The release of NotPetya was likely more explosive than even its creators intended.*«[1018] Zudem schlug NotPetya so schlagartig ein, dass keine Zeit zur Abwehr bestand. Oder in den Worten von Craig Williams, dem Direktor einer der ersten Sicherheitsfirmen, die jenen Vorfall analysierten: »*By the second you saw it [das Schadprogramm NotPetya], your data center was already gone.*«[1019] Um das durch NotPetya ausgelöste Ausmass zu illustrieren: In Kiev alleine waren mindestens vier Spitäler,

1010 Lahmann, S. 11. Näher zum zusätzlichen Radius von NotPetya aufgrund des Zusammenwirkens von Eternal Blue mit einem weiteren Schadprogramm (Mimikatz): Greenberg, Wired vom 22.08.2018; Greenberg, Sandworm, S. 163 ff.

1011 Lahmann, S. 11.

1012 Greenberg, Wired vom 22.08.2018.

1013 Lahmann, S. 12. Betschon, NZZ vom 15.05.2017.

1014 Bossert, The Wall Street Journal vom 18.12.2017.

1015 Bossert, The Wall Street Journal vom 18.12.2017; Nakashima/Rucker, Washington Post vom 19.12.2017; Bing/Lynch, Reuters vom 06.09.2018.

1016 Geschätzte 80% der infizierten staatlichen und privaten Computer befanden sich in der Ukraine: Wakefield, BBC News vom 28.06.2017.

1017 Greenberg, Wired vom 22.08.2018.

1018 Greenberg, Wired vom 22.08.2018.

1019 Greenberg, Wired vom 22.08.2018.

sechs Energieversorgungsunternehmen, zwei Flughäfen und mehr als 300 Unternehmen betroffen, davon über 22 Banken, Bankautomaten und Kartenzahlungssysteme in Verkaufsläden und Transportunternehmen sowie praktisch jede Behörde.[1020] Der Angriff hat zudem durch Wissenschaftler der Chernobyl-Wiederaufbereitungsanlage genutzte Computer lahmgelegt.[1021] Innerhalb von Stunden infizierte das Schadprogramm unzählige Computer weltweit, die von Spitälern in Pennsylvania bis hin zu Schokoladenfabriken in Tasmanien reichten.[1022] Darunter waren einflussreiche transnationale Unternehmen wie die Container-Reederei Maersk Line (A.P. Møller-Maersk), das Pharmaunternehmen Merck, FedEx und der Lebensmittelkonzern Mondelēz betroffen.[1023] Eindrücklich ist der Fall Maersk: Durch den Angriff wurde der Umschlag von etwa 3 Millionen Containern über mehrere Wochen beeinträchtigt, womit wichtige globale Lieferketten von Rohstoffen und fertigen Produkten unterbrochen wurden.[1024] Das Riesenunternehmen mit seinen transnational relevanten, zehntausenden von Tonnen Ladung, die beinahe einen Fünftel des weltweiten Produkte- und Rohstoffversands ausmacht, stand regelecht still.[1025] Und zwar aus dem »simplen« Grund, dass die Software der Datenendgeräte, die auf elektronischem Weg den Inhalt der eintreffenden Frachtschiffe lesen sollte, vollständig gelöscht war.[1026] Eine digitale Abhängigkeit, die wohl bis zu jenem Zeitpunkt – zumindest in Bezug auf das Ausmass möglicher Konsequenzen eines Aussetzens – als solche unerkannt war. Das Schadprogramm hat zudem in irreversibler Weise die Kontrolldatensätze und Backups verschlüsselt, die – vereinfacht gesagt – dem Computer sagen, wo sich sein eigenes Betriebssystem befindet. Diese Datensätze des transnationalen Riesenunternehmens konnten in der Folge nur durch einen Zufall wiederhergestellt werden: Und zwar gab es in Ghana kurz vor dem Eintreffen des Cyberangriffs einen Stromausfall, womit die Computer jener Standorte nicht infiziert wurden und das Backup erhalten blieb.[1027] Nur deshalb konnten die gesamten digitalen Prozesse und Abläufe dieses globalen Unternehmens innert überschaubarer Zeit wiederhergestellt werden.

1020 Borys, BBC vom 04.07.2017; Greenberg, Wired vom 22.08.2018.
1021 Greenberg, Wired vom 22.08.2018.
1022 Greenberg, Wired vom 22.08.2018.
1023 Greenberg, Wired vom 22.08.2018.
1024 Generell zu kritischen digitalen Lieferketten: Ziga, S. 131.
1025 Greenberg, Wired vom 22.08.2018.
1026 Greenberg, Wired vom 22.08.2018.
1027 Greenberg, Wired vom 22.08.2018.

Das Beispiel NotPetya zeigt, dass durch den (vermeintlich) auf die Ukraine gerichteten Computerwurm weltweit Computer infiziert wurden, von denen lebensnotwendige Lieferketten wie die Lieferung von Medikamenten und Lebensmitteln abhingen, die vermutlich gar nicht Teil des eigentlichen Ziels waren. Es stellt sich des Weiteren nicht nur die Gefahr, dass Schadprogramme geklaut, sondern auch, dass sie mit anderen Schadprogrammen gekoppelt werden. Durch das Zusammenspiel von External Blue mit Mimikatz konnte nicht nur jeder ungepatchte, sondern auch jeder gepatchte Computer infiziert werden.[1028] Dabei erfuhren die Angreifer wohl erst mit der Freisetzung des Schadprogrammes, wie viele Computer tatsächlich betroffen würden. Meist weisen weltweit weitaus mehr Computer genau diese Sicherheitslücken auf als nur das ursprünglich beabsichtigte Zielsystem. Dieser (mittlerweile) grundsätzlich voraussehbare Umstand wird bei der Freilassung eines solchen Schadprogrammes nach vorliegend vertretener Ansicht daher zumindest in Kauf genommen. Aufgrund der mit dem Einsatz des Schadprogrammes unkontrollierten und exponenziellen Weiterverbreitung besteht das inzwischen bekannte Risiko verheerender Schäden nicht in klar lokalisierbaren Territorien, sondern potenziell weltweit. Da Verletzlichkeiten sowie die Abhängigkeit von Computersystemen und -netzwerken je nach Land unterschiedlich ausfallen und oft nicht vollumfänglich abschätzbar sind, können somit unvorhergesehene Schäden entstehen und unzählige Interessen beeinträchtigt werden. Hinzu kommt, dass der weltweite Schaden womöglich wesentlich minimiert hätte werden können, hätte man die gefundene Sicherheitslücke bei ihrer Entdeckung offengelegt und damit schliessen können (statt ein sie ausnutzendes Schadprogramm zu programmieren).[1029]

iii. Stuxnet als Cyberboomerang?

Wie bereits eingangs erwähnt, führte im Jahr 2010 der Einsatz des Schadprogramms Stuxnet zu physischen Beschädigungen der iranischen Atomanlage in Natanz. Von einigen Seiten wurde ebendiese Beschädigung im Vergleich zu herkömmlichen militärischen Operationen als relativ gering bezeichnet.[1030] Der Computerwurm sei so genau programmiert worden, dass er nur das spezifische Ziel angriff und nichts anderes als die Zentrifugen zerstörte.[1031] Oder

1028 Greenberg, Wired vom 22.08.2018. Eingehender zu Eternal Blue, Mimikatz, WannaCry und NotPetya siehe: Greenberg, Sandworm, S. 151 ff. m.w.V.; Lahmann, S. 11 ff. m.w.V.

1029 Ähnlich: Lahmann, S. 280; Greenberg, Sandworm, S. 104.

1030 Singer/Friedman, S. 118 f.

1031 Singer/Friedman, S. 118 f.

in den Worten SINGER/FRIEDMAN's: »*It [Stuxnet] was so discriminating it essentially gave a new meaning to the term.*«[1032] Dieser Lesart zufolge sei bei Stuxnet niemand verletzt oder getötet worden, und es sei weniger Schaden oder Zerstörung angerichtet worden als es bei vergleichbaren militärischen, kinetischen Angriffen der Fall gewesen wäre.[1033] Ähnlich wurde auch schon die These vertreten, dass Cyberangriffe das Gewaltniveau in Konflikten absenkten und sehr zielgerichtet seien. So könnten bspw. Radarstationen oder Raketenwerfer gezielt lahmgelegt werden, ohne dass diese bombardiert werden müssten.[1034] Allerdings kam im Falle Stuxnet Jahre nach seiner Entdeckung ans Licht, dass sich der Computerwurm in der Zwischenzeit über iranische Computer hinaus *international* auf weitere Systeme weiterverbreitet hatte.[1035] Der Computerwurm hatte sich in unkontrollierter Weise auf unbeabsichtigte, globale Ziele verbreitet, womit er letztlich doch nicht so zielgerichtet programmiert worden war, wie ursprünglich gedacht.[1036] Wie im November 2013 – drei Jahre nach dem Auftreten der beabsichtigten Schäden – bekannt wurde, hatte das Schadprogramm nämlich u.a. auch russische Atomanlagen sowie US-amerikanische Firmen wie die Ölfirma Chevron verseucht.[1037] Obschon der ursprünglich (vermeintlich) durch die USA programmierte Computerwurm auf die iranische Atomanlage in Natanz hätte abzielen sollen, verseuchte er letztlich also auch Unternehmen im eigenen Land. Indem die indirekt ausgelösten Schäden meist zeitverschoben ausgelöst bzw. entdeckt werden und jeweils in Art und Intensität unvorhergesehen und unterschiedlich ausfallen können, fördern Cyberangriffe gewissermassen Gewalt einer anderen Art: Cyberangriffe erreichen nicht nur Personen und Einrichtungen, die keine Ziele militärischer Operationen sein sollten, sondern es ist auch schwierig zu sagen, »*wie weit das gehen wird und wer betroffen sein wird, wenn Staaten diese Angriffe zur Zerstörung einsetzen*«.[1038] Dies gilt gleichermassen für offensive Angriffe, die zur Verteidigung gedacht sind. Stuxnet hat verdeutlicht, dass der Schuss bei Cyberangriffen oft »nach hinten losgeht« und, dass »alles was man im Cy-

1032 SINGER/FRIEDMAN, S. 119. Ähnlich NEWTON/MAY, S. 279.

1033 SINGER/FRIEDMAN, S. 118 f.

1034 Siehe RID, Cyberwar and Peace, S. 85: »*The most sophisticated cyberattacks are highly targeted, and cyberweapons are unlikely to cause collateral damage in the same way conventional weapons do.*« Im Ergebnis spricht er sich jedoch ebenfalls für passive Cyberverteidigungsmassnahmen und *gegen* aktive Cyberverteidigung aus: S. 87. Vgl. KORMANN, Interview mit Sandra Joyce, NZZ vom 31.03.2020.

1035 BAEZNER/ROBIN, Stuxnet, S. 11.

1036 SINGER, S. 80.

1037 BETSCHON, NZZ vom 11.11.2013.

1038 KORMANN, Interview mit Sandra Joyce, NZZ vom 31.03.2020.

berraum tut, sich als Boomerang erweisen kann«.[1039] Eskalationsspiralen dürften somit gerade auch im Cyberbereich möglich sein, wenn auch mit (bzw. gerade aufgrund) zeitlicher Verzögerung.

d. Zwischenfazit

Die erwähnten Beispiele illustrieren, dass nicht zu unterschätzende Gefahren auch von defensiv ausgerichteten Programmen ausgehen. Auch wenn aktive Cyberverteidigungsmittel grundsätzlich zu defensiven Zwecken vorgesehen sind, werden sie offensiv (und potenziell rechtswidrig) eingesetzt.[1040] Durch digitale Selbstverteidigungshandlungen ist, wie vorangehend ersichtlich wurde, nämlich ein weitreichenderer Schaden denkbar als zuvor abschätzbar ist.[1041] Es besteht im Rahmen einer Gesamtwürdigung ferner das zusätzliche Risiko, dass durch Staaten (auch zwecks Verteidigung) vorprogrammierte Programme gestohlen werden[1042] oder sich bei ihrem Einsatz über ihr militärisches Zielsystem hinaus verbreiten. Ihre Programmierung und Herstellung verringert insgesamt (und sogar unabhängig vom konkreten Einsatz als Verteidigungsmassnahme) das allgemeine Sicherheitsniveau für digitale Infrastrukturen und widerspricht den eigentlichen Sicherheitszielen internationaler Prozesse:[1043] Der Bericht der UN GGE 2015 sowie der Paris Call for Trust and Security in Cyberspace 2018 rufen Staaten generell dazu auf, die Verbreitung von offensiven Cybermitteln zu verhindern.[1044]

Bejaht man ein Recht auf digitale Selbstverteidigung (oder Gegenmassnahmen), liegt die Konsequenz nahe, dass diese Art von Verteidigungsmassnahmen weiterhin zunimmt.[1045] Allerdings dürfen sich Staaten aufgrund strategischer Anreize nicht über das Erfordernis der Verhältnismässigkeit

---

1039 Betschon, NZZ vom 11.11.2013. Ähnlich: Middleton, S. 1 ff.; Glenny, New York Times vom 24.06.2012.

1040 Lahmann, S. 280.

1041 Ähnlich: Schmitt, Countermeasures Response Option, S. 726: »*The interconnected and interdependent nature of cyber systems may render it difficult to accurately determine the degree of damage that a countermeasure will likely cause*«.

1042 Lahmann, S. 280.

1043 Lahmann, S. 279.

1044 UN Doc. A/RES/70/174 (2015), §13(i); Paris Call 2018; Lahmann, S. 279.

1045 Lahmann, S. 283. Schmitt sieht sogar die Möglichkeit, dass digitale Gegenmassnahmen – vorausgesetzt sie werden adäquat und weise eingesetzt – auch auf nicht-digitale Völkerrechtsverletzungen folgen können, was den Radius möglicher Reaktionen erheblich erweitern würde: Schmitt, Countermeasures Response Option, S. 732.

hinwegsetzen.[1046] Solange Gegenschläge über das Ausmass des ursprünglichen Angriffs hinausgehen und zeitverschoben zivile oder staatliche Computerinfrastrukturen im eigenen oder in fremden Staaten infizieren können, werden militärische Entscheide daher jeweils auch eine völkerrechtliche Komponente haben. Für eine möglichst präzise und adäquate militärische Einschätzung werden diese Unsicherheiten daher regelmässig zu gross sein.[1047] Der globale Radius potenzieller Schäden und Verletzungen impliziert also insgesamt ein (unverhältnismässiges) Eskalationsrisiko.[1048] Es scheint somit nicht nur aus rechtlicher, sondern auch aus strategischer Sicht sinnvoll, militärische Selbstverteidigungshandlungen restriktiv zu handhaben. Aktive Cyberverteidigungsmassnahmen sollten der hiesigen Ansicht zufolge und dem völkerrechtlichen Verhältnismässigkeitsprinzips entsprechend – vergleichbar mit einem flächendeckenden kinetischen Angriff, bei dem eine hohe Anzahl möglicher »Nebeneffekte« denkbar ist – wenn überhaupt, nur sehr restriktiv als notwendig und verhältnismässig qualifiziert werden. Indem die Gefahr von Kollateralschäden beim Einsatz von Cyberverteidigungsmassnahmen jeweils sehr real ist, läuft man regelmässig Gefahr, über das Ziel der Abwehr hinauszuschiessen.[1049]

Indem weder die Art noch die Intensität der Effekte von Cyberangriffen und -gegenangriffen zum Zeitpunkt des Angriffs konkret voraussehbar sind, sollten Cyber(verteidigungs-)massnahmen im künftigen Diskurs differenzierter betrachtet werden – dies auch vor dem Hintergrund, dass retrospektiv oft nicht ganz klar ist, welche Schäden durch Cyberangriffe ausgelöst wurden, da sie oftmals unentdeckt bleiben oder die Kausalzusammenhänge schwer zurückzuverfolgen sind.[1050] Sollten für die Neutralisierung eines Cyberangriffs geeignete Hackbacks oder andere aktive digitale Verteidigungsmassnahmen definiert werden, müsste geklärt werden, wie man mit der Inkaufnahme unbeabsichtigter (auch digitaler) Folgeschäden umgeht bzw. welches Mass an Sorgfalt erforderlich ist, um solche möglichst auszuschliessen. Denn auch

1046 Vgl. Lahmann, S. 283.

1047 Vgl. Mäder/Sansano, Interview mit Süssli und Vuitel, NZZ vom 06.01.2021.

1048 Lahmann, S. 283.

1049 Vgl. Heintschel von Heinegg, Informationskrieg, S. 144 in Bezug auf elektronische Selbstverteidigungsmassnahmen: »*Kann nicht ausgeschlossen werden, dass dabei die Systeme unbeteiligter Staaten in Mitleidenschaft gezogen werden, sind zumindest ernsthafte Zweifel an der Verhältnismässigkeit und damit an der Rechtmässigkeit der Gegenmassnahmen angezeigt*«.

1050 Vgl. Newton/May, S. 71: »*Both the source of a cyber attack and the true extent of the damage it has caused will generally be opaque*«.

wenn in einzelnen Konstellationen aktive »Echtzeit«-Cyberverteidigungsmassnahmen als notwendig erachtet werden, um Schäden abzuwenden, muss man sich bewusst sein, dass man jeweils unbefugt in fremde Systeme eindringt, die unter Umständen als Brückenkopf verwendet wurden. Zudem wird man die für eine im Rahmen von Art. 51 UN-Charta vorausgesetzten physischen Schäden in den wohl meisten Fällen mit digitalen Gegenschlägen ohnehin nicht abwehren können, wenn diese *bereits* oder bei einer Frühentdeckung *noch nicht* eingetroffen sind. Hinzu kommt, dass bei den allermeisten Cyberangriffen im Falle einer ausstehenden technischen und rechtlichen Zurechnung im Moment des Angriffs nicht sogleich davon ausgegangen werden kann, dass ein Staat für die Angriffe verantwortlich ist. Eine »Echtzeit«-Cyberverteidigungsmassnahme, die im Kontext von Art. 51 UN-Charta einer sofortigen Verteidigung gegen einen anderen *Staat* dienen würde, lässt somit keinen zeitlichen Raum für die notwendige Benachrichtigung des Staates, der die (im Zweifelsfalle) nichtstaatlichen Hacker »beherbergt«.[1051] Fraglich bleibt auch, ob potenzielle »Langzeitnebeneffekte« (wie die Schädigung von Drittstaaten, der Zivilbevölkerung oder von transnationalen Unternehmen) insgesamt gegenüber dem ursprünglichen Angriff verhältnismässig wären. Dies ist auch deshalb fraglich, weil die quantitative und qualitative Abhängigkeit digitaler Infrastrukturen von Land zu Land variiert.[1052] Die vielen involvierten Interessen sowie die meist alternativ verfügbaren Möglichkeiten abseits offensiver Cyberverteidigung schliessen Letztere zwar nicht pauschal aus, drängen jedoch eine restriktive Bejahung der Verhältnismässigkeit auf. Eine ähnliche Argumentationsweise vertritt Gray im Zusammenhang mit herkömmlichen militärischen Einsätzen:[1053] Ihr zufolge kann, wie bereits unter IV.A.1.b. erwähnt, militärische Selbstverteidigung nicht notwendig sein, wenn diese zur Abwehr ungeeignet oder kontraproduktiv ist. Seien unbeabsichtigte »Nebeneffekte« einer militärischen Massnahme sehr wahrscheinlich (»*if there is a high chance of unintended consequences*«), spreche daher vieles dafür, dass der Einsatz militärischer Selbstverteidigung nicht verhältnismässig sei. Schütze eine militärische Gewaltanwendung einen Staat im Ergebnis nicht, oder sei diese für die Verteidigung des eigenen Territoriums realistisch gesehen nicht erfolgsver-

1051 Vgl. Lahmann, S. 273 f. Er verweist in diesem Zusammenhang auf den Mechanismus des »CyberCop« Systems der NSA, das auf eingehende DDoS-Angriffe automatisch mit »Counter-DDoS«-Angriffen gegen die Ursprungsserver reagiert.

1052 Lahmann, S. 132.

1053 Gray, Limits of Force, S. 114.

sprechend, gehe eine solche daher über eine rechtlich erlaubte Selbstverteidigung hinaus.[1054] Demzufolge seien unbeabsichtigte (Langzeit-)Effekte durchaus von rechtlicher Relevanz.[1055]

Insgesamt sollte der Fokus digitaler Gegenmassnahmen vermehrt auf einer effektiven Schadens*begrenzung und -beendigung* von Cyberangriffen liegen. In dieser Hinsicht steigt vor allem die Bedeutung völkerrechtlich unproblematischer, präventiver und passiver Verteidigungsmassnahmen, die das eigene System nicht verlassen. Vor dem Hintergrund einer effektiven Verteidigung müsste daher allerdings eingehender geklärt werden, welches überhaupt die zur Abwehr tauglichen aktiven und passiven digitalen Massnahmen sind.[1056] Dies erfordert ein erhöhtes interdisziplinäres Verständnis der Eigenschaften, Funktionsweisen *und* der Gefahren der jeweiligen Technologien.

Derzeit erscheint es unrealistisch, dass Staaten von der Entwicklung aktiver Cyber(verteidigungs)mittel absehen werden.[1057] Und indem erste Staaten ihre digitalen Militärkapazitäten aufrüsten, rücken weitere Staaten nach. Dennoch muss man bei der dahingehenden Ansicht, dass Hackbacks und weitere Cyberverteidigungsmassnahmen legitim sind, dringend auch die Grenzen der Aufrüstung[1058] *und* des Einsatzes von Cyberkapazitäten diskutieren.[1059] Vorgeschlagen wurde bereits eine generelle Offenlegungspflicht entdeckter Sicherheitslücken – was einer Aufrüstung offensiver technischer Kapazitäten grundsätzlich entgegenstünde.[1060] Statt sich diese für eigene Kapazitäten und Schadprogramme vorzubehalten, sollten gefundene Software- oder Hardwarefehler dem Anbieter unverzüglich mitgeteilt werden, damit das Unternehmen seine Fehler beheben, die Lücke schliessen und/oder die legitimen

1054 Sie zeigt die beschränkte Wirksamkeit von Gewalteinsätzen anhand vergangener Konflikte und deren unbeabsichtigten »Nebeneffekte« auf: GRAY, Limits of Force, S. 114 ff., S. 120 ff.

1055 GRAY, Limits of Force, S. 120.

1056 Zu einer Differenzierung aktiver und passive Mittel z.B.: SKLEROV, S. 72 ff.

1057 SCHMITT sieht grundsätzlich sogar einen Vorteil in der Erweiterung der Reaktionsmöglichkeiten auf Cybergegenmassnahmen: SCHMITT, Countermeasures Response Option, S. 732.

1058 Vgl. LAHMANN, S. 279.

1059 Ähnlich rät SCHMITT den Staaten to »*carefully consider the prospects for using countermeasures to respond to "below the threshold" cyber operations and to begin developing procedures and rules of engagement for their employment*«: SCHMITT, Countermeasures Response Option, S. 732.

1060 Eingehender dazu: DELERUE, Cyber Operations, S. 371 ff.

Nutzer von Geräten darauf hinweisen kann.[1061] Sollte eine solche Offenlegungspflicht tatsächlich und reziprok respektiert werden, könnte dies zur Erhöhung der allgemeinen Sicherheit im Cyberraum beitragen.

