Völkerrechtliche Schwierigkeiten einer effektiven Bekämpfung von Cyber-Angriffen

Stephan Hobe, Martin Schwamborn

Einleitung

Dass die vielfach verwendete Cybertechnologie nicht nur neue Chancen eröffnet, indem sie etwa autonomes Fahren, Fliegen und Ähnliches ermöglicht, ist spätestens klar geworden, seitdem es Cyberangriffe auf Estland im Jahre 2007, auf Georgien im Jahre 2008, auf den Iran im Jahre 2010,[1] auf den Deutschen Bundestag im Jahre 2017[2] sowie auf das Universitätsklinikum in Düsseldorf im Jahre 2020[3] gegeben hat. Auch der völkerrechtswidrige Angriffskrieg Russlands gegen die Ukraine[4] wird zwar in erster Linie konventionell geführt, gleichzeitig aber von Anfang an durch umfassende Cyberoperationen flankiert.[5] Schon vor Beginn des russischen Überfalls auf die Ukraine haben sämtliche Großmächte Cyberspace nicht nur als neue Dimension, sondern auch als neue Domäne der Kriegführung betrachtet. Viele Staaten, unter anderem die USA, Russland, China, das Vereinigte Königreich, Israel, Deutschland, aber auch Nordkorea, haben eigene Cybereinheiten ins Leben

1 Zu diesen und weiteren Beispielsfällen siehe *J. Dornbusch*, Das Kampfführungsrecht im internationalen Cyberkrieg, Baden-Baden 2018, S. 31 ff. sowie *C. Focarelli*, Self-defence in cyberspace, in: N. Tsagourias/R. Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl., Sheffield 2021, S. 317, 321 ff. sowie *J.-C. Woltag*, Cyber Warfare, Military Cross-Border Computer Network Operations under International Law, Cambridge (u.a.) 2014, S. 47 ff.

2 „Erneuter Hackerangriff auf Rechner von Abgeordneten", Zeit Online (29.03.2017), abrufbar unter: https://www.zeit.de/politik/deutschland/2017-03/bundestag-hackerangriff-verfassungsschutz-netzsicherheit?utm_referrer=https%3A%2F%2Fwww.google.com%2F (zuletzt abgerufen: 23.02.2023).

3 Pressemitteilung des Universitätsklinikums Düsseldorf vom 17.09.2020, abrufbar unter: https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf (zuletzt abgerufen: 23.02.2023).

4 Allgemein siehe nur *S. Schmahl*, Völker- und europarechtliche Implikationen des Angriffskriegs auf die Ukraine, NJW 2022, 969.

5 Einen aktuellen Überblick bietet die Zeitleiste des CyberPeace Insitute, abrufbar unter: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline (zuletzt abgerufen: 23.02.2023).

gerufen, die sich vor allem mit der Abwehr entsprechender Angriffe befassen. Allein für Deutschland sei nur die Errichtung des Nationalen Cyber-Abwehrzentrums im Jahre 2011 sowie die Aufstellung des Organisationsbereichs Cyber- und Informationsraum (CIR) der Bundeswehr im Jahre 2017 mit seinem Kommando Cyber- und Informationsraum in Bonn genannt.[6] Infolge des Ukraine-Krieges wurde jüngst von Bundesinnenministerin *Nancy Faeser* auch eine Debatte über eine Grundgesetzänderung angestoßen, die dem Bund zusätzliche Kompetenzen zur Abwehr von Cyberattacken inklusive der Möglichkeit aktiver Gegenangriffe, sogenannter „Hackbacks", einräumen soll.[7]