Dieser Dissertation zufolge drängt sich angesichts des Verhältnismässigkeitserfordernisses bei *jeder* digitalen oder kinetischen Selbstverteidigungshandlung im Cyberkontext eine Risikoabwägung auf. Diese (im Rahmen der staatlichen Sorgfaltspflicht zu erfolgende[1062]) technische *und* strategische Einschätzung würde dabei wie folgt lauten: Einerseits muss man die durch einen Cyberangriff kausal ausgelöste (im Rahmen von Art. 51 UN-Charta *physische*) *Schädigung* definieren, die für die Verteidigung ursächlich ist (was bereits schwierig ist). Andererseits müssen die im Rahmen der Risikoeinschätzung erwarteten *Nutzen der Abwehrsfunktion* der Verteidigungshandlung sowie die möglichen *Kosten beabsichtigter und unbeabsichtigter (Kollateral-)Schäden* abgewogen werden. Überwiegen insgesamt die Kosten einer potenziellen Eskalation den Nutzen einer Reaktion, wird eine militärische Reaktion sowohl aus rechtlicher als auch strategischer Sicht regelmässig keinen Sinn machen.[1063] Obschon dies in der Theorie einfach scheint, werden solche Abwägungen angesichts absehbarer technischer Umbrüche wie dem Aufkommen künstlicher Intelligenz oder zunehmend automatisierter Systeme mit wesentlichen Schwierigkeiten konfrontiert sein. Hinzu kommt des Weiteren die (subjektiv geprägte) Abwägung von Interessen im Einzelfall. Dies impliziert letztlich zusätzliche – unter Umständen massgebliche – Ermessensbereiche bei einer jeden Risikoabwägung.

1061 Siehe ausführlicher dazu und zu möglichen Ausnahmen dieser Offenlegungspflicht: LAHMANN, S. 280 f.

1062 Vgl. dazu SCHMITT, Countermeasures Response Option, S. 726, der im Rahmen einer Einzelfallwürdigung voraussetzt, dass ein reagierender Staat Sorgfalt walten lassen muss: »*States will have to exercise due care in assessing whether their actions will be proportionate to the injury suffered and principle involved. This may require, for instance, mapping the targeted system. Since due care is a contextual standard influenced by such factors as the severity of the harm suffered, the extent of further damage caused by any delay, the cyber capabilities of the injured State, and the responsible State's vulnerabilities, it must be determined on a case-by-case basis.*« Ähnlich leitet WICKER eine Sorgfaltspflicht (»*duty of care*«) des sich verteidigenden Staats aus dem Verhältnismässigkeitsprinzip ab: WICKER, S. 67.

1063 Im Zusammenhang mit kinetischen Reaktionen: GROSS, S. 219.

3. Zusammenfassung: Veränderte Bedeutung der Verhältnismässigkeit bei Cyberangriffen?

Die internationale Gemeinschaft hat die Verhältnismässigkeit als ein fundamentales Prinzip des *ius ad bellum* akzeptiert, das bereits vor der UN-Charta bestand und auch im modernen Völkerrecht Geltung behalten soll.[1064]

Die Bedeutung der *ius ad bellum*-Verhältnismässigkeit verändert sich bei Cyberangriffen grundsätzlich nicht. Was sich ändert (und sich wohl auch künftig verändern wird) ist der Untersuchungsgegenstand »Cyberangriffe«. Das Prinzip ist daher grundsätzlich auf Cyberangriffe anwendbar, verbleibt im Einzelnen jedoch klärungsbedürftig. Es ändern sich insb. die für die Beurteilung verhältnismässiger Selbstverteidigungshandlungen nach Art. 51 UN-Charta relevante Art und Unmittelbarkeit, die Voraussehbarkeit sowie der Radius und Kausalzusammenhang von Schädigungen. Wendet man das Prinzip allerdings seinem Sinn und Zweck entsprechend an, kann man defensive und offensive digitale und kinetische Verteidigungshandlungen rechtlich erfassen, wie andere militärische Operationen auch.[1065] Es bietet einen hinreichenden rechtlichen Rahmen, um Grenzen zu bestimmen, ohne dass neue Normen definiert werden müssten. Da es völkerrechtlich unumstritten ist, dass staatliches Verhalten im Rahmen von Art. 51 UN-Charta dem Prinzip verpflichtet ist, sollte es gem. vorliegend vertretender Meinung ernst genommen und als Rechtsprinzip gestärkt werden. Wird es ernst genommen, kann es im internationalen Kontext dazu beitragen, wie die Grenzen gewaltsamer militärischer Einsätze künftig gesehen werden. Gleichzeitig muss die Flexibilität[1066] des Prinzips gewahrt werden, damit das Recht auf Selbstverteidigung in einem zu bejahenden Fall zum Schutz eines Staates ausgeübt werden kann.

Insgesamt bleibt die völkerrechtliche Verhältnismässigkeit angesichts international divergierender Ansichten vage und bedarf einer (mitunter subjektiven) Interessenabwägung im Einzelfall. Cyberangriffe mit ihren Unsicherheiten eröffnen somit einen zusätzlichen Ermessensspielraum – und zwar in komplexen technischen Bereichen, die juristischen und politischen Entscheidungsträgern oftmals eher schwer zugänglich sein dürften. Angesichts dessen ist

1064 Gardam, Proportionality and Force, S. 403 m.w.V.

1065 Petkis, S. 1451.

1066 Zum inhärenten Erfordernis der Flexibilität des Verhältnismässigkeitsprinzips: Gardam, Proportionality and Force, S. 412; Ago, S. 69; Dinstein, War, Aggression and Self-Defence, S. 251; Dinstein, Proportionality and Necessity, S. 57; Wicker, S. 64, S. 111. Das Element der Flexibilität allerdings in Perspektive setzend: Wicker, S. 105 ff.

das Prinzip nach vorliegend vertretener Meinung im Cyberkontext zeitlich und inhaltlich eng zu fassen. Da dennoch ein dem Prinzip inhärenter Ermessenspielraum verbleibt, ist es zudem wichtig, sich anhand möglichst objektivrechtlicher Kriterien zu orientieren. Daher sollten objektive Betrachter wie die Wissenschaft und internationale Gerichtshöfe[1067] weiterhin dazu beitragen, wie man mit dem Ermessenspielraum umgehen soll. WICKER schlägt in diesem Zusammenhang für das völkerrechtliche Selbstverteidigungsrecht eine an die öffentlichrechtliche Verhältnismässigkeit des deutschen Rechts anlehnende Prüfung vor.[1068] Jener zufolge erfolgt die Prüfung – ähnlich der öffentlichrechtlichen Verhältnismässigkeitsprüfung gem. Art. 36 Abs. 3 der Schweizer Bundesverfassung – anhand der (1) Geeignetheit, der (2) Erforderlichkeit und der (3) Angemessenheit (Verhältnismässigkeit i.e.S.) einer getroffenen staatlichen Massnahme.[1069] Das letzte Kriterium impliziert dabei eine (Gesamt-)Würdigung der Zweck-Mittel-Relation vor dem Hintergrund der involvierten Interessen.[1070] Mit einer sich an diese Kriterien anlehnenden Verhältnismässigkeitsprüfung würde man folglich den flexiblen, subjektiven Ermessenspielraum im Einzelfall primär auf den letzten Punkt beschränken, da die beiden ersten Kriterien – die Erforderlichkeit und die Geeignetheit – i.d.R. objektiv festgelegt werden können.[1071] Insgesamt scheint gem. WICKER (und gem. der hier vertretenen Ansicht) die von ihm vorgeschlagene Verhältnismässigkeitsprüfung auf Art. 51 UN-Charta übertragbar, indem eine Selbstverteidigungsmassnahme jeweils geeignet sein muss, den Angriff abzuwehren (Geeignetheit), es sich um das mildeste Mittel (Notwendigkeit/Erforderlichkeit) handeln und die Massnahme insgesamt angemessen sein muss.[1072] Nach vorliegend vertretener Auffassung sollte dabei im Kontext von Art. 51 UN-Charta insb. das (gem. WICKER weitgehend objektiv bestimmbare) Erfordernis der *Geeignetheit* einer Verteidigungshandlung zur Abwehr noch expliziter im völkerrechtlichen Diskurs betont und als Prinzip gestärkt werden. Dadurch könnte eine objektive Komponente des Verhältnismässigkeitsdiskurses gestärkt werden, die auch in künftigen Diskursen unabhängig des Untersuchungsgegenstandes von Relevanz sein könnte. Denn ist eine Verteidigungshandlung nicht zur Abwehr ge-

1067 Vgl. WOLTAG, S. 181, der ebenfalls anführt, dass die (subjektive) Würdigung von unilateralen Gegenmassnahmen Gegenstand einer juristischen Abhandlung eines internationalen Gerichts oder Tribunals sein kann.

1068 Siehe: WICKER, S. 109 ff.

1069 WICKER, S. 110 m.w.V.

1070 WICKER, S. 111.

1071 WICKER, S. 111.

1072 WICKER, S. 113.

eignet, kann sie nach vorliegend vertretener Ansicht nicht der Selbstverteidigung eines Staates zur Sicherung seiner Existenz dienen und sollte folglich nicht als verhältnismässig erachtet werden können.[1073] Demnach müssen das jeweilige Ziel sowie die Tauglichkeit einer Verteidigungsmassnahme vor dem Hintergrund der Verhältnismässigkeit jeweils kritisch hinterfragt werden.[1074] Im Zusammenhang mit Cyberangriffen (DDoS-Angriffe sowie auch Würmer, Viren und trojanische Pferde) ist sowohl ein digitaler als auch ein kinetischer Gegenangriff oft ungeeignet, den Schaden zu begrenzen oder zu beenden, wenn die für einen bewaffneten Angriff relevanten physischen Schäden bereits eingetroffen oder die betreffenden Systeme bereits blockiert sind.

Ermessensspielräume und Interessenabwägungen wird es bei Verhältnismässigkeitsfragen immer geben. Historisch gesehen hat gerade diese Flexibilität den Vorteil, dass herkömmliche Normen weiterhin auf sich verändernde Untersuchungsgegenstände anwendbar bleiben. Und trotz objektiver Kriterien wird man, wie diese Abhandlung aufzuzeigen versucht hat, rechtliche Normen weiterhin flexibel anwenden können.[1075] Die internationale Staatengemeinschaft wird demzufolge weiterhin mit Ermessensspielräumen arbeiten müssen. Solange die Geltung des Prinzips insgesamt allerdings bestätigt wird, müssen sich Staaten immerhin rechtfertigen, sollten potenziell disproportionale Nebeneffekte ausgelöst werden. Extensive sowie restriktive Haltungen werden letztlich für die künftige Bedeutung oder Untergrabung des machteindämmenden Charakters des Prinzips relevant bleiben und das Prinzip (sowie künftige Konfliktführungs- und bewältigungsstrategien) weiterhin formen.

1073 GRAY, Limits of Force, S. 101 ff., S. 120 f.; WICKER, S. 113.

1074 Vgl. NEWTON, S. 32: »*Proportionality is about trying to justify tactics by considering what those tactics are aimed to accomplish*«. GARDAM, Necessity, Proportionality, S. xv: »*Proportionality is a familiar idea and is designed to ensure that the ends justify the means*«.

1075 WICKER, S. 111.

B. Verhältnismässigkeit und nicht-militärische Gegenmassnahmen

Die staatlichen Reaktionsmöglichkeiten auf eine zurechenbare völkerrechtliche Normverletzung[1076] durch Cyberangriffe sind grundsätzlich die Retorsion, nicht-militärische Gegenmassnahmen sowie das Einbeziehen des Sicherheitsrats.[1077] Daneben besteht immer auch die Möglichkeit, sich an ein internationales Gericht zu wenden.[1078] Gegenmassnahmen sind im Prinzip ausnahmsweise erlaubte Kompensationen eines vorangehenden Völkerrechtsverstosses.[1079] Diese werden im völkerrechtlichen Selbsthilferecht in einem Verletzungsfall i.d.R. unilateral durch den betroffenen Staat getroffen. Durch das Einbeziehen des Sicherheitsrats können durch die UNO allerdings auch kollektive Massnahmen gem. Art. 41 UN-Charta verhängt werden. Daneben gibt es kollektive Sanktionen der EU oder Handelssanktionen im WTO-System.[1080] Im vorliegenden Kapitel liegt der Fokus jedoch auf den konventionellen Gegenmassnahmen gem. Art. 49 ff. ARSIWA, die durch den verletzten Staat selbst veranlasst werden.[1081] Es handelt sich dabei um den Kontext der völkerrechtlichen Staatenverantwortlichkeit (im Englischen: »*state responsibility*«).

1076 Damit sind vorliegend Völkerrechtsverstösse unterhalb der Schwelle von Art. 51 UN-Charta gemeint. Siehe dazu die vorangehenden Ausführungen zu möglichen Völkerrechtsverstössen durch die Verletzung der Due-Diligence-Pflicht oder des Gewalt- und Interventionsverbots unter III.B.2.

1077 Roscini, Cyber Operations, S. 105. Eingehend zu den Konsequenzen eines Völkerrechtsverstosses: Crawford, Brownlie's Principles, S. 552 ff.

1078 Roscini, World Wide Warfare, S. 111.

1079 Diggelmann, Völkerrecht, S. 159. Substanziell zum Gegenmassnahmenrecht des Weiteren u.a.: Alland, S. 1129 ff.; Crawford, State Responsibility, S. 675 ff.; Zoller, S. 179 ff.; Elagab, S. 37 ff.; White/Abass, S. 521 ff.

1080 Peters/Petrig, S. 397.

1081 Während das Recht des verletzten Staates auf Gegenmassnahmen im Rahmen der Selbsthilfe unbestritten ist, bleibt die Frage nach einem »kollektiven« Gegenmassnahmenrecht durch Drittstaaten (sog. third-state countermeasures) umstritten. Siehe sogleich unter Fn. 1106.

Im Rahmen der Staatenverantwortlichkeit hat ein verletzter Staat auf dem unilateralen Weg zunächst Anspruch auf Beendigung und Nichtwiederholung einer Verletzung nach Art. 30 ARSIWA.[1082] Hinzu kommen gem. Art. 31 und 34 ff. ARSIWA Ansprüche auf Einstellung des völkerrechtswidrigen Verhaltens, sofern dieses noch andauert,[1083] auf Entschädigung und Wiedergutmachung.[1084] Letztere können in Form von Naturalersatz (Art. 35 ARSIWA), Schadenersatz (Art. 36 ARSIWA) oder bei immateriellen Schäden durch Genugtuung (Art. 36 ARSIWA) erfolgen.[1085] Gegenmassnahmen kommen dann zur Anwendung, wenn der Verletzerstaat sein Verhalten nicht einstellt und/oder keine Entschädigung leistet.[1086] Pönalisierende und vergeltende Repressalien sind dabei allerdings unzulässig.[1087] Gegenmassnahmen konstituieren nämlich keine Bestrafung,[1088] sondern sollen der »Durchsetzung« völkerrechtlicher Ansprüche dienen.[1089] Diese erfolgt in der dezentralen Praxis des Völkerrechts oft eben nicht automatisch.[1090] Das Gegenmassnahmenrecht ist von der Idee her somit ein »Ausgleichs- oder Kompensationsrecht«.[1091] Der Verletzerstaat soll gem. Art. 28 ff. ARSIWA bewegt werden, die Verletzung zu beheben und zu kompensieren. Die Einstellung des völkerrechtswidrigen Verhaltens soll mittels Zufügung von Nachteilen erfolgen.[1092] Die Völkerrechtsbefolgung (»*compliance*«)

1082 Dazu: Crawford, State Responsibility, S. 459 ff.

1083 Art. 30 ARSIWA; ARSIWA-Kommentar, Art. 30; IGH, Teheraner Geiselfall, §95, Ziff. 3; IGH, Nicaragua-Urteil, §292 Ziff. 12.

1084 Art. 31 ARSIWA; ARSIWA-Kommentar, Art. 31. Das Wiedergutmachungserfordernis hat bereits der Ständige Internationale Gerichtshof im Chorzów-Fall 1928 festgehalten: StIGH, Chorzów-Fall, S. 21. Eingehender dazu: Arangio-Ruiz, S. 1 ff.; Crawford, State Responsibility, S. 480 ff. Zum Verhältnis zwischen der Pflicht zur Wiedergutmachung und dem Recht zur Ergreifung von Sanktionen: Schulze, S. 69 ff.

1085 Peters/Petrig, S. 392 f.

1086 Crawford, Brownlie's Principles, S. 553; Peters/Petrig, S. 395.

1087 Eingehender dazu unter seinem Kapitel »From Reprisals to Proportionate Countermeasures«: Wicker, S. 74 ff. Ferner auch: Alland, S. 1127 ff.; Diggelmann, Völkerrecht, S. 159; O'Connell, Power and Purpose, S. 257.

1088 Cassese, S. 306; Epiney, S. 49 f.; Wicker, S. 71; Zemanek, Unilateral Enforcement, S. 37. Ferner dazu auch: Sicilianos, Reprisals and Denunciation, S. 344.

1089 Crawford, State Responsibility, S. 541; O'Connell, Power and Purpose, S. 257; Wicker, S. 72. Vgl. die Umschreibung in Teil drei der ARSIWA: »Durchsetzung der Staatenverantwortung«.

1090 Crawford, State Responsibility, S. 95.

1091 Diggelmann/Hadorn, S. 265; Roscini, Cyber Operations, S. 106; Schulze, S. 71.

1092 Diggelmann, Völkerrecht, S. 159; Peters/Petrig, S. 395; Schröder, S. 745.

und die internationale Verantwortung des Verletzerstaats sollen durch Druckausübung sichergestellt werden.[1093] Die Massnahme muss dabei »so weit möglich« reversibel sein.[1094]

Zu den nicht-militärischen Gegenmassnahmen zählen etwa ökonomische, diplomatische oder politische Massnahmen. Dazu zählen bspw. die Möglichkeit von Handelssanktionen, das Einfrieren individueller Bankkonti oder Reiseverbote.[1095] Beispiele für eine Retorsion hingegen wären der Nichtabschluss eines für die Gegenseite interessanten Handelsvertrags, der Abbruch diplomatischer Beziehungen oder die Einstellung von rechtlich nicht geschuldeter Entwicklungshilfe.[1096] Beispiele für kollektive UN-Wirtschaftssanktionen wären ferner ein Verbot des Exports oder Transports bestimmter Waren in den oder vom Zielstaat (=Embargo/Boykott). Wirtschaftssanktionen sind in der Praxis der wichtigste Fall von Gegenmassnahmen.[1097] Ein Beispiel sind die Sanktionen des UN-Sicherheitsrats gegen den Iran in den Jahren 2006 bis 2015, bei denen u.a. Bankkontoeinfrierungen, ein Verbot der Lieferung verschiedener für das Atomprogramm relevanter Materialien, ein Waffenembargo und Reisesperren verhängt wurden.[1098] Ein Beispiel für unilaterale Sanktionen wäre das US-amerikanische Embargo gegen Kuba ab 1960.[1099]

Die Rechtmässigkeit von Gegenmassnahmen unterliegt bestimmten Anforderungen. So gibt es »sanktionsfeste« Normen, die durch Gegenmassnahmen nicht missachtet werden dürfen. Dazu zählen mitunter grundlegende Menschenrechte und das *ius cogens*, das Gewaltverbot gem. Art. 2(4) UN-Charta,[1100] der Grundsatz der Unverletzlichkeit diplomatischer und konsularischer Ein-

1093 Art. 49 ARSIWA; Crawford, Brownlie's Principles, S. 573; Sreenivasa, S. 874; Wicker, S. 71.

1094 Art. 49 ARSIWA; Roscini, Cyber Operations, S. 106; Sreenivasa, S. 874.

1095 Vgl. Hathaway, Active Defense, S. 50; Hathaway/Shapiro, Enforcement, S. 311 ff.

1096 Hathaway/Shapiro, Enforcement, S. 314 ff.; Peters/Petrig, S. 396; Sreenivasa, S. 857.

1097 Peters/Petrig, S. 397. Zu ökonomischen Massnahmen u.a.: White/Abass, S. 535 ff.

1098 Peters/Petrig, S. 397 mit den entsprechenden Verweisen.

1099 Siehe: U.S. Department of State, Cuba Sanctions, abrufbar unter: <https://www.state.gov/cuba-sanctions/> (zuletzt besucht: März 2023). Zu weiteren Beispielen von Sanktionen: White/Abass, S. 535 ff.

1100 Vgl. Art. 50(1)(a) ARSIWA. Dazu: Sreenivasa, S. 869; Sklerov, S. 37. Die ausnahmsweise Möglichkeit vom Gewaltverbot abzuweichen ist – wie vorliegend bereits unter III.B. abgehandelt – abschliessend in Art. 51 UN-Charta geregelt. Obwohl das Verbot gewaltsamer Selbsthilfe im Gegenmassnahmenrecht in der Theorie bewusst absolut gehalten ist, ist die Anwendung desselben in der Praxis komplexer. Eingehender dazu: Franck, Recourse to Force, S. 109 ff., S. 174 ff. Dazu auch: Schmitt, Countermeasures Response Option, S. 701, S. 718.

richtungen sowie das humanitäre Völkerrecht.[1101] Zudem dürfen durch Gegenmassnahmen grundsätzlich keine Rechte von Drittstaaten beeinträchtigt werden.[1102] Da Gegenmassnahmen auf den Ausgleich einer Völkerrechtsverletzung gerichtet sind, sind »präventive« Gegenmassnahmen grundsätzlich nicht erlaubt.[1103] Auch sind sie daher nur so lange gerechtfertigt, als dass eine Verletzung anhält.[1104] Grundsätzlich ist zudem nur der verletzte Staat selbst subjektiv berechtigt, Gegenmassnahmen zu lancieren. Es ist umstritten, inwieweit Drittstaaten zu Gegenmassnahmen befugt sind, wenn sog. »*erga omnes*«-Normen[1105] verletzt werden.[1106] Gemäss Art. 44 lit. b ARSIWA muss der innerstaatliche Rechtsweg grundsätzlich erschöpft worden sein, bevor Gegenmassnahmen in Frage kommen. Des Weiteren muss der verletzte Staat, bevor er Gegenmassnahmen lanciert, den Verletzerstaat gem. Art. 52 Abs. 1 lit. a ARSIWA zur Einstellung des völkerrechtswidrigen Handelns auffordern und Gegenmassnahmen gem. lit. b ankündigen sowie Verhandlungen anbieten.[1107] Diese prozeduralen Voraussetzungen sollen insgesamt dem Risiko einer Eskalation durch Gegenmassnahmen entgegenwirken und werden grundsätzlich kumulativ verstanden.[1108] Von letzterem Erfordernis (lit. b) ausgenommen ist die Möglichkeit »dringlicher Gegenmassnahmen« gem. Art. 52 Abs. 2 ARSIWA. Im Kern müssen Gegenmassnahmen allerdings als eine Ausnahme verstanden werden, vom generellen Erfordernis der friedlichen Streitbeilegung

1101 Peters/Petrig, S. 398.

1102 Zu Ausnahmen von diesem Grundsatz: ARSIWA-Kommentar, Art. 49(5). Eingehender dazu nachfolgend unter IV.B.2.

1103 Zu einer Auflistung der Voraussetzungen: Peters/Petrig, S. 398 f.

1104 Wicker, S. 71.

1105 *Erga omnes*-Verpflichtungen betreffen kollektive Interessen der gesamten Staatengemeinschaft. Bei einer Verletzung gelten unter Umständen alle Staaten als (mittelbar) Berechtigte: Art. 48 Abs. 1 lit. a und b ARSIWA; ferner auch: Art. 42 lit. b ARSIWA. Siehe dazu u.a.: Diggelmann, Völkerrecht, S. 162.

1106 Vgl. Art. 54 ARSIWA. Dabei erlaubt der Wortlaut von Art. 54 ARSIWA für Drittstaaten lediglich »lawful measures«, womit im Grunde die völkerrechtlich unbedenkliche Retorsion und nicht Gegenmassnahmen gemeint sind. Die Kommentare überlassen die diesbezügliche Klärung der Weiterentwicklung des Völkerrechts. Obschon die Debatte weiterhin anhält, besteht eine Tendenz in Richtung *de lege ferenda*, Gegenmassnahmen auch für Drittstaaten zu erlauben: Wicker, S. 70. Eingehend dazu unter besonderer Betrachtung des Verhältnismässigkeitsprinzips: Katselli, S. 1 ff. Ferner: Sicilianos, Countermeasures, S. 1137 ff.; Tams, Enforcing Obligations.

1107 IGH, Gabčíkovo-Nagymaros-Urteil, §84; Luftverkehrs-Schiedsspruch (1978), §85 ff. Dies kann gem. ARSIWA-Kommentar, Art. 52(3) als generelle Praxis gewertet werden.

1108 Kamto, S. 1169 f.

abzusehen.[1109] Dies wird auch explizit durch die im Naulilaa-Schiedsspruch umschriebene Voraussetzung einer unbefriedigten Nachfrage (»*unsatisfied demand*«) unterstrichen, gem. derer ein Staat nur als letztes Mittel unilateral reagieren bzw. er »das Gesetz nur als letztes Mittel selbst in die Hand nehmen« soll.[1110] Demgegenüber wurde jedoch auch schon die Ansicht vertreten, dass das Ergreifen von Gegenmassnahmen an sich ein wirksames Mittel konstituieren könne, um Verhandlungen überhaupt erst herbeizuführen oder eine friedliche Streitbeilegung zu fördern.[1111] Folglich bleibt im Einzelnen umstritten, ob der internationale Rechtsweg bzw. die vorhandenen Mittel einer friedlichen internationalen Streitbeilegung zuvor erschöpft werden müssen.[1112] Insgesamt kann man allerdings sagen, dass das Erfordernis einer vorgängigen Notifizierung und eines Verhandlungsersuchens, um den Verletzerstaat an seine Verantwortlichkeiten zu erinnern, von einer breiten Ansicht gestützt wird.[1113] Dieser Mechanismus kann dabei (im Vorfeld eines tatsächlichen Ergreifens von Gegenmassnahmen) an sich bereits politischen Druck aufsetzen, um einen Ausgleich herbeizuführen.[1114] Und dies – an dieser Stelle nochmals – ist letztlich der Zweck von Gegenmassnahmen.

Schliesslich müssen Gegenmassnahmen verhältnismässig sein, um gerechtfertigt zu sein. Dieses Erfordernis verlangt angesichts der Schwerpunktsetzung dieser Dissertation eine nähere Betrachtung, womit es nachfolgend eingehender analysiert werden soll.

1109 Franck, Recourse to Force, S. 111. Ferner: Schachter, International Law, S. 184.

1110 Naulilaa-Schiedsspruch (1928), S. 1011; Wicker, S. 72.

1111 Dazu: Schachter, International Law, S. 188; Wicker, S. 72 u.a. m.V.a. den Luftverkehrs-Schiedsspruch (1978), §80, §84 ff. Näher zu den Haltungen der USA und Frankreichs im Luftverkehrs-Schiedsspruch: Leben, S. 25.

1112 So zum Beispiel, indem die Angelegenheit vor ein internationales Gericht gebracht wird: Vgl. Art. 52 Abs. 3 ARSIWA; Peters/Petrig, S. 399. Dazu auch: O'Connell, Power and Purpose, S. 258 ff.; Sreenivasa, S. 863 ff.

1113 Ähnlich und ausführlicher hierzu: Schachter, Dispute Settlement and Countermeasures, S. 471 ff. (mit substanziellen Verweisen auf die Diskussionen in der internationalen Völkerrechtskommission und der UN-Generalversammlung).

1114 Kamto, S. 1171. Ihm zufolge sollen für die Würdigung einer vernünftigen Zeitspanne von Verhandlungsersuchen im Einzelfall die betreffenden Umstände wie die Haltung des verantwortlich gemachten Staates, die Dringlichkeit sowie die Wahrscheinlichkeit eintreffender Schädigungen im Falle eines Zuwartens eine Rolle spielen.

1. Grundidee der Verhältnismässigkeit bei Gegenmassnahmen

Alle Arten von Gegenmassnahmen müssen gem. Art. 51 ARSIWA verhältnismässig sein.[1115] Das Erfordernis der Verhältnismässigkeit im Gegenmassnahmenrecht ist durch die völkerrechtliche Staatenpraxis, Doktrin und Rechtsprechung grundsätzlich anerkannt[1116] und stellt ein Schlüsselelement dar, um die Legalität einer Gegenmassahme zu beurteilen. Denn wie bereits einleitend angeführt, kann eine unverhältnismässige Gegenmassahme ihrerseits zur Verantwortlichkeit führen.[1117] Die konkrete Anwendung der Verhältnismässigkeit bleibt insgesamt auch im Zusammenhang mit Gegenmassnahmen komplex und ist weiterhin Gegenstand von Debatten in Praxis und Lehre.[1118] Generell besteht zwar Einigkeit, dass jede Gegenmassnahme eine gewisse Gleichwertigkeit (»*must have some degree of equivalence*«) mit der Verletzung haben muss.[1119] Im Einzelnen bleibt es jedoch schwierig, die jeweiligen Grenzen für die (Un-)Verhältnismässigkeit zu definieren.[1120]

a. Quantitative und qualitative Faktoren

Trotz Vagheit und inhärenter Flexibilität des Prinzips haben sich mit fortschreitendem Diskurs Kriterien etabliert, anhand derer die Verhältnismässigkeit von Gegenmassnahmen gewürdigt werden soll.[1121] Gemäss Art. 51 ARSIWA müssen im Rahmen der Verhältnismässigkeit die Schwere der Verletzung

1115 O'Keefe, S. 1157. Franck, Proportionality, S. 719. Siehe dazu auch den Bericht der Völkerrechtskommission zur 44. Session 1992 (UN Doc. A/47/10 (1992)), S. 70 §208.

1116 Siehe z.B. Naulilaa-Schiedsspruch (1928), S. 1011 ff.; Luftverkehrs-Schiedsspruch (1978), §83; IGH, Nicaragua-Urteil, §249. Siehe auch IGH, Gabčíkovo-Nagymaros-Urteil, §85; ARSIWA-Kommentar, Art. 51(2); Wicker, S. 77 f. m.V. auf die wiederholte Bestätigung des Prinzips während des Kodifizierungsprozesses der ARSIWA 2001. Dazu u.a. auch: O'Connell, Power and Purpose, S. 252 ff.

1117 ARSIWA-Kommentar, Art. 51(1); Crawford, State Responsibility, S. 698; Wicker, S. 78.

1118 Wicker, S. 80.

1119 Luftverkehrs-Schiedsspruch (1978), §83.

1120 O'Keefe, S. 1165; Wicker, S. 77. Siehe auch: Naulilaa-Schiedsspruch (1928), S. 1028 ff., der zwar festhält, dass Gegenmassnahmen nicht »exzessiv« und »absolut disproportional« sein dürfen, allerdings nicht im Einzelnen anführt, welche Handlungen *in abstracto* unter welchen Bedingungen exzessiv oder absolut disproportional sind. Ähnlich wurde im späteren Luftverkehrs-Schiedsspruch festgehalten, dass eine solche Abwägung »bestenfalls durch Annäherung« erreicht werden könne: Luftverkehrs-Schiedsspruch (1978), §83. Dazu auch: Crawford, Third Report, S. 83 §308 f.

1121 Wicker, S. 86.

(quantitative Faktoren) sowie die betroffenen Rechte (qualitative Faktoren) berücksichtigt werden.[1122] Für diese Abwägung sind dabei jeweils die *Effekte* der Völkerrechtsverletzung sowie der Gegenmassnahme zu messen.[1123] So verweist auch der IGH im Gabčíkovo-Nagymaros-Urteil darauf, dass die Effekte einer Gegenmassnahme unter Würdigung der betroffenen Rechte im Hinblick auf die ursprüngliche Verletzung angemessen (»*commensurate*«) sein müssen.[1124] Die qualitative Würdigung der betroffenen Rechte erlaubt es dabei, auch nicht direkt quantitativ messbare Güter (wie z.B. Menschenrechtsverletzungen oder immaterielle Schäden) abzuwägen.[1125] Der herrschenden Meinung zufolge braucht zudem keine sachliche Konnexität zwischen der Natur der Verletzung und den Gegenmassnahmen vorzuliegen.[1126] Die Verhältnismässigkeit erlaubt es daher – wie es in der Praxis oft der Fall ist –, dass zwei unterschiedliche Elemente gegenübergestellt werden.[1127] Im Vordergrund steht also vielmehr eine gesamthafte Interessenabwägung statt eine rein quantitative Gegenüberstellung von Massnahme und Gegenmassnahme.[1128] In bestimmten Fällen könnte eine strikt quantitative Gleichartigkeit oder Reziprozität sogar unangemessen sein, wenn sich unterschiedliche Rechtsgüter gegenüberstehen.[1129] Somit erlaubt die Berücksichtigung von quantitativen *und* qualitativen Aspekten eine situationsgerechte Würdigung der konkreten Umstände, der involvierten Rechtsgüter und deren Mass.[1130]

1122 Cannizzaro, Countermeasures, S. 889; O'Keefe, S. 1165. Diese beiden Elemente hatte 1980 bereits der damalige Sonderberichtserstatter Riphagen im Rahmen der Völkerrechtskommission vorgebracht: Riphagen, Preliminary Report, S. 113 §34, S. 128 §94 f.; Riphagen, Fourth Report, S. 15 §80. Dazu auch: Sreenivasa, S. 873.

1123 Luftverkehrs-Schiedsspruch (1978), §83. ARSIWA-Kommentar, Art. 51(1), (6); Crawford, State Responsibility, S. 698; O'Keefe, S. 1158, S. 1161. Gemäss dem Sonderberichtserstatter Arangio-Ruiz spielen auch Aspekte des Verschuldens (*dolus* und *culpa* in einem engen Sinn) eine Rolle, siehe: Arangio-Ruiz, S. 2 f. m.w.V.

1124 IGH, Gabčíkovo-Nagymaros-Urteil, §85, §87.

1125 Wicker, S. 87.

1126 Peters/Petrig, S. 399.

1127 Wicker, S. 85 f.; Zoller, S. 131.

1128 Wicker, S. 98. Dazu auch: Sreenivasa, S. 874.

1129 Zu einem diesbezüglichen Beispiel anhand des Teheraner Geiselfalls: Schachter, International Law, S. 191; Wicker, S. 84.

1130 Ausführlicher dazu: O'Keefe, S. 1160 ff.; ARSIWA-Kommentar, Art. 51(6).

b. Interne und externe Verhältnismässigkeit

Gegenmassnahmen sollen, wie bereits erwähnt, den Verletzerstaat dazu bewegen, das völkerrechswidrige Verhalten einzustellen, den *status quo ante* wiederherzustellen und/oder Entschädigung zu leisten.[1131] Ausschliesslich zulässig ist bei Gegenmassnahmen daher das Ziel der Wiederherstellung der völkerrechtsmässigen Lage.[1132] In dieser Hinsicht muss die Gegenmassnahme notwendig sein, den Verletzerstaat zur Wiederherstellung der Völkerrechtsmässigkeit zu bewegen.[1133]

Gemäss WICKER ist für die Beurteilung der Verhältnismässigkeit die Abwägung zwischen Gegenmassnahme und ihrem Ziel wichtig, allerdings nicht ausreichend differenziert.[1134] Er ist der Ansicht, dass im Einzelfall das Ziel an sich und nicht nur die Gegenmassnahme variieren und dadurch unverhältnismässig sein könne. So greife bspw. ein Staat, der auf die Beendigung einer Verletzung abziele, unter Umständen zu anderen Massnahmen als ein Staat, der auf eine Entschädigung oder auf den Selbstschutz abziele. Folglich könnten verschiedene Ziele zu verschiedenen Massnahmen führen, was wiederum eine unterschiedliche Würdigung der Verhältnismässigkeit impliziere.[1135] Zudem gibt es eine Vielzahl an möglichen Mitteln und Instrumenten, um die »Wiederherstellung der völkerrechtsmässigen Lage« durchzusetzen.[1136] Demnach seien Gegenmassnahmen der Natur nach multifunktional und müssen im jeweiligen Kontext verstanden werden.[1137] Vor ebendiesem Hintergrund führte CANNIZZARO die Unterscheidung zwischen »interner« und »externer« Verhältnismässigkeit ein.[1138] Die externe Verhältnismässigkeit bezieht sich auf die Angemessenheit des beabsichtigten Ziels einer Gegenmassnahme. Die Idee ist, dass das Ziel, die völkerrechtskonforme Situation wiederherzustellen, der Situation entsprechend angemessen sein muss. Die interne Verhältnismässig-

1131 WICKER, S. 94.

1132 PETERS/PETRIG, S. 399. Siehe ferner: O'KEEFE, S. 1158.

1133 ARSIWA-Kommentar, Art. 51(1), (7); CRAWFORD, State Responsibility, S. 699; O'KEEFE, S. 1158 f.

1134 WICKER, S. 97.

1135 WICKER, S. 97.

1136 CANNIZZARO, Countermeasures, S. 895; WICKER, S. 99.

1137 CANNIZZARO, Countermeasures, S. 895; WICKER, S. 99.

1138 CANNIZZARO, Countermeasures, S. 894 ff. Ähnlich: ZOLLER, S. 135. CANNIZZARO schlug zudem einen Ansatz vor, wonach jede im Rahmen einer Gegenmassnahme individuell getroffene Massnahme isoliert betrachtet werden müsse. Demnach solle jede einzelne Funktion des jeweiligen Mittels vor dem Verhältnismässigkeitsprinzip gewürdigt werden: CANNIZZARO, Countermeasures, S. 895 f. Kritisch dazu: WICKER, S. 100.

keit soll hingegen überprüfen, ob die getroffene Massnahme oder das Mittel *zur Erreichung* dieses Ziels angemessen ist. Ziel und Mittel müssen in einem »angemessenen« Verhältnis stehen.[1139] Somit muss in einem ersten Schritt geprüft werden, ob das Ziel an sich verhältnismässig ist, und in einem zweiten, ob die Mittel dazu verhältnismässig sind.[1140] WICKER hat aufgrund ebendieser massgeblichen Unterscheidung einen neuen Wortlaut für Art. 51 ARSIWA vorgeschlagen: »*The purpose of the countermeasure must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question, and the measures resorted to by the injured State must be proportionate to that objective.*«[1141] Je konkreter eine Formulierung des Verhältnismässigkeitserfordernis, desto eher kann der betreffende Ermessenspielraum eingeschränkt werden.[1142] Dieser Vorschlag fügt der vorliegenden Ansicht nach daher eine sinnvolle objektive Komponente zum inhärenten Ermessensspielraum der Verhältnismässigkeit hinzu. Zugleich bliebe der Wortlaut genügend flexibel, um eine (intern und extern) verhältnismässige Gegenmassnahme zur Wiederherstellung der völkerrechtskonformen Lage zu erlauben.

c. Zwischenfazit: Die Verhältnismässigkeit als flexibles Prinzip

Insgesamt lässt sich festhalten, dass sich die Verhältnismässigkeit im Gegenmassnahmenrecht primär am Ziel orientiert, die Völkerrechtskonformität wiederherzustellen. Im Einzelnen kann die Verhältnismässigkeit allerdings weder im Zusammenhang mit dem Selbstverteidigungsrecht nach Art. 51 UN-Charta noch bei Gegenmassnahmen präzise festgelegt werden. In beiden Bereichen verbleibt ein (unter Umständen folgeschwerer) subjektiver Spielraum. Die im Kontext von Gegenmassnahmen abzuwägenden quantitativen und qualitativen Faktoren können für Staaten von unterschiedlicher Bedeutung sein, da die Wichtigkeit betroffener Rechte und damit auch deren Beeinträchtigung immer subjektiv geprägt sein wird.[1143] Ebenso wird die Verhältnismässigkeit des jeweiligen Ziels einer Gegenmassnahme bis zu einem bestimmten Grad Gegenstand

1139 IGH, Gabčíkovo-Nagymaros-Urteil, §85.

1140 WICKER, S. 101.

1141 WICKER, S. 103 f.

1142 Ähnlich i.Z.m. negativen oder positiven Formulierungen: ARSIWA-Kommentar, Art. 51(5).

1143 O'KEEFE, S. 1165.

der jeweiligen subjektiven Begründung bleiben.[1144] Dazu kommt gerade in militärischen und sicherheitspolitischen Belangen, dass die betroffenen Rechte und deren Intensität meist auch unter Entscheidungsträgern durch sehr spezifische und subjektive Perspektiven beurteilt werden. Militäroffiziere bspw. könnten unter Umständen eine andere Auffassung von der Verhältnismässigkeit einer Massnahme haben als Vertreter einer diplomatischen Abteilung.[1145]

Um das Verhalten von Staaten trotz inhärentem Spielraum regulieren zu können ist es dennoch wichtig, auf das Verhältnismässigkeitsprinzip zurückzugreifen. Die Verhältnismässigkeit ist entscheidend, um im dezentralen System des Völkerrechts unilaterale Reaktionen auf völkerrechtswidrige Handlungen rechtlich überprüfen zu können. Das Prinzip kann zentral sein, um die Machtausübung einzelner Staaten zu würdigen und zu beschränken.[1146] Für den normativen Wert des Prinzips kommt es zunächst auf die Akzeptanz der Adressaten an, das Prinzip ernst zu nehmen und diesem zu folgen.[1147] Zudem können konkrete Anwendungsfälle in Konflikten als normative Präzedenzfälle gelten.[1148] Indem das in Art. 51 ARSIWA ausformulierte Verhältnismässigkeitsprinzip in Lehre, Rechtsprechung und Staatenpraxis anerkannt ist, kann es als grundsätzlich respektierte Norm betrachtet werden. Dabei haben sich im Laufe der Zeit zunehmend objektive Kriterien etabliert, die innerhalb des Ermessensspielraums als Orientierung dienen und zu einer gewissen Voraussehbarkeit beitragen können. Die Verhältnismässigkeit *hat* somit eine Bedeutung im Hinblick auf die (immerhin vage) Voraussehbarkeit einer Antwort und der möglichen Sanktionen.[1149] Die Auseinandersetzung mit dem Prinzip widerspiegelt, dass die Verhältnismässigkeit – trotz Flexibilität im Einzelnen – eine praktische Bedeutung für staatliches Verhalten in internationalen Beziehungen behält.[1150] Indem Staaten ihr Verhalten anhand des Prinzips rechtfertigen und es in Konflikten thematisieren, wird das Prinzip implizit bestätigt. Inhaltlich stellt es im Kontext von Gegenmassnahmen des Weiteren eine funktionale Verbindung zwischen dem legitimen Ziel von Selbsthilfemassnahmen und den (zu jener Erreichung angemessenen) Mitteln her.[1151] Der Wortlaut von Art. 51

1144 Ähnlich umschreiben Newton/May das Verhältnismässigkeitsprinzip als ein inhärent subjektives Konzept: Newton/May, S. 29.

1145 Newton/May, S. 29.

1146 Vgl. Cannizzaro, Countermeasures, S. 890, S. 915.

1147 Franck, Proportionality, S. 717.

1148 Franck, Proportionality, S. 717.

1149 Cannizzaro, Countermeasures, S. 890.

1150 Crawford, State Responsibility, S. 698; Franck, Proportionality, S. 717 f.

1151 Cannizzaro, Countermeasures, S. 915; Crawford, State Responsibility, S. 698.

ARSIWA schafft insgesamt einen rechtlichen Rahmen, der Gegenmassnahmen als Reaktion auf internationales Fehlverhalten ermöglicht und zugleich angemessene Bedingungen schafft, diese innerhalb objektiv-rechtlicher Grenzen zu halten. Die in Lehre und Rechtsprechung etablierten Kriterien sowie der seitens WICKER vorgeschlagene Wortlaut, der die interne und externe Verhältnismässigkeit einschliesst, sind angesichts dessen, dass sie eine zusätzliche Objektivität einführen, zu begrüssen.

Insgesamt bleiben im Gegenmassnahmenrecht, gerade auch verglichen mit Sanktionen im innerstaatlichen Recht, für den Sanktionierenden relativ grosse Spielräume bestehen.[1152] Weder die Art noch die exakte Intensität der Gegenmassnahme stehen fest. Die Aussicht auf eine Gegenmassnahme impliziert für den Verletzer somit zusätzliche Unsicherheiten im Hinblick auf die Folgen seines Verhaltens.[1153] Diese Diffusität der Sanktion – und dies spricht *für* einen gewissen Spielraum – kann ihrerseits einen Anreiz für die Beachtung des Völkerrechts schaffen.[1154] Darüber hinaus können die unklaren Grenzen erlaubter Gegenmassnahmen angesichts eines möglichen Eskalationspotenzials auch für den Sanktionierenden selbst Anreize schaffen, wenn immer nur möglich, milde Selbsthilfemassnahmen zu wählen.

1152 DIGGELMANN, Völkerrecht, S. 159.

1153 DIGGELMANN, Völkerrecht, S. 159.

1154 DIGGELMANN, Völkerrecht, S. 159.

2. Verhältnismässige Gegenmassnahmen gegen Cyberangriffe?

Das Verhältnismässigkeitsprinzip ist auch in Bezug auf Gegenmassnahmen im Cyberkontext relevant.[1155] Analog zum traditionellen Kontext sollen Gegenmassnahmen dem ausschliesslich zulässigen Ziel der Wiederherstellung der Völkerrechtskonformität dienen.[1156] Daher dürfen sie auch im Cyberkontext nicht zur Bestrafung eingesetzt werden.[1157] Um die Verhältnismässigkeit zu beurteilen, sollen ebenso die Schwere der Völkerrechtsverletzung (quantitative Faktoren) sowie die betroffenen Rechte (qualitative Faktoren) gewürdigt werden.[1158] Massgeblich ist jeweils der Gesamtkontext.[1159] Handelt es sich um eine Reihe mehrerer Angriffe, so ist grundsätzlich auf den Gesamteffekt abzustellen.[1160] Für den Cyberkontext nennenswert ist, wie bereits unter III.A.4. erwähnt, dass Gegenmassnahmen nicht zwingend an einem (physischen) Schaden, sondern an der Verletzung einer jeweiligen Norm gemessen werden.[1161] Es kann dabei bei durch Cyberangriffe ausgelösten Verletzungen schwierig sein, die Form einer Wiedergutmachung oder einer Entschädigung festzulegen.[1162] Die Würdigung quantitativer und qualitativer Aspekte erlaubt es jedoch grundsätzlich, dass auch immaterielle, nicht zwingend physisch oder monetär bezifferbare Cyberangriffe mit einer Gegenmassnahme abgewogen werden können.

1155 Das Tallinn Manual 2.0 statuiert in R23, dass Gegenmassnahmen – ob digitaler oder nicht digitaler Natur – gem. Art. 51 ARSIWA verhältnismässig sein müssen: Tallinn Manual 2.0, S. 127 R23 C1; Schmitt/Pitts, S. 3.

1156 Siehe u.a. Hathaway et al., S. 857 ff.; Schmitt/Pitts, S. 3; Schmitt, Countermeasures Response Option, S. 714 f.

1157 Schmitt/Pitts, S. 3; Schmitt, Countermeasures Response Option, S. 714.

1158 Vgl. Jensen, Critical National Infrastructure, S. 220 f.; Roscini, Cyber Operations, S. 106; Sklerov, S. 37 m.V.a. IGH, Gabčíkovo-Nagymaros-Urteil, §85.

1159 Diggelmann/Hadorn, S. 268.

1160 Diggelmann/Hadorn, S. 268.

1161 ARSIWA-Kommentar, Art. 2(9); Schulze, S. 66.

1162 Vgl. Delerue, Reinterpretation or Contestation, S. 323. Er verweist auf die Schwierigkeit, die Intensität eines Cyberangriffs zu eruieren sowie auf die damit verbundene Schwierigkeit, eine verhältnismässige Reaktion festzulegen.

a. Digitale Gegenmassnahmen als Retorsion?

Gemäss Tallinn Manual 2.0 soll im Rahmen der Staatenverantwortlichkeit grundsätzlich mit digitalen und nicht-digitalen Gegenmassnahmen auf eine Völkerrechtsverletzung reagiert werden können.[1163] Friedliche Gegenmassnahmen oder Retorsionshandlungen stellen dabei jeweils die verhältnismässigsten Selbsthilfeoptionen dar.[1164] Das Tallinn Manual führt dabei nicht weiter aus, was im Einzelnen »friedlich« ist und wie digitale Gegenmassnahmen vor dem Hintergrund der Verhältnismässigkeit zu würdigen sind.