Mit den verschiedenen Formen von Attacken auf Computerbetriebssysteme durch Viren, Würmer, Trojanische Pferde, Logische Bomben, Backdoor oder Denial of Service-Attacken ist die Variationsbreite möglicher Angriffe enorm.[8] Als einführendes Beispiel für Auswirkungen und Probleme, die mit Cyberangriffen sowohl in faktischer als auch in völkerrechtlicher Hinsicht verbunden sind, soll an dieser Stelle der Computerwurm Stuxnet dienen. Bei Stuxnet handelt es sich um ein Schadprogramm, welches gezielte Angriffe auf ein bestimmtes System zur Überwachung und Steuerung technischer Prozesse ermöglicht.[9] Genau dieses SCADA-System (aus dem Englischen, Supervisory Control and Data Acquisition), die Simatic S7, wurde unter anderem auch zur Steuerung von Zentrifugen zur Urananreicherung in der iranischen Atomanlage Natanz verwendet. Stuxnet manipulierte die Rotationsgeschwindigkeit der hochsensiblen Zentrifugen, was die iranische Urananreicherung empfindlich gestört und langfristig zu einer Zerstörung von etwa 1000 der 9000 Zentrifugen in Natanz geführt hat. Wer den Computerwurm in die iranische Atomanlage eingeschleust hat, ist nach wie vor

6 Dazu https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum (zuletzt abgerufen: 23.02.2023); im Überblick zu anderen Ländern siehe *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015, S. 14 f.

7 *D. Neuerer*, Ukraine-Krieg: Regierungspläne für Cyber-Gegenangriffe stoßen auf Ablehnung, Handelsblatt vom 04.04.2022, abrufbar unter: https://www.handelsblatt.com/politik/deutschland/hackerattacken-ukraine-krieg-regierungsplaene-fuer-cyber-gegenangriffe-stossen-auf-ablehnung/28225644.html?nlayer=Themen_11804704, (zuletzt abgerufen: 23.02.2023). Allgemein zu Hackbacks von Staaten *H. Lahmann*, "Hacking Back" by States and the Uneasy Place of Necessity within the Rule of Law, ZaöRV (80) 2020, 453.

8 Zu den verschiedenen Angriffsformen siehe *Dornbusch*, Kampfführungsrecht (Fn. 1), S. 30 f. sowie *Schulze*, Cyber-„War" (Fn. 6), S. 24 f.

9 Zum Stuxnet-Fall siehe nur *Woltag,* Cyber Warfare (Fn. 1), S. 47 ff.

nicht endgültig geklärt. Zwar gehen Experten wegen der Komplexität der Schadsoftware davon aus, dass die handelnden Personen Unterstützung von staatlicher Seite hatten, wobei insbesondere die USA und Israel genannt werden, doch ist die Verantwortung bis heute offen.

Der Stuxnet-Fall weist damit zwei Charakteristiken auf, die für Cyberangriffe typisch sind. Zum einen kann ein vermeintlich harmloses Computerprogramm große Schäden verursachen, was zwangsläufig zur Frage nach möglichen Gegenmaßnahmen führt. Zum anderen ist oftmals nicht oder jedenfalls nicht innerhalb kurzer Zeit zu ermitteln, von wo und vor allem durch wen der Angriff verübt wurde. Vergleichbare Szenarien wie im Stuxnet-Fall, also Angriffe auf kritische Infrastruktur wie Strom- und Wasserversorgung, Krankenhäuser oder Telekommunikationseinrichtungen können jederzeit auch die Bundesrepublik Deutschland oder einen NATO-Bündnispartner treffen.[10] Infolge des Ukraine-Krieges geht das Bundesamt für Sicherheit in der Informationstechnik (BSI) zurzeit von einer „erhöhte[n] Bedrohungslage für Deutschland" aus,[11] weshalb sich die Frage nach der völkerrechtlichen Einordnung derartiger Cyberangriffe besonders deutlich aktualisiert.

Ein besonderer Fokus soll hier auf dem Recht der Selbstverteidigung liegen. Zur besseren Einordnung ist der Beitrag in zwei Teile gegliedert. Den Anfang macht ein allgemeiner Überblick zu den rechtlichen Grundlagen und Voraussetzungen des Selbstverteidigungsrechts souveräner Staaten, einschließlich seiner Stellung im allgemeinen Völkerrecht (A.). Anschließend werden die Herausforderungen für das Selbstverteidigungsrecht beleuchtet, die sich aus den Charakteristiken des Cyberspace und der dortigen Angriffsformen ergeben (B.).

10 Vgl. BMVg, Broschüre der Bundeswehr zu Landes- und Bündnisverteidigung, Juli 2020, S. 14, abrufbar unter: https://www.bundeswehr.de/resource/blob/2338734/8bcff03f523a3962a028ef20484f3f0b/download-broschuere-de-data.pdf; BMI, Cybersicherheitsstrategie für Deutschland, 2016, S. 38 ff., abrufbar unter: https://www.bundeswehr.de/resource/blob/89756/6b2dcb8af248db01ea3e338d8a54e8bb/cybersicherheitsstrategie-data.pdf; zur Cyberabwehr Deutschlands in der NATO siehe BMVg, Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, S. 65, abrufbar unter: https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf (alle Links zuletzt abgerufen: 23.02.2023).

11 BSI, Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine, Pressemitteilung vom 12.05.2022, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html (zuletzt abgerufen: 23.02.2023).

A. Grundlagen und Einordnung des Selbstverteidigungsrechts souveräner Staaten nach Art. 51 UN-Charta

Um die Besonderheiten und Herausforderungen für das Selbstverteidigungsrecht gegenüber Cyberangriffen vollständig erfassen zu können, kommt man nicht umhin, die völkerrechtlichen Grundlagen des in Art. 51 UN-Charta verankerten Selbstverteidigungsrechts zu betrachten. Ausgangspunkt ist Art. 2 Ziff. 1 UN-Charta, wonach die Organisation der Vereinten Nationen auf dem Grundsatz der souveränen Gleichheit aller ihrer Mitglieder beruht. Die sogenannte *Friendly Relations Declaration* der UN-Generalversammlung vom 24. Oktober 1970 hat diesen „Grundsatz der souveränen Gleichheit der Staaten" wie folgt konkretisiert:

> „Alle Staaten genießen souveräne Gleichheit. Sie haben gleiche Rechte und Pflichten und sind ungeachtet wirtschaftlicher, sozialer, politischer oder anderer Unterschiede gleichberechtigte Mitglieder der internationalen Gemeinschaft."[12]

Abgesichert wird die souveräne Gleichheit aller Mitgliedstaaten der UN durch verschiedene völkerrechtliche Grundprinzipien, die weitgehend auch in Art. 2 UN-Charta festgehalten sind. Für die hier relevante Frage nach dem Umgang mit Cyber*angriffen* ist neben dem sogenannten Interventionsverbot, auf das noch zurückzukommen sein wird, insbesondere das Gewaltverbot von Interesse.[13] Nach Art. 2 Ziff. 4 UN-Charta unterlassen alle Mitglieder in ihren internationalen Beziehungen jede gegen die territoriale Unversehrtheit oder die politische Unabhängigkeit eines Staates gerichtete oder sonst mit den Zielen der Vereinten Nationen unvereinbare Androhung oder Anwendung von Gewalt. Entsprechend seiner Funktion zur Sicherung des Welt-

12 UN Generalversammlung, Erklärung über Grundsätze des Völkerrechts betreffend freundschaftlicher Beziehungen und Zusammenarbeit zwischen den Staaten im Einklang mit der Charta der Vereinten Nationen, A/RES/2625 (XXV) vom 24.10.1970; zur rechtlichen Einordnung siehe nur *H. Keller*, Friendly Relations Declaration, MPEPIL, abrufbar unter https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e938?rskey=2SnJUn&result=1&prd=MPIL (zuletzt abgerufen 23.02.2023).