Einige Autoren – und dies ist vorliegend näher zu betrachten – sehen digitale Gegenmassnahmen als eine friedliche Möglichkeit, auf Völkerrechtsverletzungen zu reagieren bzw. teilweise sogar als völkerrechtlich zulässige Retorsion.[1165] Einer solchen Lesart nach werden Cybergegenmassnahmen folglich als eine effiziente Form der Selbsthilfe gesehen, um sich gegen Cyberangriffe eines anderen Staates zu wehren.[1166] Einigen Ansichten zufolge sind dabei auch aktive Massnahmen wie Hackbacks völkerrechtlich nicht zu rechtfertigen, da sie ohne Zwangselement keine Völkerrechtsverletzung darstellten.[1167] Unter Umständen seien folglich auch aktive Cybergegenmassnahmen als gewaltlose Gegenmassnahmen zu verstehen.[1168] Da bei aktiven digitalen Gegenmassnahmen wie Hackbacks allerdings unvorhergesehene und gegebenenfalls physische Effekte ausgelöst werden können, wird vorliegend die Ansicht vertreten, dass Hackbacks und weitere digitale Gegenmassnahmen, die in fremde

1163 Tallinn Manual 2.0, S. 128 R23 C7.

1164 Tallinn Manual 2.0, S. 128 R23 C7.

1165 Siehe Diggelmann/Hadorn, S. 269, die das vorübergehende Blockieren von bestimmten Servern aus dem Angreiferstaat als Retorsion qualifizieren, da kein Staat völkerrechtlich verpflichtet sei, die Erreichbarkeit von Servern sicherzustellen. Dies kann allerdings nur angenommen werden, wenn die Blockierung der Server strikt im eigenen Territorium stattfindet und dadurch keine bestehenden Verträge oder Völkergewohnheitsrecht verletzt werden: Lotrionte, S. 92; Schmitt, Countermeasures Response Option, S. 701 f. Ähnlich umschreiben Newton/May, S. 280 Cybergegenmassnahmen als völkerrechtskonforme Retorsion. Ferner dazu: Halberstam, S. 213 ff.

1166 Vgl. Delerue, Reinterpretation or Contestation, S. 323.

1167 So ist z.B. die UK der Ansicht, dass Hackbacks keine Souveränitätsverletzungen darstellen, da dies keine alleinstehende Völkerrechtsnorm sei: Wright, Rede vom 23.05.2018.

1168 Harrison Dinniss, S. 107 f.; Hathaway, Active Defense, S. 50. Vgl. Sklerov, S. 37, der darauf verweist, dass auch »beschränkte« Cyberangriffe als Gegenmassnahme gegen Angreifer eingesetzt werden können sollen. Ähnlich hält Wingfield daran fest, dass Staaten Gewalt anwenden können müssen, um Aggressionen abzuschrecken. Demzufolge seien digitale Gewaltanwendungen nicht per se ausgeschlossen: Wingfield, S. 361 f.

Systeme eingreifen, auf jeden Fall völkerrechtlich gerechtfertigt sein müssen.[1169] Aktive Cybergegenmassnahmen können nämlich, wie vorangehend unter IV.A.2. erläutert, Konsequenzen haben, deren Ausmass und Auswirkungen einer unzulässigen Intervention oder einer Gewaltanwendung gem. Art. 2(4) UN-Charta gleichkommen. Damit würden sie über ledigliche Retorsionshandlungen hinausgehen – bspw. wenn durch eine digitale Gegenmassnahme zufällig ein Kontrollystem oder ein Server eines Krankenhauses blockiert wird.[1170] So könnte auch ein lediglich vorübergehendes Blockieren von bestimmten Servern im Angreiferstaat unter Umständen unvorhergesehene Schädigungen auslösen.

Die Expertengruppe im Tallinn Manual 2.0 ging indes sogar so weit, die Frage offen zu lassen, ob *gewaltsame* digitale und/oder herkömmliche Gegenmassnahmen auf Völkerrechtsverletzungen im Rahmen der Staatenverantwortung zulässig sein sollten, solange sie nicht die Schwelle eines bewaffneten Angriffs gem. Art. 51 UN-Charta erreichten. Die Minderheit der Experten im Tallinn Manual bejaht dies, indem sie gewaltsame Gegenmassnahmen als angemessene Reaktion auf Cyberangriffe betrachtet.[1171] Sie stützen sich bei dieser extensiven Ansicht auf die richterliche Mindermeinung von Richter Simma im Ölplattformen-Urteil.[1172] Insgesamt anerkannte die Expertengruppe allerdings dennoch, dass reagierende Staaten ehebliche Sorgfalt walten lassen müssten, um sich nicht selbst völkerrechtlich verantwortlich zu machen.[1173] Aufgrund der Uneinigkeit zwischen den Experten wurde die Frage nach gewaltsamen Gegenmassnahmen im Ergebnis zumindest nicht ausgeschlossen.[1174] Mit einem dahingehenden Verständnis würde man sich allerdings vom grundsätzlich rechtlich Zulässigen entfernen: Denn wie bereits unter III.B.1. abgehandelt, ist *gewaltsame* Verteidigung *nur* ausnahmsweise im Falle eines bewaffneten Angriffs nach Art 51 UN-Charta erlaubt. Das im Völkerrecht widerspiegelte Bestreben, dezentrale Gewaltanwendungen so weit als möglich zu beschränken,

1169 Ebenso: LAHMANN, S. 128.

1170 BAUMGÄRTNER et al., Der Spiegel vom 24.11.2017; LAHMANN, S. 128.

1171 Tallinn Manual 2.0, S. 125 R22 C12.

1172 IGH, Ölplattformen-Urteil, (separate Meinung Richter Simma), §13. Simma gewichtete in seiner separaten Meinung durch sein extensiveres Verständnis von Gewaltanwendung ferner die Prinzipien der Verhältnismässig- und Notwendigkeit im Ergebnis stark.

1173 Unter Tallinn Manual 2.0, S. 128 R23 C6 verweisen die Experten darauf, dass Staaten erhebliche Sorgfalt walten lassen müssen, wenn sie die Verhältnismässigkeit ihrer Gegenmassnahmen würdigen. Dies impliziere gewisse Vorkehrungen. Ob die Würdigung adäquat sei, hänge mitunter von der Voraussehbarkeit potenzieller Konsequenzen ab.

1174 Tallinn Manual 2.0, S. 125 R22 C9 f.

würde daher im Widerspruch zu gewaltsamen Gegenmassnahmen stehen.[1175] Das Gewaltverbot zählt gem. IGH[1176] sowie auch laut Wortlaut von Art. 50(1)(a) ARSIWA sogar explizit zu den sanktionsfesten Normen.[1177] Das Tallinn Manual gibt in dieser Hinsicht somit weniger die *lex lata* wieder, sondern bewegt sich mit diesen Ausführungen vielmehr in Richtung einer extensiven *lex ferenda*.[1178] Zudem bleibt es zu erinnern, dass man sich im Kontext völkerrechtlicher Gegenmassnahmen – anders als im Kontext von Art. 51 UN-Charta – im Bereich *nicht-militärischer* Möglichkeiten bewegt. Es bleibt nach vorliegend vertretener Ansicht somit fraglich, ob digitale staatliche Massnahmen *überhaupt* als völkerrechtlich erlaubte (nicht-militärische) Gegenmassnahmen in Frage kommen. Im Rahmen nicht-militärischer Gegenmassnahmen könnten sie nämlich nur gerechtfertigt sein, solange sie mit Sicherheit keine für das Gewaltverbot relevanten Schädigungen auslösen und den weiteren Verhältnismässigkeitaspekten genügen.[1179] Aufgrund der globalen Vernetzung und Interdependenzen von Computersystemen ist es jedoch *de facto* sehr schwierig, die von Cybergegenmassnahmen ausgehenden Konsequenzen und Effekte im Voraus absehen zu können.[1180]

Neben der Gefahr, dass aktive Cybergegenmassnahmen für eine Gewaltanwendung gem. Art. 2(4) UN-Charta relevante Effekte auslösen, besteht auch das bereits erwähnte Risiko, dass sich ein als Gegenmassnahme eingesetztes Schadprogramm unkontrolliert weiterverbreitet[1181] und dadurch Computer und Server von unbeteiligten Drittparteien trifft.[1182] Obschon Gegenmassnahmen zwar grundsätzlich nur auf den für die Völkerrechtsverletzung verantwortlichen Staat gerichtet werden dürfen, der seinen Beendigungs- oder Entschädigungspflichten nicht nachgekommen ist[1183], schliesst eine Beeinträchtigung von Drittstaaten die Rechtmässigkeit einer Gegenmassnahme

1175 Schröder, S. 729; Schulze, S. 70. Ähnlich verweist Dörr, S. 641 f. auf die Wiedergutmachungsfunktion der Staatenverantwortlichkeit.

1176 IGH, Korfu Kanal-Urteil, S. 35; IGH, Nicaragua-Urteil, §249.

1177 So letztlich auch die Mehrheit der Experten im Tallinn Manual: Tallinn Manual 2.0, S. 125 R22 C11.

1178 Vgl. Lotrionte, S. 93.

1179 Ähnlich: Lahmann, S. 130; Roscini, Cyber Operations, S. 106.

1180 Dies erkennen trotz der teilweise extensiven Ansichten auch die Experten im Tallinn Manual: Tallinn Manual 2.0, S. 128 R23 C6.

1181 Lahmann, S. 131; Roscini, World Wide Warfare, S. 114.

1182 Hathaway et al., S. 859.

1183 ARSIWA-Kommentar, Art. 49(4). Dazu auch: Schmitt/Pitts, S. 6 ff. m.V.a. den Bericht der Völkerrechtskommission zur 44. Session 1992 (Doc. A/47/10 (1992)).

nicht kategorisch aus. Gemäss §5 zum Art. 49 der ARSIWA Kommentare darf eine Gegenmassnahme unter gewissen Umständen Drittparteien beeinflussen, da indirekte oder kollaterale Effekte (auch im traditionellen Kontext) nicht gänzlich vermieden werden können.[1184] Dies wäre bspw. der Fall, wenn durch die Suspendierung einer Handelsvereinbarung mit dem verantwortlichen Staat Unternehmen in einem Drittstaat bankrott gehen würden.[1185] Gemäss Lehre ist der reagierende Staat zwar jeweils verpflichtet, alles ihm Mögliche zu unternehmen, um die Beeinträchtigung Dritter zu vermeiden, oder, sollte eine Verletzung unvermeidlich sein, sicherzustellen, dass diese auf ein Minimum beschränkt wird.[1186] Allerdings bleibt es in diesem Zusammenhang fraglich, welches Mass an Sorgfalt im Einzelnen erforderlich ist.[1187] Aufgrund der unübersichtlichen Konstellationen im Cyberkontext ist davon auszugehen, dass aktive Cybergegenmassnahmen, die mit grosser Wahrscheinlichkeit die Beeinträchtigung von Drittstaaten oder -parteien implizieren, nicht gerechtfertigt sind.[1188] Das Gleiche sollte auch dann gelten, wenn (unbeabsichtigte) Beeinträchtigungen oder Schädigungen »vernünftigerweise absehbar« sind,[1189] wovon man im Cyberkontext in den meisten Szenarien wohl ausgehen muss.

b. Quantitative und qualitative Faktoren

Zur Würdigung der Gesamteffekte kommt bei aktiven Cybergegenmassnahmen schliesslich die Frage der quantitativen und qualitativen Verhältnismässigkeit hinzu. Und zwar grundsätzlich auch für den Fall, dass nur die Computersysteme des verantwortlichen Staates getroffen werden. Gemäss HINKLE gibt es keine Garantie dafür, dass reziproke Gegenmassnahmen (also die Beantwortung von Cyberangriffen mit Cybergegenmassnahmen) im Cyberkontext auch zu reziproken Effekten führen.[1190] So könnten bei aktiven Cyberge-

1184 ARSIWA-Kommentar, Art. 49(5); LAHMANN, S. 131; SCHMITT/PITTS, S. 7 ff.

1185 ARSIWA-Kommentar, Art. 49(5).

1186 ELAGAB, S. 113.

1187 LAHMANN, S. 131.

1188 LAHMANN, S. 131 m.V.a. HATHAWAY et al., S. 859; SCHMITT, Law of Countermeasures, S. 687 und Weitere. Dazu auch: SCHMITT/PITTS, S. 11 ff., insb. 20 f. (unter Verweis auf die anhaltenden Unklarheiten) muss ihnen zufolge jeder Staat, der Gegenmassnahmen in Betracht zieht, die folgenden Aspekte sorgfältig in Erwägung ziehen: 1) *wer* von den betreffenden Cybergegenmassnahmen betroffen sein wird; 2) *wie* die betreffende Partei betroffen sein wird; 3) ob der Effekt ein Interesse oder ein Recht tangiert; und 4) ob das Verbot einer Gegenmassnahme, die Rechte Dritter berührt, das betroffene Recht umfasst.

1189 LAHMANN, S. 131.

1190 HINKLE, S. 20; ROSCINI, Cyber Operations, S. 106.

genmassnahmen unter Umständen durch die Manipulierung oder Blockierung von Computersystemen verschiedene Rechte und eine unterschiedliche Anzahl von Computern tangiert werden. »Counter-DDoS«-Angriffe bspw. zielen darauf ab, schädigende Signale an die IP-Adresse(n) zurückzuschicken, von der sie kommen. Diese wiederum sind jedoch nicht zwangsläufig die Adressen des Kontrollservers, von dem die Angriffe gesteuert werden. Zudem gehen DDoS-Angriffe i.d.R., wie im Beispiel Estlands 2007, von vielen Computern gleichzeitig aus.[1191] Hätte man die Angriffe auf Estland mit sog. »Counter-DDoS«-Angriffen gegen die vielen in Russland befindlichen Server beantwortet (vorausgesetzt, dass Russland tatsächlich Urheber der Angriffe war und eine verbotene Intervention bejaht worden wäre), hätte dies zu unverhältnismässigen Konsequenzen führen können: Indem die Gegenmassnahmen vom vergleichsweise kleinen Computernetzwerk Estlands auf das um ein Vielfaches grössere russische Netzwerk lanciert worden wären, wären quantitativ wohl viel mehr Computer von einer Blockierung durch die Gegenangriffe betroffen gewesen.[1192] Allein durch die potenziell viel grössere Anzahl betroffener Computersysteme wären quantitativ mehr Schädigungen denkbar gewesen.[1193] Somit kann die Reaktion auf völkerrechtswidrige Cyberangriffe mit Cybergegenmassnahmen unter Umständen nicht die angestrebten verhältnismässigen, sondern oft auch unverhältnismässige Konsequenzen auslösen.[1194]

Darüber hinaus besteht in qualitativer Hinsicht auch die Schwierigkeit, bei Cybergegenmassnahmen abschliessend die *Art* der beeinträchtigten Interessen und Rechtsgüter vorauszusehen. Durch den digitalen Zugriff auf zivile Daten könnte bspw. der unter der Privatsphäre geschützte Bereich individueller Rechte verletzt werden. Zudem besteht das reale Risiko, dass mit einer aktiven Cybergegenmassnahme (unbeabsichtigt) Systeme von Infrastrukturen blockiert werden, die lebenserhaltende Funktionen oder Daten von sicherheitspolitischer oder nationaler Relevanz kontrollieren. Eine Beeinträchtigung solcher Rechte könnte unter Umständen einschneidender sein als die Hinnahme der ursprünglichen Völkerrechtsverletzung.[1195] Würde man aktive Cybergegenmassnahmen zusehends als (womöglich automatisierte) Standardreaktion festlegen, könnte ein weiterer möglicher Nebeneffekt sein, dass An-

1191 Dittrich/Himma, S. 664 ff.

1192 Hinkle, S. 20 ff.

1193 Hinkle, S. 21.

1194 Hinkle, S. 21.

1195 Caltagirone/Frincke, S. 263; Lahmann, S. 135.

greifer kritische Infrastrukturen als »Schutzschilder« nutzen könnten.[1196] Mit anderen Worten könnten Angreifer eine Motivation haben, absichtlich kritische Infrastrukturen als Brückenkopf für ihre Cyberangriffe zu missbrauchen. Dadurch könnten Gegenmassnahmen fundamentale Rechte der Zivilbevölkerung treffen[1197] und dabei – sollten Menschenrechte tangiert werden – auch gegen die sanktionsfeste Norm in Art. 50(1)(b) ARSIWA verstossen.[1198] Es bleibt fraglich, ob Cybergegenmassnahmen technisch so programmiert und eingesetzt werden können, dass sie sich mit Sicherheit nicht weiterverbreiten und/oder unbeabsichtigte Computersysteme treffen.[1199] Gemäss Hinkle ist es bei »Counter-DDoS«-Angriffen daher nicht möglich, das Risiko für zivile Infrastrukturen mit Sicherheit zu minimieren.[1200] Dies ist nach vorliegend vertretener Ansicht auch für weisse Computerwürmer oder weitere Schadprogramme anzunehmen.[1201]

Insgesamt sprechen die Gefahr einer (womöglich unverhältnismässigen) Beeinträchtigung Dritter sowie die quantitativ wie qualitativ nicht mit Sicherheit begrenzbaren Schäden eher dagegen, aktive Cybergegenmassnahmen im Rahmen der nicht-militärischen Selbsthilfe zu erlauben.[1202] Der hier vertretenen Ansicht nach handelt es sich bei Cybergegenmassnahmen zudem i.d.R. nicht – bzw. überwiegend nicht mit Sicherheit – um eine völkerrechtlich zulässige Retorsion. Hinzu kommt, dass aufgrund der potenziellen Weiterverbreitung und eines möglichen Blockierens von Servern kritischer Infrastrukturen nicht nur Drittparteien, sondern letztlich auch die Netzwerke und damit Interessen des die Gegenmassnahmen lancierenden Staates selber getroffen werden können.[1203] Angesichts dessen, dass Gegenmassnahmen der völkerrechtlichen Verhältnismässigkeit genügen müssen, sind aktive digitale Mittel daher jeweils (auch im Hinblick auf eigene Sorgfaltspflichten) sehr kritisch zu hinterfragen, sollte ein Staat diese im Einzelfall in Erwägung ziehen.

1196 Caltagirone/Frincke, S. 263. Ähnlich: Dittrich/Himma, S. 677. Mit einem ähnlichen Bsp.: Baumgärtner et al., Der Spiegel vom 24.11.2017.

1197 Geiss/Lahmann, S. 642.

1198 Roscini, Cyber Operations, S. 106. Zum Verbot, als Gegenmassnahme Gewalt anzuwenden auch: Crawford, Brownlie's Principles, S. 573; Sreenivasa, S. 869 ff. m.w.V.

1199 Lahmann, S. 134. Ähnlich: Schmitt, Law of Countermeasures, S. 684.

1200 Hinkle, S. 21.

1201 Ähnlich: Dewar, Active Cyber Defense, S. 7. Ihm zufolge kann dieses Risiko allerdings bei einer Kombination mit passiven Verteidigungsmitteln minimiert werden: Dewar, Triptych of Cyber Security, S. 7 ff.

1202 Vgl. Dittrich/Himma, S. 679; Lahmann, S. 137.

1203 Dittrich/Himma, S. 679.

c. Wiederherstellung der Völkerrechtskonformität

Die Experten des Tallinn Manuals 2.0 bestätigen, dass Gegenmassnahmen darauf ausgerichtet sein müssen, den Verletzer zur Einstellung des völkerrechtswidrigen Verhaltens oder zur Entschädigung zu bewegen.[1204] Gegenmassnahmen dürfen daher auch im Cyberkontext nicht zur Bestrafung eingesetzt werden.[1205] Analog zum herkömmlichen Kontext gelten der vorliegenden Ansicht nach zudem auch im Cyberkontext die Konzepte der externen und internen Verhältnismässigkeit,[1206] wonach das Ziel einer Gegenmassnahme an sich sowie auch die Massnahme zum Ziel verhältnismässig sein müssen.

Primär fragt sich also, ob digitale Gegenmassnahmen mittels Hackbacks oder »Counter-DDoS«-Angriffe den Verletzerstaat zur Einstellung des völkerrechtswidrigen Verhaltens bewegen können.[1207] In dieser Hinsicht ist zunächst daran zu erinnern, dass bei aktiven digitalen Gegenmassnahmen i.d.R. allerdings entweder die Neutralisierung[1208] eines Angriffs, die Informationsbeschaffung zu Investigationszwecken oder gem. DITTRICH/HIMMA auch teilweise pönalisierende Motive (die gem. Völkerrecht weder unter der Selbstverteidigung noch im Gegenmassnahmenrecht erlaubt sind) im Vordergrund stehen.[1209] Greift man mittels Hackbacks auf ein fremdes System zu, um dort ein Schadprogramm zu neutralisieren, gleicht dies dabei einer aktiven Abwehr eines Angriffs und weniger dem Entziehen eines Vorteils, anhand dessen ein Ausgleich oder eine Verhaltensänderung des Verletzerstaates herbeigeführt werden soll. Offensive Gegenmassnahmen werden des Weiteren gem. DITTRICH/HIMMA meist nicht so programmiert, einen Angriff zu beenden, sondern könnten häufig zu einer Eskalation des Angriffs führen.[1210] Ähnlich ist es im Zusammenhang mit »Counter-DDoS«-Angriffen fraglich, ob die zur Blockierung führende Überlastung von Ursprungssystemen aufgrund der aktiven

1204 Tallinn Manual 2.0, S. 128 R23 C4 m.V.a. ARSIWA-Kommentar, Art. 51(6); CRAWFORD, State Responsibility, S. 699.

1205 Zum Zweck von Gegenmassnahmen gem. Tallinn Manual: Tallinn Manual 2.0, S. 116 ff. R21, insb. S. 117 R21 C2 m.V.a. Luftverkehrs-Schiedsspruch (1978), §91.

1206 CANNIZZARO, Countermeasures, S. 894 ff.; WICKER, S. 101.

1207 Anderer Ansicht: HALBERSTAM, S. 201. Der Autorin zufolge sollen digitale Gegenmassnahmen unter Einhaltung der prozeduralen Voraussetzungen erlaubt sein, wenn der Staat vernünftigerweise davon ausgeht, dass die digitalen Massnahmen notwendig sind, um den Angreifer zur Beendigung seiner verletzenden Cyberangriffe zu bewegen.

1208 Siehe näher zu aktiver Cyberverteidigung zur Neutralisierung: OWENS et al., S. 15, S. 142 ff. unter dem Abschnitt »*Active Defense for Neutralization as a Partially Worked Example*«.

1209 DITTRICH/HIMMA, S. 665.

1210 DITTRICH/HIMMA, S. 677.

Komponente als ein »Entziehen von Vorteilen« des Gegenmassnahmenrechts gesehen werden kann. Dies gilt ebenso für den Einsatz weiterer *aktiver* digitaler Massnahmen. Ferner zielen »Honey Pots« und weitere der Informationsbeschaffung dienende Gegenmassnahmen wohl nicht darauf ab, einen Gegner zur Einstellung der Völkerrechtsverletzung oder zu Reparationsleistungen zu bewegen, da diese grundsätzlich anonym und ohne das Wissen des Letzteren erfolgen.

Das im Kontext der Verhältnismässigkeit ausschliesslich zulässige Ziel von Gegenmassnahmen, die Völkerrechtskonformität wiederherzustellen, impliziert des Weiteren, dass Gegenmassnahmen nur solange erlaubt sind wie eine Verletzung anhält.[1211] Somit müsste bei jeder Gegenmassnahme grundsätzlich sichergestellt werden, dass keine irreversiblen Schäden verursacht werden.[1212] Dies würde gem. LAHMANN aggressive digitale Gegenmassnahmen grundsätzlich ausschliessen, die denselben Schaden auslösen sollen wie der ursprüngliche Angriff oder ein Angreifersystem dahingehend beschädigen sollen, dass keine künftigen Angriffe lanciert werden können.[1213] Wenn solche Massnahmen allerdings für den Erfolg einer Gegenmassnahme unentbehrlich seien, sieht LAHMANN die Möglichkeit, dass diese durch das Gegenmassnahmenrecht gerechtfertigt sein könnten.[1214] Und zwar dann, wenn Angriffe dadurch gestoppt werden können und der die Gegenmassnahme lancierende Staat Vorkehrungen trifft, dass keine weiteren Schädigungen (auf dem betreffenden System oder anderweitig) entstehen.[1215] In diesem Zusammenhang fügt er das Beispiel an, dass im Falle von DDoS-Angriffen ein gezieltes Hacken eines Kontrollcomputers[1216] u.U. ein ganzes Netz kompromittierter Bots neutralisieren könne (vorausgesetzt, dass man den Kontrollcomputer während eines Angriffs

1211 LAHMANN, S. 136 m.V.a. CRAWFORD, Third Report, S. 88 §331.

1212 Vgl. ARSIWA-Kommentar, Art. 49(9). Irreversiblen Schädigungen könnten gegebenenfalls – und unter Einhaltung der *ius ad bellum*-Verhältnismässigkeit – vielmehr unter Art. 51 UN-Charta gerechtfertigt sein.