13 Zu den Grundprinzipien der zwischenstaatlichen Beziehungen siehe nur *M. Herdegen*, Völkerrecht, 20. Aufl., München 2021, S. 267 ff.; *S. Hobe*, Einführung in das Völkerrecht, 11. Aufl., Tübingen 2020, S. 205 ff.; allgemein zur Einordnung von Cyberoperationen als Verstoß gegen das Gewaltverbot *M. Roscini*, Cyber operations as a use of force, in: N. Tsagourias/R. Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl., Cheltenham 2021, S. 297 (301 ff.).

friedens untersagt Art. 2 Ziff. 4 UN-Charta jede Form der Gewaltanwendung. Ohne bereits an dieser Stelle ins Detail gehen zu wollen, können vom Gewaltverbot neben dem klassischen Anwendungsfall der militärischen Gewalt im Sinne einer Waffenanwendung gegen das Hoheitsgebiet oder die Streitkräfte eines anderen Staates auch Maßnahmen unterhalb der Schwelle eines Krieges, wie beispielsweise die Entsendung bewaffneter Rebellengruppen oder Banden, fallen.[14] Auf diese letzte Fallgruppe und den in diesem Zusammenhang relevanten *Nicaragua*-Fall des Internationalen Gerichtshofs[15] wird noch im späteren Verlauf des Beitrags zurückzukommen sein.

An dieser Stelle genügt es zunächst einmal festzuhalten, dass Art. 2 Ziff. 4 UN-Charta jede Form der Gewaltanwendung zwischen den Staaten untersagt und dass die UN-Charta nur zwei Ausnahmen von diesem Grundsatz kennt.[16] Ausdrücklich vom Gewaltverbot ausgenommen sind zum einen Maßnahmen der kollektiven Sicherheit nach Art. 39 bis 50 UN-Charta, also Handlungen des UN-Sicherheitsrats zur Friedenssicherung. Die zweite Ausnahme bildet das Selbstverteidigungsrecht der Staaten. Der insoweit relevante Art. 51 UN-Charta beinhaltet folgende Regelung:

> „Diese Charta beeinträchtigt im Falle eines bewaffneten Angriffs gegen ein Mitglied der Vereinten Nationen keineswegs das naturgegebene Recht zur individuellen oder kollektiven Selbstverteidigung, bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat. Maßnahmen, die ein Mitglied in Ausübung dieses Selbstverteidigungsrechts trifft, sind dem Sicherheitsrat sofort anzuzeigen; sie berühren in keiner Weise dessen auf dieser Charta beruhende Befugnis und Pflicht, jederzeit die Maßnahmen zu treffen, die er zur Wahrung oder Wiederherstellung des Weltfriedens und der internationalen Sicherheit für erforderlich hält."

Bereits dem Wortlaut von Art. 51 UN-Charta lassen sich verschiedene Anforderungen und Grenzen des staatlichen Selbstverteidigungsrechts entneh-

14 Dazu *Hobe*, Völkerrecht (Fn. 13), S. 207 f.; ausf. zum Gewaltbegriff des Art. 2 Ziff. 4 UN-Charta auch *A. Randelzhofer/O. Dörr* in: Simma/Khan/Nolte/Paulus, The Charter of the United Nations, A Commentary, 3. Aufl., Oxford 2012, Art. 2 (4) Rn. 14 ff.

15 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, insb. § 195.

16 Der Ausnahme über die sog. Feindstaatenklausel nach Art. 53 und 107 UN-Charta kommt nach einhelliger Auffassung keine Bedeutung mehr zu. Dazu nur *Randelzhofer/Dörr* in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 2 (4) Rn. 45 m.w.N.

men.[17] Nicht zuletzt, um Wiederholungen im zweiten Teil des Beitrags zu vermeiden, geht es an dieser Stelle nur darum, einen Überblick zu den einzelnen Voraussetzungen und den damit verbundenen Problemen zu geben, die sich bei der Reaktion auf Cyberattacken stellen.