1213 Er verweist dabei auf aggressive digitale Gegenmassnahmen wie umschrieben von SKLEROV, S. 25 und DITTRICH/HIMMA, S. 679.

1214 LAHMANN, S. 136. Ähnlich sieht ROSCINI Cybergegenmassnahmen, die auf die Funktionsbeeinträchtigung von Infrastrukturen abzielen, ohne sie zu beschädigen, als nützliches Mittel: ROSCINI, Cyber Operations, S. 106.

1215 LAHMANN, S. 137. Klärungsbedürftig bleibt allerdings auch im vorliegenden Kontext das Mass an Sorgfaltspflichten im Hinblick auf die Vermeidung irreversibler Schädigungen.

1216 KESAN/HAYES, S. 475 sieht die das Zurücksenden von DoS-Angriffen auf das Botnetkontrollsystem sowie das Hacken desselben als zwei potenzielle Möglichkeiten, Angriffe zu neutralisieren.

findet). Ihm zufolge soll somit ausnahmsweise das permanente physische Zerstören des *einen* Kontrollsystems erlaubt sein, wenn kein anderweitiger Weg für die Neutralisierung eines Angriffs besteht.[1217] Vorliegend anzufügen ist, dass solche, auf eine Abwehr gerichteten Massnahmen nur ausnahmsweise vor dem Hintergrund *dringlicher* Massnahmen nach Art. 52(2) ARSIWA gerechtfertigt sein können, wenn diese notwendig sind, um die Rechte eines Staates sicherzustellen.[1218] In Bezug auf digitale Gegenmassnahmen mittels Schadprogrammen (insb. weissen Computerwürmern) besteht allerdings weiterhin das Problem, dass man die möglicherweise davon ausgehenden Schäden nicht in dem Sinne kontrolliert »beenden« kann, wenn diese sich unkontrolliert weiterverbreiten.[1219] Schadprogramme können sich, wie bereits aufgezeigt, von einem (Kontroll-)System aus grundsätzlich auf weitere Systeme verbreiten. Mitunter also auch in Konstellationen, in denen der betreffende Staat die Verletzung seinerseits bereits eingestellt und Entschädigungen geleistet hat. Hinzu kommt, dass je nachdem, was der durch Hackbacks zurückangegriffene oder blockierte Server kontrolliert, irreversible Folgeschäden entstehen könnten.[1220] So zum Beispiel, wenn durch die Blockierung von Spitalcomputern Menschen sterben.[1221] Obschon Sekundärverletzungen im Gegenmassnahmenrecht nicht kategorisch unzulässig sind,[1222] sprechen die unübersichtlichen Verhältnisse im Cyberraum und die potenziell (qualitativ und quantitativ) irreversiblen Sekundärverletzungen allerdings dafür, eine Inkaufnahme von Sekundärverletzungen sehr restriktiv zuzulassen. Dies würde somit im Ergebnis die Rechtmässigkeit der meisten digitalen Massnahmen im Kontext des Gegenmassnahmerechts ausschliessen.

1217 Lahmann, S. 137. Siehe: ARSIWA-Kommentar, Art. 49(9) mit dem Hinweis, dass die Reversibilität nicht absolut ist.

1218 ARSIWA-Kommentar, Art. 52(6).

1219 Der entgegengesetzten Auffassung, dass Cyber(gegen)angriffe in Umfang, Dauer und Effekten beschränkt werden können: Newton/May, S. 280.

1220 Lahmann, S. 136 handelt solche Folgeschäden als Sekundäverletzungen ab.

1221 Daneben, dass solche Verletzungen irreversibel sind, könnten in einem solchen Fall auch, wie bereits erwähnt, sanktionsfeste Normen (in diesem Falle Art. 50(1)(b) ARSIWA) verletzt werden.

1222 Lahmann, S. 136 m.V.a. Crawford, Third Report, S. 88 §330.

d. Vorgängige Notifizierung

Jede völkerrechtliche Gegenmassnahme erfordert grundsätzlich eine vorgängige Notifizierung – analog gilt dies daher auch, wenn ein Staat mit Gegenmassnahmen auf Cyberangriffe reagieren möchte. Der reagierende Staat muss den verantwortlichen Staat gem. Art. 51(1) ARSIWA zuerst notifizieren, ihm die Gelegenheit zur Beendigung des rechtswidrigen Zustandes geben sowie Verhandlungen anbieten.[1223] Allerdings vertritt eine Mindermeinung die Ansicht, dass eine Notifizierung die strategische Anonymität einer digitalen Gegenmassnahme untergräbt und im Cyberkontext daher nicht erforderlich sei.[1224] Die Experten im Tallinn Manual 2.0 gingen dabei so weit, dass sie es (im Rahmen von §6 der Kommentare zu Art. 52 ARSIWA) als nicht erforderlich sahen, die Gegenpartei über die Absicht, Gegenmassnahmen zu lancieren, zu informieren, wenn dies die Gegenmassnahme obsolet mache.[1225] Allerdings ist zu betonen, dass die in Art. 52(2) ARSIWA vorgesehene Ausnahme, von einer Notifizierung abzusehen, sich nur ausnahmsweise auf den Fall *dringlicher* Massnahmen bezieht.[1226] Von einer Notifizierung kann somit nur ausnahmsweise im Falle dringlicher Gegenmassnahmen abgesehen werden.[1227] Ansonsten muss der Gegenpartei daher grundsätzlich immer Gelegenheit zur Beendigung eines Angriffs gegeben werden.

Gegenmassnahmen müssen, wie vorangehend erwähnt, jeweils gegen den Angreiferstaat gerichten sein. Angesichts dessen, dass nichtstaatliche oder staatliche Angreifer regelmässig die IP-Adressen Dritter als Brückenkopf missbrau-

---

1223 Tallinn Manual 2.0, S. 120 R21 C10 m.V.a. Art. 52(1) ARSIWA; IGH, Gabčíkovo-Nagymaros-Urteil, §84; Luftverkehrs-Schiedsspruch (1978), §85 ff. Zur Notifizierung auch: Crawford, Brownlie's Principles, S. 573; O'Connell, Power and Purpose, S. 250 ff. Für den Cyberkontext auch: Schmitt, Countermeasures Response Option, S. 717.

1224 Die UK hat am 23.05.2018 kommuniziert, dass das Erfordernis einer vorangehenden Benachrichtigung nicht als völkerrechtliche Voraussetzung im Cyberkontext zu betrachten sei: Wright, Rede vom 23.05.2018. Ähnlich: Roscini, Cyber Operations, S. 106. Siehe dazu: Lahmann, S. 138 m.V.a. ARSIWA-Kommentar, Art. 52(5).

1225 Tallinn Manual 2.0, S. 120 R21 C12 (mit angeführtem Beispiel, dass eine Notifizierung u.U. dem Angreiferstaat Zeit verschaffen könnte, um eigene Vorkehrungen treffen zu können).

1226 Die Experten anerkennen zwar, dass Art. 52 ARSIWA sich auf dringliche Gegenmassnahmen bezieht, kamen jedoch dennoch zum Schluss, dass die Ausnahme in analoger Weise auf alle Gegenmassnahmen im Cyberkontext Anwendung finden solle: Tallinn Manual 2.0, S. 120 R21 C12 unter Fn. 241.

1227 Tallinn Manual 2.0, S. 120 R21 C11 m.V.a. Art. 52(2) ARSIWA.

chen,[1228] räumt eine vorzeitige Notifizierung einem Staat die Möglichkeit ein, selbst tätig zu werden. So könnte er bspw. Massnahmen einleiten, um die von seinem Territorium ausgehenden Schädigungen zu unterbinden, die betreffenden IP-Adressen im eigenen Staat zu blockieren oder strafrechtliche Investigationen einzuleiten. Aufgrund der unübersichtlichen Konstellationen im Cyberkontext erscheint es daher sinnvoll, ohne eine vorangehende Inkenntnissetzung keine Gegenmassnahmen gegen einen Staat richten zu dürfen, von dem schädigende Cyberangriffe ausgehen. Eine Notifizierung minimiert das Risiko, mit Gegenmassnahmen einen möglicherweise »falschen« oder unwissenden Staat zu verletzen. Die Inkenntnissetzung ermöglicht es dem vermeintlichen Angreiferstaat gegen die schädigenden Angriffe in seinem Territorium vorzugehen und dadurch auch seine völkerrechtliche Due Diligence-Pflicht wahrzunehmen. Sollte der betreffende Staat nach seiner Inkenntnissetzung über die von seinem Territorium ausgehenden Aktivitäten nicht das ihm Zumutbare und Mögliche unternehmen, um die Schädigungen zu beenden oder zumindest zu kooperieren, könnte er folglich seine Due Diligence-Verpflichtungen verletzen.[1229] Damit könnte auch ein als Brückenkopf missbrauchter Staat völkerrechtlich verantwortlich werden. Bei einer Bejahung der Due Diligence-Verletzung durch den als Brückenkopf missbrauchten Staat impliziert die Verhältnismässigkeit allerdings, dass eine Gegenmassnahme gegen Letzteren an der *Unterlassung* des ihm Zumutbaren – also der Verletzung der Due Diligence-Pflicht – und nicht an den durch den Angreifer versursachten Verletzungen zu messen ist.[1230] Die Völkerrechtsverletzung erfolgt in einer solchen Konstellation durch die Missachtung seiner Sorgfaltspflichten,[1231] von seinem Territorium ausgehende Schädigungen zu unterbinden, und nicht durch die Schädigungen an sich.[1232] Durch diesen Mechanismus wird also insgesamt Raum und Anreiz für Kooperation geschaffen. Vorliegend wird daher die Ansicht vertreten, dass gerade im Cyberkontext zwingend an der rechtlichen Voraussetzung einer Notifizierung festzuhalten ist.

1228 Tallinn Manual 2.0, S. 120 R21 C11. Dazu auch: SCHMITT, Countermeasures Response Option, S. 717.

1229 Eingehender zur Due Diligence-Pflicht siehe vorangehend unter III.B.2.c.

1230 Tallinn Manual 2.0, S. 130 R23 C11.

1231 Siehe III.B.2.c. sowie Tallinn Manual 2.0, S. 43 R7.

1232 Tallinn Manual 2.0, S. 130 R23 C12.

e. Zwischenfazit: Kooperationscharakter des Gegenmassnahmenrechts

Zusammenfassend kann festgehalten werden, dass verhältnismässige Gegenmassnahmen auf dem unilateralen Weg grundsätzlich als Reaktion auf Cyberangriffe denkbar sind. Allerdings kommen sie erst subsidiär zu friedlichen Streitbeilegungsmechanismen und Kooperationsersuchen in Betracht.[1233] Im Grunde ist das zwischen gleichen, souveränen Staaten geltende Völkerrecht genossenschaftlich bzw. koordinations- und kooperationsrechtlich ausgestaltet und schliesst strafende Sanktionen, wie sie für innerstaatliche Subordinationsverhältnisse typisch sind, grundsätzlich aus.[1234] Art. 49(1) ARSIWA statuiert, dass Gegenmassnahmen (nur) lanciert werden dürfen, um den verantwortlichen Staat zur Wiederherstellung der völkerrechtskonformen Situation zu bewegen und, dass jener gem. Art. 30 und 31 ARSIWA zur Beendigung und Nichtwiederholung der Verletzung sowie zu Entschädigungsleistungen verpflichtet ist. Diesen Kooperationscharakter unterstreicht grundsätzlich, dass die Parteien gem. IGH eine generelle Pflicht haben, bei der für die Streitigkeit relevanten Beweisetablierung zusammenzuarbeiten und zu kooperieren.[1235]

Es bleibt fraglich, ob vom Charakter her nicht-kooperativ ausgestaltete und nicht einer Wiedergutmachung dienende, aktive Cybergegenmassnahmen diesen Grundsätzen gerecht werden können. Auch angesichts der quantitativen und qualitativen Verhältnismässigkeitserfordernisse bleibt es fraglich, ob digitale Gegenmassnahmen zulässig sein sollen. Eine strikt juristische Verhältnismässigkeitsprüfung würde dies, wenn, dann nur sehr restriktiv zulassen.[1236] Die meisten Ansichten zu aktiven Cybergegenmassnahmen verkennen den im Vordergrund stehenden Zweck eines Ausgleichs und den Umstand, dass Cybergegenschläge dazu oft nicht dienlich sind. Bei Manipulationen und Blockierungen durch Cyberangriffe sind digitale Gegenmassnahmen oft ungeeignet, einen Ausgleich oder die Wiederherstellung der völkerrechtskonformen Situation (durch den Verletzerstaat) herbeizuführen. Durch das aktive Eingrei-

1233 Vgl. Sklerov, S. 36; Wingfield, S. 84 f., (zu möglichen praktischen, politischen Nachteilen bei einer Missachtung von Art. 2(3) UN-Charta) S. 87.

1234 Schulze, S. 70 m.w.V. Ähnlich: Dörr, S. 641. Dazu ferner u.a. auch: Epiney, S. 45; Zemanek, Schuld- und Erfolgshaftung, S. 315 ff.

1235 Mikanagi/Mačák, S. 67 u.a. m.V.a. IGH, Zellstofffabriken-Fall, §163; IGH, Kroatien-Genozid-Urteil, §173.

1236 Schmitt/Pitts kommen in ihrer Analyse zu Cybergegenmassnahmen mit Effekten gegen Drittstaaten im Ergebnis zu einer ähnlichen Schlussfolgerung, allerdings mit Verweis auf anhaltende Graubereiche: Schmitt/Pitts, S. 20 f.

fen in ein fremdes System oder das Blockieren von IP-Adressen oder Servern wird der reagierende Staat vielmehr selbst tätig, als dass er zur Durchsetzung von Rechtsansprüchen Druck aufsetzt. Es ginge weniger um ein im Gegenmassnahmenrecht verankertes Entziehen eines Vorteils, sondern vielmehr um ein selbständiges, oftmals anonymes, offensives Eingreifen. Zudem benötigen Cybergegenmassnahmen i.d.R. viel Zeit für die Programmierung und das Erlangen eines beabsichtigten Zugangs.[1237] Dadurch würden sie weniger als zeitnahes Druckmittel, sondern auch im Kontext der Staatenverantwortung vielmehr als (anonymer) Vergeltungsschlag fungieren. Gleichzeitig läuft man sowohl bei »Counter-DDoS« als auch bei durch Hackbacks freigelassenen Schadprogrammen Gefahr, weitergehende, unverhältnismässige Schädigungen durch die Reaktion auszulösen. Dies würde insgesamt eine Eskalation denkbar machen. Da im internationalen Kontext konstante Cyberaktivitäten unterschiedlicher Akteure zu vernehmen sind, drängt sich eine Zurückhaltung zusätzlich auf, aktive, in fremde Systeme eingreifende Cybergegenmassnahmen zu erlauben.[1238] Indem nicht jede Cyberoperation tatsächlich zu Völkerrechtsverletzungen führt und Hacker oftmals verschiedene Methoden »ausprobieren«, bei denen man i.d.R. noch nicht genau weiss, um was es den Angreifern geht,[1239] erschiene es insgesamt unverhältnismässig, jede Operation (direkt) mit aktiven Gegenmassnahmen zu beantworten. Obschon man solche Operationen durchaus im Auge behalten sollte, sollten ständige, impulsive Reaktionen auf jedes identifizierte Schadprogramm vermieden werden.[1240] Hinzu kommt, dass bei den meisten Ansichten in Bezug auf Cybergegenmassnahmen protektionistische Aspekte im Vordergrund stehen. Aus dem Verhältnismässigkeitserfordernis im Gegenmassnahmenrecht rührt jedoch, dass protektionistische Ziele vielmehr dem Charakter der Selbstverteidigung gem. Art. 51 UN-Charta und wenn, dann dem beschränkt zulässigen Rahmen *dringlicher*

1237 Siehe: Kormann, Interview mit Sandra Joyce, NZZ vom 31.03.2020, in dem die Sicherheitsexpertin Sandra Joyce digitale Vergeltungsschläge durch Staaten bespricht. Sie verweist darauf, dass man für das Eindringen in Computersysteme jeweils Zeit brauche. Um sich Zugang zu Computersystemen zu verschaffen, würde in gewissen Fällen bspw. sog. »password spraying« betrieben.

1238 Insgesamt aus ähnlichen Gründen für eine strategische Zurückhaltung: Dewar, Contextualizing, S. 14.

1239 Kormann, Interview mit Sandra Joyce, NZZ vom 31.03.2020.

1240 Dewar, Contextualizing, S. 14.

Gegenmassnahmen gem. Art. 52(2) ARSIWA entsprechen.[1241] Im Rahmen der Staatenverantwortung geht es nicht um die Existenzsicherung eines Staates, sondern um die Wiedergutmachung. Um den Schutz von Infrastrukturen zu erzielen, ohne einen offensiven Gegenschlag auszuüben, eignen sich zudem auch passive, nicht in fremde Systeme eindringende Cybermassnahmen. Etwa durch das Ausschalten oder Blockieren ausgewählter eigener Server – vorausgesetzt die innerstaatlichen und transnationalen Folgeschäden sind verhältnismässig (und damit milder als offensive Gegenschläge).[1242]

Insgesamt bietet sich im Kontext der Staatenverantwortlichkeit das Zurückgreifen auf *herkömmliche* Mechanismen und Gegenmassnahmen an – auch und gerade als Reaktion auf Cyberangriffe. Insbesondere stellt die Voraussetzung der vorzeitigen Notifizierung des (vermeintlich) verletzenden Staates ein Schlüsselelement dar, dem gerade im unübersichtlichen Cyberbereich eine enorme Bedeutung zukommen kann, um (für die Cybersicherheit und die technische Zurückverfolgung unerlässliche) Kooperationsbemühungen und einen Informationsaustausch zu fördern. Sollte der informierte Staat nicht reagieren und gegebenenfalls dadurch – ob er mit den Angriffen in Verbindung steht oder nicht – seine Due Diligence-Pflicht verletzen, könnte man in einem letzten Schritt, wenn alle Streitbeilegungs- und Verhandlungsbemühungen aussichtslos bleiben, als *ultima ratio* immer noch auf herkömmliche nichtmilitärische Gegenmassnahmen zurückgreifen.[1243] Angesichts der Verhältnismässigkeit bieten sich statt aktiven Cybergegenmassnahmen wie Hackbacks allerdings vielmehr traditionelle Massnahmen an wie z.B. die Androhung eines Waffenembargos oder das Nichtabschliessen eines interessanten Handelsvertrags. Statt »Counter-DDoS«-Angriffe zu lancieren wäre bspw. im Falle Estlands denkbar gewesen, dass finanzielle Verpflichtungen gegenüber Russland im Umfang der mutmasslichen Schadenssumme hätten ausgesetzt werden können, um Kooperation herbeizuführen.[1244] Ferner könnte man das Konzept von Waffenembargos allenfalls auch auf den digitalen Raum übertragen, indem

1241 Lahmann, S. 124. Bei dringlichen Gegenmassnahmen sollen umso höhere Anforderungen an den Nachweis gelten, da in jenen Fällen von verfahrensrechtlichen Voraussetzungen einer Gegenmassnahme abgesehen werden kann und, da irrtümlich ergriffene Selbsthilfemassnahmen die internationale Stabilität gefährden können: Krieger, S. 16.

1242 Lotrionte, S. 92.

1243 Vgl. Lahmann, S. 200.

1244 Diggelmann/Hadorn, S. 268.

bspw. die Lieferung gewisser Technologien eingestellt wird.[1245] Auch das Tallinn Manual 2.0 sieht Gegenmassnahmen, die in keinem Zusammenhang mit dem völkerrechtswidrigen Verhalten stehen, als ein wirksames Mittel, um den Verletzerstaat zur Wiederherstellung der völkerrechtskonformen Lage zu bringen.[1246] So bspw. indem ein von Cyberangriffen betroffener Küstenstaat seine Territorialgewässer für den oder die (vermeintlich) verantwortlichen Staaten schliessen würde.[1247] Dadurch könnte der Staat, von dem die Angriffe ausgehen, unter Druck gesetzt werden, um zu kooperieren und Entschädigungen zu leisten. Dies könnte gegebenenfalls eine mildere und wirksamere Massnahme sein, als wenn bspw. ganze Computernetzwerke im eigenen oder in einem anderen Staat (mit womöglich unverhältnismässigen Folgeeffekten) vom Internet abgekoppelt würden.

Eine zentrale Bedeutung könnte daher insb. der völkerrechtlichen Retorsion zukommen. Und zwar gerade, da es im Cyberkontext schwierig ist, Völkerrechtsverletzungen einem Staat zuzurechnen.[1248] Bei mächtigen Staaten kann allenfalls bereits die Erwähnung der blossen Möglichkeit einer Retorsion genügen, damit ein Rechtsverletzer sein rechtswidriges Verhalten aufgibt[1249] oder im Falle, dass er als Brückenkopf missbraucht wurde, Beendigungs- und Kooperationsbemühungen einleitet. Retorsionen können zudem teilweise mehr Wirkung erzielen als harte Gegenmassnahmen.[1250] Eine subtile Reaktion lässt nämlich mehr Raum für Gesichtswahrung sowie für ressourcenschonendes Austragen eines Konflikts – auf beiden Seiten.[1251] In den letzten Jahren wurde zunehmend die Stategie einer öffentlichen, politischen Zurechnung (sog. politische Attribution) diskutiert.[1252] Schädigende Cyberangriffe sollen diesem Konzept zufolge öffentlich den verantwortlichen Staaten zugeschrieben werden, um Fehlverhalten zu signalisieren und politischen Druck aufzusetzen.[1253] Eine solche öffentliche Attribution könnte angesichts möglicher

1245 Ähnlich wie beim Waffenhandel könnte ein Nachteil solcher Embargos sein, dass der Erwerb von dual-use Technologien und Schadprogrammen sich zunehmend auf den Schwarzmarkt verschiebt. Im Darknet gibt es bereits heute eine ganze »Industrie«, die vorprogrammierte Schadprogramme anbietet.

1246 Tallinn Manual 2.0, S. 129 R23 C10.

1247 Tallinn Manual 2.0, S. 129 R23 C10.

1248 Vgl. dazu: Delerue, Reinterpretation or Contestation, S. 323 f.; Lotrionte, S. 92.

1249 Diggelmann, Völkerrecht, S. 159, S. 166 f. Ähnlich: Cassese, S. 306; Wicker, S. 86.

1250 Diggelmann, Völkerrecht, S. 166.

1251 Diggelmann, Völkerrecht, S. 166.

1252 Broeders/De Busser/Pawlak, S. 9 ff. m.w.V.; Egloff/Wenger, S. 1.

1253 Siehe z.B. in: US National Cyber Strategy 2018, S. 21.

Gesichtsverluste, ähnlich einer Retorsionsandrohung, Anreize für Kooperationen im Einzelfall schaffen. Beispiele offizieller Reaktionen waren die öffentliche Attribution der Cyberangriffe auf Sony Pictures 2015[1254] an Nord-Korea oder die öffentliche Attribution der Cyberangriffe auf die US-Wahlen von 2016 an Russland.[1255] In letzterem Fall wurden auch Diplomaten ausgewiesen.[1256] Obschon dies starke Zeichen der Missbilligung sind, sind diese Reaktionen insgesamt als völkerrechtlich grundsätzlich erlaubte Retorsionen zu qualifizieren.[1257]

Insgesamt ist die Retorsion somit gerade im Cyberkontext die rechtlich unproblematischere staatliche Reaktion als es harte Sanktionen sind. Dennoch verzeichnen jüngere Entwicklungen eine gewisse Tenzenz hin zu härteren herkömmlichen Massnahmen. So haben sich die USA am 15. April 2021 infolge der sog. Solarwinds-Cyberangriffe[1258] für Sanktionen gegen Moskau entschieden, nachdem sie diese bereits zwei Monate zuvor angedroht hatten. Die Massnahmen umfassten einerseits die Ausweisung von Diplomaten. Andererseits wurden bestimmte Technologiefirmen auf eine schwarze Liste des amerikanischen Finanzministeriums gesetzt und der Handel mit neuen russischen Staatsschuldenpapieren in den USA verboten.[1259] Auch die EU verhängte laut einer Pressemitteilung vom 30. Juli 2020 erstmals Sanktionen gegen sechs Personen und drei Einrichtungen als Reaktion auf Cyberangriffe.[1260] Unter anderem bestanden diese aus Reiseverboten und dem Einfrieren von Vermögenswerten sowie dem Verbot für EU-Angehörige, den aufgelisteten Personen und Einrichtungen finanzielle Mittel zur Verfügung zu stellen. Betont wurde, dass dadurch eine abschreckende Wirkung erzielt werden sollte. Die Möglichkeit solcher Massnahmen wurde in den rechtlichen Rahmen des EU-»Instru-

1254 Roberts, The Guardian vom 02.01.2015; Schmitt, Just Security vom 17.12.2014. Im Zusammenhang mit WannaCry: Bossert, The Wall Street Journal vom 18.12.2017.

1255 Zu einem offiziellen Bericht zu den Zurechnungsinformationen: Intelligence Community Assessment vom 06.01.2017. Dazu auch: Watts, Just Security vom 14.10.2016.

1256 Perez/Diaz, CNN vom 03.01.2017. Siehe auch: The White House, Statements and Releases vom 29.12.2016; Mazzetti/Adam, New York Times vom 30.12.2016.

1257 Lotrionte, S. 92.

1258 Paul et al., The Guardian vom 24.02.2021.

1259 Mäder, NZZ vom 16.04.2021; Rüesch, NZZ vom 15.04.2021; Winkler, NZZ vom 16.04.2021.

1260 Europäischer Rat, Pressemitteilung vom 30.07.2020.

mentariums für die Cyberdiplomatie« integriert, der auch künftig gemeinsame diplomatische Reaktionen der EU auf böswillige Cyberaktivitäten ermöglichen soll.[1261]

An dieser Stelle lässt sich aus völkerrechtlicher Sicht festhalten, dass auch herkömmliche Sanktionen und Gegenmassnahmen, sobald diese zwangsweise in die Integrität eines anderen Staates eingreifen, mitunter unter den rechtlichen Aspekten der Verhältnismässigkeit zu rechtfertigen sind. Dabei muss, wie vorangehend aufgezeigt, jede Gegenmassnahme grundsätzlich jeweils auf die Wiederherstellung der Völkerrechtskonformität abzielen sowie quantitative und qualitative Aspekte würdigen. Daher müssen auch *herkömmliche* Sanktionen als Reaktion auf Cyberangriffe näher betrachtet und der jeweilige Kontext berücksichtigt werden.[1262] Herkömmliche Selbsthilfemassnahmen können kein »Allzweck«-Mittel sein, um jeden geopolitischen, komplexen Konflikt abzukühlen. In der Praxis stellen sich neben ihrer Verhältnismässigkeit mitunter im Hinblick auf ihre Effizienz und Geeignetheit weitergehende Fragen, die den Umfang der vorliegenden Abhandlung sprengen würden.[1263] Festhalten lässt sich dennoch, dass herkömmliche nicht-militärische Gegenmassnahmen im Vergleich zu aggressiven digitalen Gegenschlägen zu bevorzugen sind. Da Zurechnungsschwierigkeiten von Völkerrechtsverletzungen im Cyberkontext bestehen bleiben, wird bei herkömmlichen nicht-militärischen Gegenmassnahmen das Eskalationspotenzial wohl insgesamt überschaubarer bleiben als bei (anonymen sowie u.U. zeitverzögerten und schwer kalkulierbaren) digitalen Gegenschlägen.

Letztlich bleibt jede einseitig ergriffene, herkömmliche und digitale Massnahme im internationalen Kontext mit erheblichen Herausforderungen verbunden. Die internationale Völkerrechtskommission hat bereits in ihren Berichten von 1992 und 1993 ihre Besorgnis geäussert, dass der unilaterale Charakter von Gegenmassnahmen mit einem erheblichen Missbrauchspotenzial verbunden sei.[1264] Für eine grundsätzlich restriktive Handhabung von unilateral ergriffenen Massnahmen spricht letztlich auch das für das Völkerrecht

1261 Europäischer Rat, Pressemitteilung vom 17.05.2019. So folgten weitere Sanktionen auf Cyberangriffe durch die EU: Europäischer Rat, Pressemitteilung vom 22.10.2020.

1262 Eingehender zu Sanktionen gegen Cyberangriffe: Moret/Pawlak, S. 1 ff.

1263 Zur (begrenzten) Effizient, Geeignetheit und den Kosten von Sanktionen u.a.: Moret/Biersteker et al.

1264 Siehe den Bericht der Völkerrechtskommission zur 45. Session 1993 (UN Doc. A/48/10 (1993)), S. 38 §228 und den Bericht zur 44. Session 1992 (UN Doc. A/47/10 (1992)), S. 39 §117 ff.; Dazu: Schachter, Dispute Settlement and Countermeasures, S. 472.

massgebende Konsensprinzip.[1265] Ein nachhaltiger Konsens sowie Kooperations- und Entschädigungsbestreben der Beteiligten, die letztlich auch die internationale Stabilität insgesamt beeinflussen, können primär durch die verschiedentlich ausgeprägte Wiedergutmachungsidee erreicht werden.[1266] Unilateral getroffene, eine Gegenpartei im unübersichtlichen Cyberkontext womöglich verletzende Massnahmen sind daher langfristig meist nicht geeignet, um dauerhafte und friedliche Lösungen zu erreichen. Dies spricht gesamthaft gerade im Cyberkontext dafür, sich verstärkt an bestehenden (und noch zu etablierenden) Kooperations- und Wiedergutmachungmechanismen zu orientieren. Unilateral ergriffene Selbsthilfemassnahmen, die in die Souveränität eines anderen Staates eindringen, sind aus völkerrechtlicher Sicht stets als *ultima ratio* zu betrachten.[1267] Diese sollen nur lanciert werden dürfen, wenn ein Konflikt nicht mehr mittels friedlicher Bemühungen gelöst werden kann bzw. diese ausgeschöpft wurden.[1268] Daher sollten bereits im Vorfeld von konkreten Cyberangriffen *institutionalisierte* technische oder politische Kooperations- und Schadensbegrenzungsmechanismen etabliert werden.

1265 Zum Konsensprinzip: SCHRÖDER, S. 700; SCHULZE, S. 70. Ähnlich: WHITE/ABASS, S. 521.

1266 SCHULZE, S. 70.

1267 CRAWFORD umschreibt Gegenmassnahmen als »*ultimate remedy which an injured state may take after efforts to obtain cessation and reparation have failed*«: CRAWFORD, Brownlie's Principles, S. 553.

1268 Im Ergebnis ähnlich: SCHACHTER, Dispute Settlement and Countermeasures, S. 471 ff.

C. Zusammenfassung

1. Verhältnismässigkeit im Cyberkontext eng zu fassen

Insgesamt sind die Reaktionsmöglichkeiten sowohl herkömmlicher als auch digitaler Art in beiden Bereichen unilateraler Selbsthilfe – beim Selbstverteidigungsrecht und bei Gegenmassnahmen – im Cyberkontext nur sehr restriktiv zu bejahen. Das in Lehre und Rechtsprechung anerkannte Verhältnismässigkeitsprinzip setzt in beiden Bereichen objektiv-rechtliche Schranken. Grundsätzlich kann man zudem festhalten, dass in der Diskussion um die Legalität von *digitalen* Selbsthilfemöglichkeiten nicht klar zwischen den rechtlich zu unterscheidenden Bereichen der Selbstverteidigung nach Art. 51 UN-Charta und Gegenmassnahmen gem. ARSIWA unterschieden wird. In beiden Diskursen werden aktive Cybergegenmassnahmen thematisiert und der Tendenz nach bejaht, obschon die Verhältnismässigkeit in den beiden Bereichen eine divergierende Bedeutung hat. Aus vorliegender Sicht ist es daher zentral, die unterschiedlichen rechtlichen Regime zu differenzieren. Die Mehrheit der Autoren, die digitale Gegenmassnahmen als Selbsthilfehandlungen gegen Cyberangriffe analysieren, sieht ihre Funktion zudem primär in einer Verteidigung gegen Cyberangriffe – das heisst als unilaterale Notfallmassnahmen zum Schutz betroffener Netzwerkinfrastrukturen eines Staates.[1269] Diese sofortige Ausrichtung solcher Massnahmen passt allerdings grundsätzlich nicht zum Charakter aktiver Gegenmassnahmen, da neben einer technischen Attribution und dem Nachweis einer (Sorgfalts-)Pflichtverletzung[1270] auch das Programmieren von aktiven digitalen Gegenmassnahmen Zeit benötigt. Daher dürften sowohl automatisierte als auch im Einzelfall zu programmierende Gegenschläge, die im Nachgang an Verletzungen gegebenenfalls zu Schädigungen von Unbeteiligten führen könnten, i.d.R. weder der völkerrechtlichen Verhältnismässigkeitsprüfung des Selbstverteidigungs- noch des Gegenmassnahmenrechts standhalten.

Angesichts der Notwendigkeit, bei schwerwiegenden Cybersicherheitsstörungen (kritischer) Infrastrukturen unverzüglich zu handeln, werden automatisierte digitale Verteidigungsmittel (oder anderweitige Reaktionsmechanis-

---

1269 Lahmann, S. 124.

1270 Lahmann, S. 200.

men) allerdings wohl weiterhin erkundet und aufgerüstet werden.[1271] LAHMANN schlug vor diesem Hintergrund insb. aufgrund der verbleibenden Attributionsproblematik mögliche Elemente eines rechtlichen »Cyber Notfall-Regime« vor.[1272] Demzufolge denkbar sei, dass ein Staat im Rahmen eines Notstandes sinngemäss zu Art. 25 ARSIWA und abseits des völkerrechtlichen Gegenmassnahmen- und Selbstverteidigungsrechts sofortige aktive Schutzmassnahmen gegen Cyberangriffe einleiten können soll.[1273] Daraus entstehende Schädigungen Dritter könnten in jenem Kontext allenfalls aufgrund einer Notlage gerechtfertigt werden. Zudem müsste man aufgrund einer Notlage die technische und rechtliche Zurechnung nicht abwarten,[1274] da die Notstandsklausel gem. Art. 25 ARSIWA grundsätzlich – anders als das Selbstverteidigungs- und das Gegenmassnahmenrecht – nicht am jeweils vorangehenden Verhalten eines Staates ansetze.[1275] In Fällen, in denen man sofort handeln muss, um fundamentale Interessen gegen ernsthafte, imminente Gefahren zu schützen, während man noch nicht weiss, wer hinter dem Angriff steht, könne ein solches Regime insofern von der Idee her Abhilfe schaffen.[1276] Die Doktrin ist allerdings nicht unproblematisch:[1277] Die Notstandsidee hat ähnlich dem Selbstverteidigungsrecht nämlich einen Ausnahmecharakter, der auf der Annahme fusst, dass die grundsätzlich geltenden Rechtsgrundlagen nur ausnahmsweise ausgesetzt werden sollen, wenn nicht anders auf eine faktische Notlage reagiert werden kann.[1278] Bei einem regelmässigen Gebrauch des Notstandstatbestands würde man daher seinen Ausnahmecharakter untergraben. Zudem bliebe es angesichts des Wissens um die ständige Bedrohung von Cyberangriffen fraglich, ob offensive digitale Gegenschläge regelmässig den »einzigen Weg«[1279] darstellen, zumal oft passive Alternativen zur Verfügung stehen. Hinzu kommt, dass im Zusammenhang mit dem Notstand wiederum ein anderes Verständnis der Verhältnismässigkeit gelten würde, das separat zu betrachten wäre. Zudem stellt sich das faktische Problem des potenziell unkontrollierten und quantitativen Übermasses einer digitalen Reaktion sowie die

1271 LAHMANN, S. 274.

1272 LAHMANN, S. 272 ff.

1273 Zur Aufarbeitung des Notstands im Cyberkontext siehe: LAHMANN, S. 201 ff.; Tallinn Manual, 2.0, S. 135 ff. R26. Ferner auch: Tallinn Manual 2.0, S. 114 R20 C12.

1274 LAHMANN, S. 264.

1275 Vgl. ARSIWA-Kommentar, Art. 25(2).

1276 Mit dem Beispiel von DDoS-Angriffen: LAHMANN, S. 275.

1277 Ausführlicher dazu: LAHMANN, S. 264.

1278 LAHMANN, S. 265 m.w.V.; ZWITTER, S. 100 f. Eingehender zu Schwierigkeiten i.Z.m. dem Notstand: AGO, S. 14 ff. Ähnlich auch: IGH, Gabčíkovo-Nagymaros-Urteil, §51.

1279 Siehe Wortlaut von Art. 25(1)(a) ARSIWA.

Frage nach der Geeignetheit einer gewaltsamen Verteidigung im Cyberkontext weiterhin. Ebenfalls gibt es in der IGH-Rechtsprechung keine Anhaltspunkte dafür, dass der Gerichtshof die Notstandsidee als unilateral erlaubte Gewaltanwendung akzeptieren könnte.[1280] Bisher haben sich zudem auch im traditionellen Kontext nur vereinzelte Autoren für eine Notstandsausnahme ausgesprochen.[1281]

Die vorangehenden Ausführungen sprechen gesamthaft dafür, das Verhältnismässigkeitsprinzip im Cyberkontext eng zu fassen. Als völkerrechtskonforme, sofortige Reaktion denkbar sind daher insgesamt primär deeskalierende Massnahmen *ohne Gegenangriff*, das sofortige Informieren der – vorausgesetzt diese ist im Zeitpunkt der Verletzung bekannt – das »schädigende« Computersystem beherbergenden Partei oder das Zurückgreifen auf herkömmliche Retorsionshandlungen.

2. Verhältnismässigkeit als Sicherung des Sinn und Zwecks der Selbsthilfe

Das Völkerrecht basiert in seinen Grundsätzen auf der Idee der Erhaltung und Wiederherstellung von Stabilität.[1282] Zu dieser trägt es u.a. mittels seiner Institutionen des Rechts der diplomatischen Beziehungen, der Souveränität, des Gewalt- und Interventionsverbot sowie der daran anküpfenden Selbsthilfe bei.[1283] Wie vorliegend ersichtlich wurde, stellt das Verhältnismässigkeitsprinzip insgesamt ein völkerrechtliches Schlüsselelement dar, um den Sinn und Zweck der auf der Stabilitätsidee fussenden völkerrechtlichen Selbsthilfe sicherzustellen. Das Prinzip kann von fundamentaler Bedeutung sein, das Eska-

1280 Kress, S. 594. Ihm zufolge scheint auch die Staatengemeinschaft sich darüber einig zu sein, Gewaltanwendungen auf der Grundlage eines Notstands zu verbieten: Kress, S. 603. Eingehender zu den sich methodologisch stellenden Problemen eines Notstands sowie dazu, dass die Notstandsidee im herkömmlichen Kontext grundsätzlich *nicht* anerkannt ist: Corten, Necessity, S. 861 ff.

1281 Kress, S. 593 u.a. m.V.a. Laursen, Necessity, S. 485 ff. Für eine Notstandstandsausnahme auch: Gazzini/Werner/Dekker, S. 3 ff. Obschon Ago, in der Funktion als Sonderberichtserstatter der Völkerrechtskommission, eine grundsätzliche Offenheit für eine (sehr restriktiv anzunehmende) Notstandsklausel geäussert hat (siehe: Ago, S. 14 ff.), hat es die Völkerrechtskommission gem. Kress letztlich unterlassen, diese Frage im Artikelentwurf für die Verantwortlichkeit von Staaten (ARSIWA) oder deren Kommentaren festzuhalten. Siehe dazu: Heathcote, Necessity, S. 498 f. Zu schwierigen Fragen i.Z.m. einem Notstand im Rahmen der Staatenverantwortlichkeit des Weiteren: Sloane, Necessity, S. 447 ff.

1282 Diggelmann, Völkerrecht, S. 200.

1283 Diggelmann, Völkerrecht, S. 200.

lationspotenzial innerhalb von Konflikten zu reduzieren, (übermässige) Gewalt einzuschränken und Voraussehbarkeit zu schaffen. Da transnationale Schädigungsradien und -möglichkeiten zunehmen, wird die Frage nach der Verantwortlichkeit und Handhabung transnationaler Völkerrechtsverletzungen die internationale Staatengemeinschaft weiterhin beschäftigen. Es ist daher von besonderer Wichtigkeit, dass das Verhältnismässigkeitsprinzip verstärkt in den Diskurs um Cyberangriffe aufgenommen wird. Bei der Aufrüstung digitaler Verteidigungsmittel wird man sich insb. nicht nur verstärkt die Fragen stellen müssen, was man mit digitalen Massnahmen erreichen möchte, sondern auch, was man rechtlich darf. Man muss, um das rechtliche Prinzip der Verhältnismässigkeit zu wahren, über das beabsichtigte Ziel nachdenken und sicherstellen, dass dies beim Einsatz digitaler Massnahmen (gezielt) programmierbar und das Risiko von Kollateral- und Sekundärschädigungen (Dritter) minimierbar ist. Da Zurechnungsschwierigkeiten technisch bestehen bleiben und sowohl im Bereich der Selbstverteidigung als auch im Gegenmassnahmenrecht zeitlich verzögerte Vergeltungsschläge verboten sind, bieten insb. die traditionell etablierten Institutionen des Gegenmassnahmenrechts Chancen zur Konfliktbewältigung. Vor dem Hintergrund der Stabilitätsidee und der damit zusammenhängenden Rechtsstaatlichkeit scheint es zudem wichtig, dass Cyberangriffe nicht regelmässig unter einen als restriktive Ausnahme zu verstehenden Notstand subsumiert werden.[1284] Dadurch würde man nämlich den bewährten rechtlichen Strukturen ausweichen, die der vorliegenden Ansicht nach genügend Grundlagen bieten, das Phänomen von Cyberangriffen zu erfassen. Insbesondere schaffen die Mechanismen der Notifizierung sowie herkömmliche, auf politische Druckausübung ausgerichtete Retorsionshandlungen und Gegenmassnahmen Raum und Anreiz für Kooperation. Gerade *traditionelle* Retorsionshandlungen und die Notifizierung stellen ein für den Cyberkontext zentrales Instrument dar, da diese aufgrund ihrer grundsätzlichen Völkerrechtskonformität auch gegen einen Staat gerichtet sein können, bei dem die technische und rechtliche Verantwortung nicht zweifelsohne feststeht. Unternimmt der informierte Staat sodann nicht das ihm Mögliche, um eine Verletzung zu beenden und wird (unter Umständen auch erst später) dadurch eine Due Diligence-Verletzung festgestellt, können gegebenenfalls Reparationsansprüche geltend gemacht werden. Eine solche *ex post facto*-Rolle von Gegenmassnahmen könnte in den kommenden Jahren an Bedeutung ge-

[1284] Vgl. LAHMANN, S. 264. Er sieht im Ergebnis ein auf der Notstandsidee fussendes Cyber-Notfall-Regime ebenfalls als rechtstaatlich nicht unproblematisch.

winnen, da eine erfolgreiche (und akkurate) technische Zurückverfolgung jeweils Zeit benötigt, die meist zeitlich über die ausschlaggebende Verletzung hinausgeht.[1285]

3. Würdigung des Gesamtkontexts

Im Zusammenhang mit der Verhältnismässigkeit wird immer ein Ermessensspielraum bestehen bleiben, anhand dessen die jeweilige Schwere und die involvierten Rechte der Verletzung mit der Gegenmassnahme abgewogen werden können und müssen. Diese Folgerung unterstreicht daher die Wichtigkeit, Cyberangriffe nie isoliert zu betrachten.[1286] Gerade im global vernetzten Cyberraum, in dem Verletzungen schwierig messbar und Angreifer schwierig ausmachbar sind, ist es umso wichtiger, den gesamten geopolitischen Kontext zu betrachten.[1287] Um die Verhältnismässigkeitsprüfung mit deren Ermessensspielraum auf den Cyberraum zu übertragen, ist es demzufolge unabdingbar, nicht-digitale Umstände in die Würdigung aufzunehmen. Diese Folgerung scheint zwar banal, kann allerdings von fundamentalem Ausmass sein, damit ein Staat handlungsfähig bleibt, während er sich gleichzeitig völkerrechtskonform verhält. Darüber hinaus unterstreichen die unübersichtlichen Verhältnisse und die Attributionsschwierigkeiten bei Cyberangriffen, dass sich gerade im digitalen Bereich zunehmend eine Notwendigkeit aufdrängt, bereits zu Friedenszeiten verstärkte technische, rechtliche und politische Kooperationsmechanismen zu etablieren. Indem der überwiegende Anteil digital vernetzter Infrastrukturen nicht nur territoriumsübergreifend, sondern meist auch privat ist, betreffen dabei die Fragen nach der Ausgestaltung von Kooperation nicht nur den zwischenstaatlichen Bereich, sondern auch zunehmend die Zusammenarbeit zwischen Staat und Privaten. Durch einen institutionalisierten,

---

1285 LAHMANN, S. 200.

1286 Ähnlich (allerdings auch die inhärente Subjektivität der Beweiserbringung betonend): WOLTAG, S. 181.

1287 Ähnlich: MIKANAGI/MAČÁK, S. 68. Ihnen zufolge ist im Cyberkontext indirekten und die Umstände würdigenden Beweisen besonderes Gewicht zuzuschreiben, wenn sie auf einer Reihe zusammenhängender Tatsachen beruhen. Dabei verweisen sie auf das Korfu Kanal-Urteil, S. 18, in dem der IGH indirekte und die Umstände würdigende Beweise u.U. zulässt: »*[b]y reason of this exclusive [territorial] control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence*«. Eine solche Bezugnahme darf dabei gem. IGH »keinen Raum für begründete Zweifel« ('no room for reasonable doubt') belassen. Siehe ferner dazu: BRUNNER/DOBRIĆ/PIRKER, S. 86 f.

technischen Informationsaustausch kann nicht nur die Resilienz digitaler Infrastrukturen im Vorfeld konkreter Angriffe generell erhöht werden, sondern es können auch verbesserte *ad hoc*-Kooperations- und Reaktionsmechanismen aufgegleist werden, die in einem Cybervorfall die jeweilige Schadensbegrenzung, -beendigung und erforderliche Investigation unterstützen können.