Ausgangspunkt und Grundvoraussetzung des Selbstverteidigungsrechts ist das Vorliegen eines „bewaffneten Angriffs" auf einen Mitgliedstaat der Vereinten Nationen. Während ein konventioneller, das heißt in diesem Zusammenhang vor allem analoger Militärschlag eines Staates gegen das Territorium oder die Streitkräfte eines anderen Staates regelmäßig ohne Weiteres als „bewaffneter Angriff" eingeordnet werden kann, ist die Lage bei Cyberattacken, die jedenfalls im Ausgangspunkt im rein digitalen Raum ablaufen, nicht immer eindeutig. Hinzu kommt, dass der „bewaffnete Angriff" von einem anderen Staat ausgehen oder diesem jedenfalls zurechenbar sein muss. Stellt die Frage der Zurechnung von Handlungen privater Akteure an Staaten das Völkerrecht in Zeiten des internationalen Terrorismus schon bei analogen Angriffen vor nicht unerhebliche Herausforderungen, kommt bei Cyberattacken das Problem der schwierigen – wenn nicht sogar unmöglichen – technischen Rückverfolgbarkeit hinzu. Mit anderen Worten: Der Verursacher kann regelmäßig nicht ermittelt werden. Auch die weiteren Voraussetzungen bzw. die Grenzen des völkerrechtlichen Selbstverteidigungsrechts können im Einzelfall mit nicht unerheblichen Schwierigkeiten verbunden sein. So muss die Selbstverteidigung der Abwehr eines *gegenwärtigen* Angriffs dienen und die ergriffenen Verteidigungsmaßnahmen müssen verhältnismäßig sein. Insbesondere wenn man die schwierige und unter Umständen langwierige Rückverfolgung von Cyberattacken betrachtet, kann das Kriterium der Gegenwärtigkeit des Angriffs bzw. der Unmittelbarkeit der Verteidigung problematisch sein. Unter dem Gesichtspunkt der Verhältnismäßigkeit ist insbesondere zu diskutieren, welche Reaktionen auf Cyberattacken möglich und vor allem angemessen sind. Neben diesen quantitativen und qualitativen Anforderungen an das Selbstverteidigungsrecht kommt noch eine weitere zeitliche Grenze hinzu. So muss die Selbstverteidigung sofort dem UN-Sicherheitsrat angezeigt werden und das Recht zur Selbstverteidigung endet spätestens, wenn der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat. In der Anzeigepflicht kommt die rechtliche Subsidiarität des Selbstverteidi-

17 Zu den Anforderungen siehe nur *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 16 ff. m.w.N. sowie sogleich ausf. unter B. II.

gungsrechts gegenüber Maßnahmen des UN-Sicherheitsrats zur kollektiven Sicherheit zum Ausdruck.

Bevor im zweiten Teil des Beitrags die einzelnen Voraussetzungen und Grenzen ausführlicher erläutert und hinsichtlich ihrer Anwendbarkeit auf Cyberattacken einer kritischen Betrachtung unterzogen werden, gilt es im allgemeinen Teil mit dem Interventionsverbot noch ein weiteres völkerrechtliches Grundprinzip für die zwischenstaatlichen Beziehungen zu behandeln. Wie soeben geschildert, ist die Grundvoraussetzung des Selbstverteidigungsrechts das Vorliegen eines „bewaffneten Angriffs". Wie zu zeigen sein wird, sind gerade im Bereich des Cyberspace nicht wenige Szenarien denkbar, die man umgangssprachlich als „Hacker-*Angriff*" einordnen würde, die im juristischen Sinne aber nicht die Schwelle des „bewaffneten Angriffs" nach Art. 51 UN-Charta bzw. die Schwelle des Gewaltverbots aus Art. 2 Ziff. 4 UN-Charta überschreiten. Dies schließt zwar die Möglichkeit zur Selbstverteidigung aus, stellt den betroffenen Staat aber nicht vollkommen schutzlos. Es kommt nämlich nach wie vor ein Verstoß gegen das völkerrechtliche Interventionsverbot in Betracht.

Das Interventionsverbot schließt eine Einmischung in innere Angelegenheiten eines anderen Staates aus. So untersagt Art. 2 Ziff. 7 UN-Charta, außer im Falle von Maßnahmen der kollektiven Sicherheit, ein Eingreifen der Vereinten Nationen in „Angelegenheiten, die ihrem Wesen nach zur inneren Zuständigkeit eines Staates gehören". Doch nicht nur für die Vereinten Nationen ist ein solcher Eingriff ausgeschlossen. Auch zwischen den Mitgliedstaaten besteht ein allgemeines Interventionsverbot. Der Internationale Gerichtshof hat im *Nicaragua*-Fall die Geltung des Interventionsverbots als Satz des Völkergewohnheitsrechts unter Bezugnahme auf die bereits angesprochene *Friendly Relations Declaration* ausdrücklich anerkannt.[18] Eine verbotene Intervention setzt voraus, dass eine Einmischung in die inneren Angelegenheiten eines Staates vorliegt, die unter Androhung oder Anwendung von Zwang erfolgt ist.[19] Als innere Angelegenheiten gelten jene Bereiche, die dem Staat vorbehalten sind (sog. *domaine reservé*), wozu der Internationale Gerichtshof die Wahl des politischen, wirtschaftlichen, sozialen und kulturellen

18 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, § 202.

19 Ausführlich zum Interventionsverbot *U. Scheuner*, Intervention und Interventionsverbot, Zeitschrift für die Vereinten Nationen 5/1980, 149.

Systems sowie die Formulierung der auswärtigen Politik gezählt hat.[20] Problematischer ist demgegenüber, wann eine bestimmte Handlung als verbotener Zwang einzuordnen ist. Dass eine Cyberattacke, die keinen „bewaffneten Angriff" im Sinne des Art. 51 UN-Charta darstellt, einen Verstoß gegen das Interventionsverbot begründen kann, ist allerdings alles andere als von vornherein ausgeschlossen. Natürlich stellen sich auch hier die bereits angesprochenen Probleme der Rückverfolgbarkeit und Zurechnung sowie der Angemessenheit einer staatlichen Gegenmaßnahme. Dennoch bietet auch das Interventionsverbot einen völkerrechtlichen Anknüpfungspunkt für einen Umgang mit Cyberattacken, weshalb im weiteren Verlauf des Beitrags auch darauf noch ausführlicher einzugehen sein wird.

B. Cyberangriffe als Herausforderung für das Selbstverteidigungsrecht

Im Anschluss an den kurzen Überblick über die völkerrechtlichen Grundlagen des Selbstverteidigungsrechts können nun die Herausforderungen in den Blick genommen werden, die mit den schier unbegrenzten Angriffsmöglichkeiten im Cyberspace und ihren Auswirkungen einhergehen. Um diese nicht nur zu erfassen, sondern möglichst auch völkerrechtlich zu bewältigen, muss zunächst eine wichtige Vorfrage geklärt werden. Ausgangspunkt der Überlegungen muss selbstverständlich die Frage sein, was unter Cyberspace und Cyberattacken zu verstehen ist und vor allem, ob und wenn ja unter welchen Voraussetzungen beide Phänomene einer völkerrechtlichen Erfassung und Regelung zugänglich sind. In keinem Fall darf Cyberspace als „Wilder Westen" oder gar „rechtliches Niemandsland" angesehen werden.[21] Vielmehr können die Regeln des analogen Völkerrechts grundsätzlich auch im digitalen Raum zur Anwendung gebracht werden.[22] Welche Herausforderungen sich dabei stellen bzw. ob und wie die analogen Regelungen unter

20 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, § 205; s.a. UN, A/RES/2625 (XXV) vom 24.10.1970.

21 Ausdrücklich gegen eine Einordnung als „völkerrechtliches Niemandsland" auch *W. Heintschel von Heinegg*, Cyberspace – Ein völkerrechtliches Niemandsland?, in: R. Schmidt-Radefeldt/C. Meissler (Hrsg.), Automatisierung und Digitalisierung des Krieges, Drohnenkrieg und Cyberwar als Herausforderung für Ethik, Völkerrecht und Sicherheitspolitik, Baden-Baden 2012, S. 159 (159 f.).

22 Dazu *A. v. Arnauld*, Völkerrecht, 4. Aufl., Heidelberg 2019, S. 389 ff. Rn. 859 ff., insb. S. 392 ff. Rn. 864 ff.; *D. J. Svantesson*, A New Jurisprudential Framework for Jurisdiction, AJIL Unbound 109 (2015), 69; *S. Schmahl*, Zwischenstaatliche Kompetenzabgrenzung

Umständen angepasst oder modifiziert werden müssen, soll im Folgenden untersucht werden.