V. Konklusionen und Ausblick

A. Konklusionen

1. Stabiliserung der internationalen Ordung durch Voraussehbarkeit und Kontinuität

Sowohl die militärische Selbstverteidigung als auch nicht-militärische Gegenmassnahmen sind und bleiben problematische und störungsanfällige Institutionen. Gleichzeitig kann man nicht auf sie verzichten, da sie im dezentralen System des Völkerrechts voraussehbare Strukturen für den Umgang mit Völkerrechtsverstössen schaffen. Die Grundschwierigkeit besteht allerdings darin, dass die Möglichkeit zur Selbsthilfe so weit bestehen muss, dass sich Rechtsverletzungen für einen Staat nicht »lohnen«.[1288] Es soll eine ernsthafte, konsequente sowie *angemessen* unangenehme Reaktion in Aussicht stehen, sodass kein Anreiz zu einem Völkerrechtsverstoss besteht. Gleichzeitig darf die Selbsthilfe nicht so weit gehen, dass sie ihrerseits die internationale Stabilität und Rechtsordnung gefährdet oder eine Konflikteskalation fördert. Das völkerrechtlich anerkannte Verhältnismässigkeitsprinzip spielt in dieser Hinsicht eine zentrale Rolle, um – mit seiner unterschiedlichen Ausrichtung in den jeweiligen Bereichen – einen voraussehbaren, wenn auch vagen Rahmen für eine Reaktion zu schaffen. Die Verhältnismässigkeit kann dazu dienen, dass eine Selbsthilfemassnahme nicht selbst zu einer Gefahr für die Rechtsordnung wird, indem das Verhalten des ursprünglich Verletzten zum grösseren Problem wird als jenes des ursprünglichen Verletzers.[1289]

Das Problem übermässiger Selbsthilfemassnahmen beschäftigt das Völkerrecht seit seinen Anfängen[1290] und zieht sich – trotz sich ändernder Konfliktformen und -mittel – bis in heutige Debatten. Obschon auch das in diesem Zusammenhang oft diskutierte Verhältnismässigkeitserfordernis weiterhin Gegenstand weitreichender Diskussionen ist, hat sich das Prinzip als ein zentrales Element für die Beschränkung übermässiger Gegenmassnahmen herauskristallisiert.[1291] Dabei wird der dem Verhältnismässigkeitsprinzip – wie

---

1288 DIGGELMANN, Völkerrecht, S. 161.

1289 Zum Abschnitt: DIGGELMANN, Völkerrecht, S. 161.

1290 DIGGELMANN, Völkerrecht, S. 161.

1291 Vgl. O'CONNELL, Power and Purpose, S. 264: »*Although countermeasures are measures of self-help, they are not ›lawless‹ in the sense that anything goes.*« Sie verweist dabei mitunter auf das Erfordernis der Verhältnismässigkeit.

auch anderen Völkerrechtsnormen – inhärente Ermessensspielraum die Staaten weiterhin begleiten. Die Auslegung von Völkerrechtsnormen wird im Einzelfall weiterhin Interessenabwägungen implizieren und bis zu einem gewissen Grad Gegenstand subjektiver Interpretationen bleiben. So wurden bereits vor den Zeiten des Gewaltverbots unter dem Titel der Repressalie oder der Gegenmassnahme klassische Angriffskriege geführt, indem Rechtsverletzungen der Gegenseite als Vorwand für Aggressionen missbraucht wurden.[1292] Indem gewaltsame (militärische) Massnahmen auch in jüngeren Entwicklungen und potenziell auch als Reaktion auf Cyberangriffe eingesetzt werden könnten, könnten sich vergleichbare Konstellationen bis in die Gegenwart ziehen. Die vorliegende Abhandlung sollte dabei insgesamt die Wichtigkeit aufgezeigt haben, dass im Diskurs um die Reaktion auf Cyberangriffe – trotz konzeptueller Nähe unilateraler Selbsthilfemassnahmen zueinander – rechtlich klar und konsequent zwischen militärischen und nicht-militäritschen Gegenmassnahmen unterschieden werden muss – insb. und gerade auch im Hinblick auf Cyberangriffe (und Hackbacks).

Es sollte zudem deutlich geworden sein, dass völkerrechtliche Normen innerhalb der internationalen Staatengemeinschaft jeweils von einer breiten Facette an Faktoren, teilweise gegenläufigen Interessen sowie kulturell divergierenden Haltungen geprägt sind. Zum einen widerspiegeln sie insb. durch den Einbezug von Staatenpraxis und *opinio iuris* staatliche Interessen und Ziele sowie den Versuch, innerhalb des Systems kollektiver Sicherheit Sanktionsmechanismen und -strukturen zu schaffen. Zum anderen sollen sie internationale Stabilität fördern, was den Handlungsspielraum von Staaten teilweise gerade beschränken können soll. Und obschon das Globalisierungs- und Digitalisierungszeitalter immense Veränderungen mit sich brachte, wird das Völkerrecht weiterhin eine Wechselwirkung mit den geopolitischen Grundkonstellationen sowie bestehenden Mächteungleichgewichten zwischen Staaten bleiben.[1293] Dabei sind neue technologische Möglichkeiten sowie das Aufkommen weiterer (völkerrechtlich u.U. relevanter) Akteure mit Errungenschaften, aber, wie vorliegend aufgezeigt wurde, auch mit neuen Problemen verbunden. Was zunächst – und dies auch im Hinblick auf die Regulierung von Cyberangriffen – als »gut« oder »schlecht«, als »richtig« oder »falsch« erscheint, erweist sich bei näherer Betrachtung oft als komplexer.[1294] Die Debatte um die Anwendung von Völkerrecht wird immer von unterschiedlichen Interessen,

1292 Diggelmann, Völkerrecht, S. 161.

1293 Diggelmann, Völkerrecht, S. 199.

1294 Diggelmann, Völkerrecht, S. 199.

von subjektiv betroffenen sowie auch distanzierten Betrachtern sowie von ungleichen Machtstrukturen geprägt sein. Dies bedeutet – auch im Cyberraum – ein ständiges Austarieren von geopolitischen Interessen und Gegebenheiten.

Vor dem Hintergrund des Diskurses um Cyberangriffe lässt sich schliessen, dass die geltenden Völkerrechtsprinzipien auf staatliches Verhalten im Cyberbereich grundsätzlich anwendbar sind.[1295] Sie sind genügend offen, um neue Phänomene zu erfassen und bieten zugleich einen rechtlichen Rahmen, der als Orientierungshilfe für staatliches oder dem Staat zurechenbares Verhalten dienen kann. Obschon Uneinigkeiten im Hinblick auf Auslegungsfragen bestehen bleiben, gibt es nämlich grundsätzliche Bestimmungen, in derer Substanz man sich einig ist.[1296] Indem es auch im völkerrechtlichen Diskurs zu Cyberangriffen um die Regulierung staatlichen Handelns und Unterlassens geht, widerspiegelt der Diskurs daher (weiterhin) herkömmliche Fragen der internationalen Konfliktlösung und -definierung sowie die Frage nach der Schaffung und Aufrechterhaltung von Stabilität. Einerseits ist dabei das Argument berechtigt, dass bestehende Normen angesichts neuer Phänomene weiterentwickelt werden müssen, um ihren normativen und regulatorischen Wert nicht zu verlieren. Andererseits kann das Festhalten an der traditionellen Ausrichtung etablierter Normen insgesamt zentral sein, um die historisch gewachsene, internationale Stabilität weiterhin zu fördern. Im Grunde ändert sich mit Cyberangriffen nämlich »nur« der Untersuchungsgegenstand, indem sich die in Konflikten oder zu strategischen Zielen eingesetzten Mittel und Technologien verändern. Geopolitische Dynamiken, Konflikte und Fragen nach friedlicher Streitbeilegung bleiben, wie gesagt, in ihrem Kern bestehen. Unverkennbar ist dabei dennoch, dass Cybertechnologien durch ihre globale Vernetzung fundamentale Veränderungen mit sich bringen, in der hybride, private oder anonyme Akteurskonstellationen und Verflechtungen zunehmend und wechselseitig auftreten – Veränderungen, die die an territoriale Grenzen anknüpfende staatliche Souveränität herausfordern und denen sich die gegenwärtige Suche nach Antworten zu Anwendungsfragen stellen muss. Völkerrechtliche Fra-

1295 Im Grunde ähnlich: Heintschel von Heinegg, Informationskrieg, S. 154. Er verweist dabei auf die Notwendigkeit, dass Auslegungsergebnisse vom Konsens der Vertragsparteien bzw. von der Rechtsüberzeugung der Staaten umfasst sein müssen.

1296 Vgl. Schachter, Armed Force, S. 1645: »*Yet underlying the disagreements, there is a considerable area of agreement on the core substantive law. It would be a mistake to conclude that the international law of force is so vague and fragmentary as to allow governments almost unlimited latitude to use force. International texts and the legal positions taken by governments reveal a coherent body of principles that apply to a wide range of conduct involving armed force*«.

gen zur Auslegung und Anwendung eines über Jahrzehnte etablierten Rechtssystems auf sich verändernde Umstände werden daher weiterhin aufkommen. Das etablierte internationale System an sich leistet jedoch durch die längjährigen Kodifizierungs- und Spezifizierungsprozesse mit seinen objektiv festmachbaren Kriterien und Grundsätzen einen nicht unwesentlichen Beitrag, das fragile internationale System kollektiver Sicherheit aufrecht zu erhalten.

Die Erkenntnisse dieser Dissertation erlauben die Folgerung, dass die Anwendung des Verhältnismässigkeitsprinzips insb. im diffusen und sich technisch wohl weiterhin verändernden Kontext von Cyberangriffen ernst genommen, bestätigt und eingehender diskutiert werden muss. Das Prinzip kann gerade im Cyberbereich von fundamentaler Bedeutung sein, um Grenzen staatlichen Handelns zu definieren. Der hier vertretenen, rechtlichen Meinung nach ist die Verhältnismässigkeit angesichts der verbleibenden Unübersichtlichkeiten bei den Effekten von Cyberangriffen sowie angesichts des Sinn und Zwecks einer unilateralen Reaktion inhaltlich und zeitlich eng zu fassen. Eine verstärkte Auseinandersetzung mit der Anwendung des Prinzips im Cyberbereich durch Wissenschaft und Praxis kann für eine Konsensfindung in dieser Hinsicht zentrale, voraussehbare Orientierungshilfen bieten und (restriktive oder extensive) Auslegungsmöglichkeiten bestätigen. Dazu unabdingbar ist gerade auch für den künftigen Weg ein verstärkter Wissenstransfer zwischen den technischen, politischen und rechtlichen Disziplinen, um einerseits die Radien und Effekte staatlichen Handelns im Cyberbereich besser zu verstehen und andererseits, um abseits politischer Möglichkeiten auch den Sinn und Zweck völkerrechtlicher Normen im System kollektiver Sicherheit nicht zu verkennen.

2. Zum Umgang mit Interpretationsspielräumen

Gesamthaft betrachtet führen die sich aus den dezentralen Strukturen sowie auch aus den der Thematik inhärenten Interpretationsspielräumen ergebenden Unschärfen des Völkerrechts zu einem höheren Theoriebedarf als dies in anderen juristischen Disziplinen der Fall ist.[1297] Je grösser die Unbestimmtheit eines Rechts ist, desto mehr Relevanz erhält folglich die Auseinandersetzung in Wissenschaft und Praxis. »*Der Grund, auf dem man sich bewegt*«, so DIGGELMANN, »*schwankt eben stärker als in anderen Disziplinen*«.[1298] Insofern

[1297] DIGGELMANN, Völkerrecht, S. 127.

[1298] DIGGELMANN, Völkerrecht, S. 127. Ähnlich: KAMMERHOFER, Kelsenian Perspective, S. 57, der angesichts inhärenter Unklarheiten im Völkerrecht die Wichtigkeit der Auseinandersetzung in der Lehre mit denselben und den damit verbundenen Mehrheitsmeinungen betont.

können weitergehende Grundsatzdiskussionen zum für staatliches Verhalten fundamentalen Verhältnismässigkeitsprinzip wichtige (objektive) Orientierungshilfen bieten, um mit sich verändernden Untersuchungsgegenständen und Phänomenen umzugehen. Bei internationalen Normen geht es zudem regelmässig um einen minimal und zugleich maximal möglichen Konsens. Die oftmals vorgebrachte Unbestimmtheit und die Interpretationsspielräume völkerrechtlicher Selbsthilfenormen führen dabei regelmässig zu grösseren Handlungspielräumen und (strategisch-politischen) Auslegungsmöglichkeiten durch ihre Betrachter. Gerade deshalb ist die Auseinandersetzung in der Wissenschaft von besonderer Bedeutung. Als solche ermöglicht sie nämlich eine objektiv-rechtliche Reflexion der zugrundeliegenden Grundsatzaspekte und erlaubt es, politisch sowie subjektiv geprägte Auslegungen von *Recht*snormen kritisch zu hinterfragen.

Im Hinblick auf den normativen Wert unbestimmter Rechtsprinzipien wie der Verhältnismässigkeit ist es ebenfalls wichtig, dass diese durch Staaten, Lehre und Rechtsprechung explizit im Cyberraum thematisiert werden.[1299] Angesichts der Absenz von Normenhierarchien im dezentralen System des Völkerrechts und einer potenziellen Etablierung von Völkerrechtsnormen durch Staatenpraxis und *opinio iuris* haben Staaten eine einflussreiche Verantwortung (und ein offensichtliches Interesse), die Anwendung bestehender Normen zu klären.[1300] Dahingehende Ansichten, dass Staatenpraxis und *opinio iuris* dabei die wichtigsten oder sogar die einzigen Beiträge sind, um Graubereiche in der Anwendung völkerrechtlicher Normen im Cyberbereich zu klären,[1301] fokussieren sich dabei allerdings wohl zu sehr auf die diesbezügliche Bedeutung von Staaten.[1302] Vor dem Hintergrund einer möglichst objektiv-rechtlichen Würdigung vager Rechtsnormen hat die vorliegende Analyse nämlich die Wichtigkeit aufgezeigt, gerade auch objektive, dem Recht verpflichtete Gegengewichte in den Diskurs einzubeziehen. Daher ist es wichtig, dass sich auch von politischen Spannungen unbetroffene Betrachter einbringen und Haltungen auch zu Friedenszeiten geäussert werden. Die zunehmenden Bemühungen auf Ebene der UNO, Staaten proaktiv in den Cyberregulierungsprozess miteinzubeziehen und ihnen den Zugang zum Diskurs zu ermöglichen (z.B. mittels OEWG) stellen wichtige, erforderliche Weichenstellungen für mög-

1299 Zum normativen Wert von Normen im Hinblick auf die Steuerung staatlichen Handelns (sog. »compliance-pull«): FRANCK, Legitimacy among Nations, S. 45 ff.

1300 EGAN, S. 180.

1301 Vgl. z.B. SCHMITT, Grey Zones, S. 20.

1302 Dazu, dass Staaten im Diolag um die Etablierung von Völkerrecht zwar wichtige, jedoch nicht die einzigen Akteure sind: ROBERTS/SIVAKUMARAN, S. 89 ff.

liche Konsensfindungen und eine politische Voraussehbarkeit dar. Dennoch könnte es gerade im Zusammenhang um die Frage der Regulierung *unilateraler* Selbsthilfemöglichkeiten im Cyberkontext nach vorliegend vertretener Ansicht einen inhaltlichen Mehrwert bringen, wenn Staaten im Verlauf dieses Prozesses ihre alternative Reaktionsmöglichkeit nutzen, einen völkerrechtlich relevanten Cybervorfall oder daraufhin ergriffene Selbsthilfemassnahmen gegebenenfalls einem internationalen (Schieds-)Gericht zu unterbreiten. Die anhaltenden Versuche, Cyberangriffe völkerrechtlich zu erfassen sowie der subjektiv geprägte Charakter unilateraler Massnahmen lassen einen bedeutenden, objektiv-rechtlichen Beitrag eines einschlägigen (Gerichts-)Urteils im Cyber-Diskurs vermuten. Namentlich könnte eine Betrachtung durch den IGH einen Präzedenzfall schaffen, der einer objektiven Klärung von Auslegungsfragen völkerrechtlicher Selbsthilfenormen dienen kann.[1303] Wie in Art. 92 UN-Charta statuiert, stellt der IGH nämlich das Hauptrechtsprechungsorgan der Vereinten Nationen dar. Zudem hatte der IGH im Zusammenhang mit Gewaltanwendungen bereits in seinem Nicaragua-Urteil ausdrücklich statuiert, dass ihn politische Dimensionen in einer Sache nicht an einer völkerrechtlichen Beurteilung derselben hindern: »*It must be remembered that, as the Corfu Channel case [...] shows, the Court has never shied away from a case brought before it merely because it had political implications or because it involved serious elements of the use of force.*«[1304] Der Gerichtshof hat dadurch explizit auf die *rechtliche* Dimension des Selbstverteidigungsrechts verwiesen.[1305] Darin kann man, wie Kress anführte, eine implizite Bestätigung des berühmten Zitats des Nürnbergtribunals sehen: »*Whether action taken under the claim of self-defense was in fact aggressive or defensive must ultimately be subject to investigation and adjudication if international law is ever to be enforced.*«[1306] Kress geht in diesem Kontext von einem Gefühl einer richterlichen Pflicht aus, vulnerable, doch fundamentale Völkerrechtsregeln (rechtlich) zu konsolidieren.[1307] Der vorlie-

1303 Vgl. Kress, S. 598 (sich darauf beziehend, dass der IGH bisher in dieser Hinsicht wenig Orientierung bietet).

1304 IGH, Nicaragua, Jurisdiktions-Urteil, §96; Kress, S. 565.

1305 IGH, Nicaragua, Jurisdiktions-Urteil, §98; Kress, S. 565.

1306 IMT, Nürnberg-Urteil, S. 207; Kress, S. 565.

1307 Kress, S. 565 f., S. 601. Ähnlich in IGH, Ölplattformen-Urteil, §38. Der IGH hat im Ölplattformen-Urteil, §38 die Darlegung relevanter rechtlicher Aspekte des Selbstverteidigungsrechts (folglich mitunter der Verhältnismässig- und Notwendigkeit) als von »höchster Bedeutung« erachtet, obschon diese für die Entscheidung des Falles an sich nicht mehr erforderlich war. Der Gerichtshof hatte nämlich bereits in §64 einen bewaffneten Angriff verneint, womit sich seine darauffolgenden Ausführungen zur Verhältnismässigkeit strikt gesehen erübrigt hätten. Dazu Raab, S. 726.

genden Einschätzung nach könnte ein ebensolches Verantwortungsgefühl als weitere, massgebliche völkerrechtliche Orientierungshilfe im künftigen, mitunter unilateralen Umgang mit Cyberangriffen (und vergleichbaren transnationalen Risiken) dienen und einen objektiv-rechtlichen Mehrwert im Diskurs schaffen.

3. Stabilisierung der internationalen Ordnung durch die Stärkung kooperationsrechtlicher Verantwortlichkeiten

Das Völkerrecht bietet in vielen Bereichen trotz Interpretationsspielräumen bereits eine historisch gewachsene, hohe Dichte an Orientierungshilfen. Grundsätzlich kann festgehalten werden, dass die Strukturen des Völkerrechts (und damit auch der UN-Charta und des Gegenmassnahmenrechts) auf die Priorisierung friedlicher Streitbeilegungsmechanismen ausgerichtet sind.[1308] Der Ausnahmecharakter der Selbstverteidigung sowie der Kooperationscharakter von Gegenmassnahmen machen deutlich, dass die Möglichkeit eines unilateralen Durchsetzens des Völkerrechts erst subsidiär zu friedlichen Mechanismen und nur in Notsituationen eröffnet werden soll. Dieser strukturellen Begünstigung zwischenstaatlicher Kooperation und (friedlicher) Streitbeilegung mit der Verhältnismässigkeit gewissermassen als letztem Ventil zur Erhaltung dieser übergeordneten Zwecke kann gerade im Cyberkontext eine Schlüsselrolle zukommen. Da eine ausschliesslich reaktive Betrachtung bereits eingetroffener Verletzungen durch Cyberangriffe in den überwiegenden Fällen weder die erstrebte Wiedergutmachung noch eine Abwehr eines völkerrechtlich relevanten, bewaffneten Angriffs ermöglicht, sollte im Kontext der Cybersicherheit eine zunehmende Bedeutung auf der technischen Früherkennung von Cyberangriffen sowie auf der Etablierung effektiver Prozesse zur Schadensverhinderung und -begrenzung liegen. Dazu unabdingbar ist auf technischer Ebene ein frühzeitiger, zwischenstaatlicher sowie auch staatlich-privater Informationsaustausch zu entdeckten Sicherheitslücken und Schadprogrammen. Ein in dieser Hinsicht sicherheitstechnisch relevanter Informationsaustausch kann dabei in weitgehend anonymisierter Form erfolgen,

[1308] Vgl. SCHACHTER, International Law, S. 184: »*The UN Charter deliberately accords priority to the peaceful resolution of disputes rather than to the enforcement of law* (...)«. Ähnlich sieht auch SCHRÖDER, S. 726 die Pflicht zur friedlichen Streitbeilegung der UN-Charta als »ein Grundprinzip der zwischenstaatlichen Beziehungen«. Ähnlich: FRANCK, Recourse to Force, S. 111; SHAW, S. 879. Zum Umschwung des Völkerrechts in Richtung kooperationsrechtlicher Strukturen nach 1945: FRIEDMANN, insb. S. 365 f.; PETERS/KRIEGER/KREUZER, Dissecting the Leitmotif, S. 18. Explizit auch statuiert in Art. 2(3) UN-Charta und Art. 33 UN-Charta. Dazu: HIGGINS/WEBB/AKANDE/SIVAKUMARAN/SLOAN, S. 327, S. 1096.

indem technische Sicherheitsfirmen oder nationale CERTs vor Schadprogrammen oder schädigenden IP-Adressen, die in Netzwerken beobachtet und entdeckt werden, warnen.[1309] Aus der vorliegend völkerrechtlichen Analyse lässt sich dabei schliessen, dass Staaten historisch gesehen grundsätzlich nicht völlig losgelöst von sorgfaltspflichtsrechtlichen Strukturen agieren.[1310] Vor diesem Hintergrund werden sie demzufolge gute Rahmenbedingungen zur Risikominimierung von internationalen Cyberschädigungen schaffen müssen. Bejaht man die völkerrechtliche Due Diligence-Pflicht in Bezug auf Cyberschäden, könnten Staaten im Grunde angehalten werden, zur Verhinderung extraterritorialer Schädigungen legislative und administrative Mindestvorkehrungen zu treffen.[1311] Zumal im Cyberkontext weiterhin ein Grossteil der digitalen Infrastrukturen und Sicherheitsfirmen privat geführt werden, werden solche Regulierungsansätze jeweils auch unter Einbezug und der Ausrichtung auf die Privatwirtschaft erfolgen müssen.[1312] Dabei könnten Mindestmassnahmen bspw. Pflichten umfassen, dass realistische Vorkehrungen gegen die Materialisierung eines bestimmten Risikos zu treffen sind.[1313] Dies kann bspw. durch der Prävention dienende Kooperations-, Melde- und Warnmechanismen geschehen. Der Staat könnte hier mittels einschlägiger Melde- und Warnerfordernisse sinnvolle Anreize für eine breitere Institutionalisierung internationaler

1309 Dabei bestehen auch Informationsaustauschplattformen, die Informationen zu schädigenden Programme der Öffentlichkeit zugänglich machen. Ein Beispiel hierzu ist die technische Platform MISP. Siehe: MISP, Open Source Threat Intelligence Platform and Open Standards For Threat Information Sharing, <https://www.misp-project.org> (zuletzt besucht: März 2023). Technisch ist ein Informieren über schädigende Programme in einem Netzwerk daher grundsätzlich möglich, ohne in ein betroffenes System eindringen zu müssen. Einschlägige datenschutzrechtliche sowie fernmelderechtliche Vorgaben sind dabei weiterhin zu beachten.

1310 Peters/Krieger/Kreuzer, Risk Management Tool, S. 124 u.a. m.V.a. die ILC, Draft Articles on Prevention of Transboundary Harm (2001), deren inhaltliche Ausarbeitung bereits im Jahr 1978 begann und geradezu auf Präventions- und Kooperationspflichten ausgerichtet sind.

1311 Peters/Krieger/Kreuzer unterscheiden dabei zwei überlappende Due Diligence-Typen. Und zwar einerseits prozedurale Pflichten und andererseits die institutionellen Kapazitäten eines Staates: Peters/Krieger/Kreuzer, Risk Management Tool, S. 124. Da die Umsetzung und Ausgestaltung der Due Diligence-Pflicht für den Cyberraum im Einzelnen einer weitergehenden Betrachtung bedürfen, die den hiesigen Rahmen sprengen würde, soll vorliegend in grundsätzlicher Hinsicht auf die substanziellen Beiträge von Krieger/Peters/Kreuzer verwiesen werden.

1312 Es gibt bereits verschiedene Vorschläge für Kooperationsformen zu Attributionszwecken: Mikanagi/Mačák, S. 70 ff. m.V.

1313 Peters/Krieger/Kreuzer, Risk Management Tool, S. 124.

und nationaler Kooperationsmechanismen setzen.[1314] Solche auf Kooperation ausgerichteten Instrumente, die gewisse Risiko- oder Folgeneinschätzungen vorschreiben, können bereits in anderen Bereichen wie dem internationalen Umweltrecht, bei Menschenrechten oder im Bereich der Geldwäschereibekämpfung beobachtet werden.[1315]

Inhaltlich bleibt es aus einer völkerrechtlichen Sicht wichtig zu betonen, dass das Due Diligence-Prinzip vielschichtig ausgestaltet ist und, je nach Kontext, verschiedene Funktionen hat. Es geht, wie bereits betont, jeweils um für einen Staat *zumutbare* und *angemessene* Vorkehrungen zur Verhinderung international verursachter Schädigungen. Da im Hinblick auf die (technische) Verhinderung und Vorbeugung von Cyberschäden noch viele Unklarheiten bestehen, wird auch die Etablierung von sinnvollen regulatorischen Rahmenbedingungen in dieser Hinsicht wohl noch Zeit beanspruchen. So scheinen bspw. Fragen, inwiefern ein Staat im Cyberbereich Kenntnis über schädigendes Verhalten haben können muss oder inwiefern eine solche Kenntnis technisch tatsächlich Sinn macht, Gegenstand weitergehender Diskussionen zu sein. Das Prinzip, an dieser Stelle nur so viel, impliziert insgesamt allerdings weder absolute Überwachungspflichten[1316] noch vermag es entgegenstehende nationale oder internationale Individualrechte wie diejenigen der Privatsphäre und des Datensschutzes ausser Kraft zu setzen. Es geht immer um ein angemessenes, dem jeweiligen Staat und seinen Bürgerinnen und Bürgern institutionell zumutbares und datenschutzkonformes Mass.[1317]

Im internationalen Kontext könnte die Bestätigung einer übergeordneten Due Diligence-Pflicht von Staaten für den Cyberbereich gesamthaft betrachtet zweierlei positive Konsequenzen nach sich ziehen: Einerseits könnte die Klarheit und Voraussehbarkeit gestärkt werden, dass bei einem wissentlichen Untätigbleiben trotz zumutbarer (Verhinderungs-, oder Kooperations-)Möglichkeiten völkerrechtliche Verantwortlichkeiten drohen können. Es ist denkbar, dass Staaten im Rahmen der Due Diligence immerhin dazu angehalten werden, ihr Verhalten oder ihr Nichttätigwerden im Hinblick auf zumutbare Vorkeh-

1314 Peters/Krieger/Kreuzer, Risk Management Tool, S. 124.

1315 Dazu eingehender: Peters/Krieger/Kreuzer, Risk Management Tool, S. 124 (mit konkreten Beispielen).

1316 Näher hierzu: Delerue, Cyber Operations, S. 359 ff.

1317 Vgl. Delerue, Cyber Operations, S. 362 mit Verweis auf das Weiterbestehen nationaler und internationaler Standards sowie auch zur Differenzierung der unterschiedlichen technischen Überwachungsmöglichkeiten von Staaten. Ähnlich: Mikanagi, S. 1037; Peters/Krieger/Kreuzer, Risk Management Tool, S. 124.

rungen zu erklären[1318] und sie damit Einbussen ihrer Glaubwürdigkeit und ihrer politischen Zuverlässigkeit in Kauf nehmen müssten. Dies könnte den normativen Wert der Due Diligence verstärken und gerade auch (insb. *post facto*) Kooperationsanreize fördern. Andererseits würden bei einem Bekenntnis zu einer Due Diligence-Pflicht für Staaten Anreize geschaffen, präventive technische Sicherheits- und Kooperationsstandards im Hinblick auf die eigenen Infrastrukturen zu erhöhen, was insgesamt auch technische Zurückverfolgungsmöglichkeiten verbessern könnte.

Gesamthaft sollte diese Dissertation aufgezeigt haben, dass von Cyberangriffen realistische Risiken transnational und sicherheitspolitisch relevanter Verletzungen ausgehen. In grundsätzlicher Hinsicht kann festgehalten werden, dass die völkerrechtliche Bedeutung und Auseinandersetzung mit dem Due Diligence-Prinzip und damit die Erwartung an Staaten, Sorgfalt walten zu lassen, in verschiedenen Bereichen zunimmt – auch im Cyberkontext.[1319] Die Verhinderung von Gefahren für die internationale Sicherheit sowie die Nichtverletzung anderer souveräner Staaten stellen nämlich – wie von Krieger/Peters/Kreuzer umschrieben – geradezu eine »*raison d'être*« der gesamten internationalrechtlichen Ordnung dar.[1320] Dabei sollte aus den vorangehenden Ausführungen deutlich geworden sein, dass das Due Diligence-Prinzip die Verhinderung einer Materialisierung solcher Risiken in verschiedener Hinsicht fördern kann. Der vorliegenden Einschätzung nach wird in Bezug auf regulatorische und institutionelle Rahmenbedingungen insb. auch im Cyberkontext die Bedeutung einer Stärkung und Klärung von Due Diligence-Verantwortlichkeiten von Staaten weiter wachsen.

Gegenwärtig wurde das Due Diligence-Prinzip seitens der Staatengemeinschaft nur sehr zurückhaltend, wenn überhaupt, explizit bestätigt. Das damit wohl im Grunde zusammenhängende Bedürfnis nach Souveränität und Entscheidungsautonomie scheint dabei nachvollziehbar. Lehnt man die Anwendbarkeit eines Rechts jedoch ab, liegt die Annahme nahe, dass man sich damit einen grösseren Ermessensspielraum vorbehalten möchte, um sich in begründeter Weise rechtlichen Verantwortlichkeiten zu entziehen. Das Due Diligence-Prinzip scheint durch seine Flexibilität allerdings nationale Eigenheiten und Abweichungen gerade eben zuzulassen. Es soll erst dort greifen, wo die (weitgehend zu respektierende) Autonomie zu einer verhinderbaren Fremd-

1318 Ähnliche Entwicklungen gibt es bereits im internationalen Umweltrecht: Sparks/Peters, S. 904 ff., insb. S. 906.

1319 Krieger/Peters, S. 351. Eingehend zu Cyber Due Diligence: Dias/Coco, S. 6 ff.

1320 Peters/Krieger/Kreuzer, Dissecting the Leitmotif, S. 15.

gefährdung wird. Dahingehende Ansichten, dass durch eine zunehmende Bedeutung des Due Diligence-Prinzips ein struktureller Wandel des Völkerrechts stattfinden würde[1321] sind dabei nachvollziehbar. Ebenso sind es Ansichten, gem. derer Staaten durch eine solche Sorgfaltspflicht zunehmend und übermässig für unübersichtliches, privates Verhalten verantwortlich würden. Dennoch ist zu erinnern, dass der IGH im Korfu Kanal-Fall 1949, und damit in seinem ersten Urteil überhaupt, gerade eine solche sorgfaltsrechtliche Pflicht von Staaten definiert hat, Schädigungen vom eigenen Territorium aus und in zumutbarer Weise zu verhindern. Demzufolge müsste eine solche, für die Staaten geltende (und kooperationsrechtlich geprägte) Pflicht im Grunde nicht »neu« bestätigt werden.[1322] Auch die anhaltenden Unklarheiten zur konkreten Anwendung und Ausgestaltung der Due Diligence für den Cyberkontext können daher das Bestehen der Kernfunktion des Prinzips nicht absprechen.[1323] Staaten sind aus völkerrechtlicher Sicht im Umgang mit der Verhinderung transnationaler Verletzungen nicht *per se* frei, sondern bewegen sich grundsätzlich bereits innerhalb eines übergeordneten Rahmens gewohnheitsrechtlich anerkannter Normen der internationalen Staatenverantwortlichkeit. Eine staatliche Due Diligence-Pflicht reiht sich daher insgesamt in die historisch gewachsenen Orientierungshilfen moderner Völkerrechtsstrukturen ein und könnte – bei ihrer (auf Kooperation ausgerichteten) Umsetzung – eine stabilisierende Wirkung auf die internationale Ordnung und (Cyber-)Sicherheit haben.

1321 Krieger/Peters, S. 351 ff.

1322 Akande/Coco/Dias, EJIL Blog vom 05.01.2021. Bereits 1992 zu Konstellationen der Due Diligence-Pflicht: Epiney, S. 205 ff. Zu einem historischen Abriss der Due Diligence: Hessbruegge, S. 265 ff. u.a. m.V.a. Hershey, S. 162 aus dem Jahr 1918.

1323 Mikanagi, S. 1032.

B. Ausblick

Das Völkerrecht hat historisch gesehen vom *ius ad bellum* des 19. Jahrhunderts bis zum heute in Art. 2(4) UN-Charta statuierten Gewaltverbot einen weiten Weg zurückgelegt.[1324] Es kann durchaus als Errungenschaft gesehen werden, dass die Staatengemeinschaft Gewalt – und zwar auch als Selbsthilfe – im Grundsatz ächtet.[1325] Ebenso kann als Errungenschaft erachtet werden, dass mit den Strukturen des Völkerrechts ein Fundament für die Priorisierung friedlicher Streitbeilegung geschaffen wurde. Gesamthaft hat ebendieses völkerrechtliche Gesamtkonstrukt trotz seiner fehlenden zentralisierten Durchsetzungsmacht bisher bereits einen wesentlichen Beitrag zu einer historisch gewachsenen, internationalen Stabilität geleistet und könnte dies – versucht man etwas näher hinzuschauen – weiterhin tun. »Stabilität«, so DIGGELMANN, fällt nämlich »nicht vom Himmel«.[1326] Vielmehr ist sie Ergebnis langwieriger Prozesse sowie eines anhaltenden Aushandelns und Austarierens einer Vielzahl von Interessen, und wird dies wohl auch künftig bleiben.

Die stetige Weiterentwicklung moderner Technologien und die zunehmende Verflechtung hybrider Akteurskonstellationen werden, neben einem Fortschritt für unsere moderne Gesellschaft, weiterhin (neue) sicherheitspolitische Risiken mit sich bringen. Angesichts der sich – simultan neben privaten Kapazitäten – auch stetig militärisch weiterentwickelnden Technologien, werden sich die internationale Staatengemeinschaft und die sich darin bewegenden Akteure weiterhin mit dem zugrundeliegenden Recht auseinandersetzen müssen. Eröffnet man dabei die Möglichkeit unverhältnismässiger Eskalationsspiralen, wenn aus Unbehagen oder Abschreckungsabsichten neue Phänomene mit »Krieg« und militärischer Gewalt beantwortet werden? Oder verschliesst man die Augen vor neuen Entwicklungen, wenn man, an der traditionellen Auslegung von Völkerrechtsnormen festhaltend, veränderten Formen der Gewalt und neuen Akteursformen die Qualität eines Krieges abspricht?[1327]

1324 LESAFFER, S. 35 ff.

1325 KRESS, S. 603.

1326 Dieses Zitat von DIGGELMANN lässt sich auf die internationale Stabilität übertragen, obschon es sich im angeführten Artikel auf die Stabilität *innerstaatlicher* Institutionen bezog. Auffindbar ist es im Interview mit ihm: GJON, Plädoyer vom 20.11.2017, S. 14 f.

1327 MÜNKLER, S. 12.

Jüngere Entwicklungen haben gezeigt, dass sich das Modell herkömmlicher Staatenkriege, die Radien von Interventions- und Schädigungsmöglichkeiten sowie die für die globale Sicherheit relevanten Risiken verändert haben und dies womöglich weiterhin tun werden. Es ist anzunehmen, dass technologische Fortschritte (wie z.B. die Weiterentwicklung Künstlicher Intelligenz oder sog. internet of things-Geräten) unsere Gesellschaft weiterhin fundamental beeinflussen und verändern werden, dass gegenwärtig noch unbekannte technische Risiken erst entdeckt und zusätzlich neue Verletzlichkeiten entstehen werden, während zugleich bei rechtlichen Normen missbrauchsanfällige Graubereiche bestehen bleiben. Es ist anzunehmen, dass die Schädigungsradien technischer Möglichkeiten und auch die Angriffsflächen unserer global vernetzten und interdependenten Wirtschaft noch weiter zunehmen werden – möglicherweise sogar so weit, dass diese zu einem hohen Grad automatisiert und für den Menschen weitgehend unkontrollierbar werden. Es bleibt zu hoffen, dass immerhin die durch Entscheidungsträger beeinflussbaren Risiken – allen voran die Handhabung völkerrechtlicher Ermessensspielräume und völkerrechtlich relevanter Entscheide – kritisch hinterfragt werden (und menschlichen Akteuren vorbehalten bleiben). Gefahren für die internationale Staatengemeinschaft gehen nämlich nicht nur von neuen Technologien aus, sondern – je nach Betrachtung – auch von Entscheidungen, *wie* man auf eine Gefahr oder eine Schädigung reagiert. Die Entscheidung, staatliche (und mitunter militärische) Handlungen als illegitim, legitim, unverhältnismässig oder verhältnismässig und somit als illegal oder gerechtfertigt zu deklarieren, wird bis zu einem gewissen Grad im Auge des Betrachters bleiben – und damit zusammenhängend auch das Verständnis von *Gerechtigkeit*. Auch künftig wird Recht nicht nur gewalteindämmend wirken, sondern – je nach Auslegung – gewisse Handlungen, die gerade im Völkerrecht immense Konsequenzen haben können, auch legitimieren können. Recht kann das Töten von Menschenleben sowie eine Inkaufnahme von Kollateralschäden in einer Konfliktsituation u.U. nicht nur verbieten, sondern auch rechtfertigen. Daher kann das Recht die Legalität von militärischen Massnahmen letztlich nicht nur in Frage stellen, sondern diese auch gerade ermöglichen.[1328] Und die internationale Staatengemeinschaft wird, wie bereits erläutert, weiterhin mit Ermessensspielräumen und Interessenabwägungen arbeiten müssen. Es bleibt die Hoffnung, dass diese Spielräume anhand der vorhandenen völkerrechtlichen Orientierungshilfen und den bereits etablierten, objektiv-rechtlichen Kriterien (mit-

[1328] KENNEDY, S. 41.

unter der Verhältnismässigkeit und des Gewaltverbots) betrachtet werden.[1329] Einerseits umfasst sind dabei die historisch gewachsenen, rechtlichen Grenzen *für* eine (sowohl digital als auch kinetisch lancierte) Gewaltanwendung (»limits *on* force«).[1330] Wie GRAY jedoch überzeugend statuiert, sollten – gerade auch aufgrund ihrer rechtlichen Relevanz – auch die Grenzen *der* Gewaltanwendung (»limits *of* force«) als geeignetes Mittel für eine effektive Verteidigung eines Staates explizit in die Würdigung von Selbsthilfemassnahmen hineinfliessen.[1331] Insbesondere scheinen dahingehende Ansichten, dass gewaltsame Verteidigungshandlungen gegen Cyberangriffe mehr Probleme lösen als schaffen werden, zudem das in Art. 2(3) UN-Charta statuierte Erfordernis der friedlichen Streitbeilegung zu verkennen.[1332] Diese in der UN-Charta statuierte Norm ist als Grundsatz für jede internationale Streitigkeit vorgesehen. Damit geht eine friedliche Streitbeilegung grundsätzlich *jeder* unilateral ergriffenen Selbsthilfemassnahme vor – ob militärisch oder nicht-militärisch, restriktiv oder extensiv verstanden.

Das oft angeführte Unbehagen, dass schwerwiegende internationale Angriffe auf einen Staat und dessen Bevölkerung im System kollektiver Sicherheit keine harten Konsequenzen haben könnten, ist dabei nachvollziehbar. Es ist dennoch daran zu erinnern, dass die Strukturen der völkerrechtlichen Selbsthilfe eben *nicht* auf einen pönalisierenden Umgang mit Völkerrechtsverstössen, sondern vielmehr auf den Erhalt eines internationalen Gleichgewichts zwischen souveränen Staaten ausgerichtet sind. Es fragt sich daher, ob unilaterale, insb. militärische Selbsthilfe ein im Cyberkontext primäres und geeignetes Gefäss sein kann, um Rechtsverletzungen zu adressieren. Diese Zurückhaltung soll dabei die Möglichkeit unilateraler Reaktionen nicht absprechen, wenn diese die letzten, geeigneten Mittel zum Schutz eines Staates oder zur Wiederherstellung der völkerrechtskonformen Lage sind. Die nähere Betrachtung der Verhältnismässigkeit in der vorliegenden Abhandlung und die Erfahrungen aus dem Umgang mit Konflikten in der Vergangenheit[1333] sollten vielmehr aufgezeigt haben, dass staatliche Reaktionen (gerade auch im Cyberkontext) das realistische Potenzial haben, *selbst* zu einer grösseren Ge-

1329 Vgl. das einleitende Zitat von KENNEDY's, Of War and Law: »*may the human freedom of responsible decision be the vocation of our politics*«.

1330 GRAY, The Limits of Force, S. 109.

1331 GRAY, The Limits of Force, S. 109.

1332 GRAY, The Limits of Force, S. 104. Dieser Grundsatz ist ebenfalls festgehalten in der Declaration on Friendly Relations (UN Doc. A/RES/2625 (XXV), S. 123. Zu Art. 2(3) UN-Charta auch: WINGFIELD, S. 83 ff., insb. S. 85.

1333 GRAY, The Limits of Force, S. 109 ff.

fahr für die internationale Gemeinschaft zu werden. Zudem bedeutet eine restriktive Handhabung des völkerrechtlichen Selbsthilferechts nicht, dass keine anderweitigen Rechtswege für den Umgang mit (internationalen) Rechtsverletzungen offenstehen. Einem pönalisierenden Umgang mit Verstössen, der symbolisch durchaus nicht nur für die Politik, sondern auch für die Öffentlichkeit wichtig sein kann, würde von der Natur her wohl eher ein (international-) strafrechlicher Rahmen Abhilfe schaffen. Dabei wird vor dem Hintergrund der Implementierung eines solchen Rahmens künftig wohl auch die völkerrechtliche Due Diligence eine zunehmende Rolle spielen. Ein Staat wird künftig wohl zunehmend zumindest begründen müssen, wenn er im Hinblick auf (strafrechtliche) Investigationen zu von seinem Territorium ausgehenden Cyber-Schädigungen untätig bleibt oder nicht kooperiert.

In der Cybersicherheit (sowie auch im Völkerrecht) wird es immer auch um den Umgang und die Handhabung von Risiken gehen. Wie diese Dissertation aufzuzeigen versucht hat, sollten sich sicherheitspolitische Ziele und Bemühungen daher insgesamt verstärkt auf die *Prävention* von Verletzungen fokussieren. Ein Umgang mit Risiken ist dabei aus völkerrechtlicher Sicht als solcher nicht neu. Nova stellen in diesem Kontext vielmehr die Dimension der Interkonnektivität, die Akkumulierung und die global vernetzten Radien von Cyberrisiken dar, die *gemeinsame* Ansätze eines Risikomanagements unumgänglich machen. Die völkerrechtliche Due Diligence-Norm hat dabei das Potenzial, eine zentrale Bedeutung im Umgang mit sicherheitspolitischen Risiken einzunehmen.[1334] Die Umsetzung ebendieser Norm könnte nicht nur den völkerrechtlichen Kooperationscharakter widerspiegeln, sondern einen solchen Kooperationscharakter für einen künftigen Weg geradezu auch definieren.

Nationale Cyberstrategien und Stellungnahmen sowie die daraus folgenden Einflüsse (mächtiger) Staaten lassen im Hinblick auf die Cyberregulierung gewisse Tendenzen durchblicken. Wohin dies in einem übergeordneten Sinne für den internationalen Diskurs führen wird, bleibt es auszuhandeln. Ansichten zu Auslegungsfragen von Normen werden im Einzelnen wohl auch künftig divergieren. Allerdings – und dies ist eine Haupterkenntnis der vorliegenden Analyse – werden Staaten mit isoliert betrachteten, nationalen Herangehensweisen die Herausforderungen, die sich durch global vernetzte Cybertechnologien und -risiken für die internationale Gemeinschaft stellen, weder unilateral noch im Alleingang lösen können. Für eine nachhaltige Cybersicherheit unabdingbar wird es daher für den künftigen Diskurs sein, einen die (technisch interdependente) Staatengemeinschaft als Ganzes sowie die für die Cybersi-

1334 Peters/Krieger/Kreuzer, Risk Management Tool, S. 121 ff.

cherheit relevanten Akteure inkludierenden und auf Reziprozität und Kooperation ausgerichteten Multilateralismus zu fördern. Dabei sollte diese Dissertation aufgezeigt haben, dass es sich bei dieser Aussage nicht um einen rein pazifistischen Wunsch handelt, sondern diese vielmehr auf einer Dichte von historisch gewachsenen, über Jahrzehnte präzisierten Völkerrechtsauslegungen und -strukturen beruht.

Es bleibt zu hoffen, dass Staaten, um ihre völkerrechtliche Stellung und Glaubwürdigkeit in der internationalen Gemeinschaft nicht zu untergraben, die Beachtung des Völkerrechts auch künftig auf die eine oder andere Art sicherstellen werden. Dabei werden wir, wie MÜNKLER bereits 2003 richtig statuierte, im Hinblick auf neue Kriege und die internationale Sicherheit – sowie angesichts absehbarer weiterer, fundamenaler technologischer Umbrüche – im 21. Jahrhundert wohl in bewegte Zeiten hineinkommen.[1335]

[1335] MÜNKLER, bereits in seiner 4. Aufl. 2003, S. 243.

Curriculum Vitae

Sara Pangrazzi erlangte ihren Bachelor und Master of Law an der Universität Zürich. Dabei absolvierte sie im Rahmen ihres Masters ein Austauschsemester an der Universität New South Wales in Sydney. Im Anschluss an das Studium arbeitete sie von 2018–2020 als wissenschaftliche Assistentin am Lehrstuhl für Völkerrecht, Europarecht, Öffentliches Recht und Staatsphilosophie von Prof. Dr. iur. Diggelmann. Während ihrer Zeit als Doktorandin an der Universität Zürich bildete sie sich zudem im Datenschutz und der Informationssicherheit weiter und war am Forschungsprojekt der Digital Society Initiative der Universität Zürich zur »Schaffung eines ethischen und rechtlichen Governance-Rahmens für vertrauenswürdige Cybersicherheit in der Schweiz« beteiligt. Sie war ausserdem Gastforscherin am Lauterpacht Center for International Law der Universität Cambridge (UK), am the Hague Program for Cybernorms der Universität Leiden sowie am Woodrow Wilson Center for Scholars in Washington D.C. Seit 2022 ist sie als Juristin am Bundesamt für Justiz tätig, wo sie unter anderem als Teil der Schweizer Delegation an den internationalen Verhandlungen des Ad Hoc Committee zu einer UNO-Cybercrime Konvention mitwirkt und Schweizer Vertreterin im Cybercrime Convention Committee, dem Expertengremium der Budapester Cybercrime Konvention des Europarats, ist.

Cyberangriffe sind eine Folge des rasanten technologischen Fortschritts und werden zu den grössten sicherheitspolitischen Herausforderungen des 21. Jahrhunderts gezählt. Sie können weltweit zu erheblichen ökonomischen und physischen Schäden führen. Was bedeutet dies für die internationale Staatengemeinschaft? Wann und wie dürfen Staaten auf Cyberangriffe reagieren, ohne das Völkerrecht zu verletzen? Gegenstand dieser Dissertation ist eine Aufarbeitung der völkerrechtlichen Zulässigkeit staatlicher Selbsthilfemöglichkeiten bei Cyberangriffen. Ein besonderer Fokus liegt dabei auf der Verhältnismässigkeit von (digitalen) Verteidigungs- und Gegenmassnahmen. Die Dissertation zeigt insgesamt auf, weshalb für einen erfolgreichen Schutz vor Cyberangriffen ein präventiv ausgerichtetes, internationales Risikomanagement und zwischenstaatliche Kooperation nicht nur technisch, sondern auch rechtlich betrachtet zentral bleiben.