I. Ausgangspunkt: Cyberspace und Völkerrecht

Was ist also Cyberspace und warum stellt er das Völkerrecht vor besondere Herausforderungen? Eine allgemeinverbindliche völkerrechtliche Definition von Cyberspace gibt es bislang nicht. Als Begriff taucht „Cyberspace" zum ersten Mal in zwei Science-Fiction-Werken von William Gibson auf, die 1982 und 1984 erschienen sind.[23] Umschreiben lässt sich Cyberspace am ehesten als „der virtuelle Raum, der durch die entsprechenden Verbindungen zwischen Sender und Empfänger und deren Computer hergestellt wird" oder aber als „kommunikativer Raum zwischen Computern und fließenden Netzwerken".[24] Eine ganz ähnliche Definition findet sich im Glossar der Cybersicherheitsstrategie für Deutschland des Bundesministeriums des Inneren, für Bau und Heimat (BMI) aus dem Jahr 2021:

> „Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann."[25]

Als virtueller und durch weltweite Vernetzung geprägter Raum zeichnet sich Cyberspace insbesondere durch seine Ubiquität, also seine Ungebundenheit an einen bestimmten Standort aus. Obwohl einzelne Aspekte des virtuellen Raums wie beispielsweise Standorte von Computern oder Servern lokalisierbar sind, liegt der eigentliche Kern des Cyberspace in seiner dezentralen Vernetzung. Während im Völkerrecht klassischerweise eine Anknüpfung an staatliche Territorien und dem damit verbundenen Regelungsanspruch des

---

im Cyberspace, AVR 47 (2009), 284 (291 ff.); s.a. *R. Uerpmann-Wittzack,* GLJ 11 (2010), 1245 (1258).

23 *W. Gibson*, Burning Chrome, New York 1982; *W. Gibson*, Neuromancer, New York 1984; zur Urheberschaft Gibsons siehe *Hobe*, Völkerrecht (Fn. 13), S. 428.

24 *Hobe*, Völkerrecht (Fn. 13), S. 428.

25 BMI, Cybersicherheitsstrategie für Deutschland 2021, S. 133, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf (zuletzt abgerufen am 23.02.2023).

jeweiligen Staates möglich ist,[26] können im Cyberspace Ursprung, Zwischenstationen und Effekt einer Handlung räumlich weit auseinanderfallen und dennoch innerhalb kürzester Zeit verschiedene Staaten betreffen.[27] Um es mit den Worten des Völkerrechtlers *Andreas von Arnauld* zu sagen: „Der virtuelle Raum des Cyberspace und der geographische Raum des Staates überlappen sich, passen aber nicht aufeinander."[28]

Wie bereits gesagt, sollte Cyberspace aber nicht vorschnell als völkerrechtliches „Niemandsland" eingeordnet werden. Vielmehr geben die Staaten ihre grundsätzlich umfassenden Regelungsansprüche für das eigene Territorium auch im Angesicht von Cyberspace nicht auf.[29] In Bezug auf das völkerrechtliche Selbstverteidigungsrecht nennen beispielsweise die Vereinigten Staaten in der *National Cyber Strategy* von 2018 ausdrücklich auch militärische Mittel als mögliche Antwort auf Cyberattacken.[30] Auch NATO-Generalsekretär *Jens Stoltenberg* hat keinen Zweifel daran gelassen, dass die NATO den Cyberspace als Domäne der Kriegführung auffasst und bereit ist, bei schweren Cyberattacken auch Maßnahmen der kollektiven Selbstverteidigung zu ergreifen.[31] Inwieweit diese erklärte Bereitschaft auch auf eine völkerrechtliche Grundlage gestützt werden kann, gilt es noch im Einzelnen zu klären. Zuvor muss aber noch einmal das Bewusstsein für die zentrale Herausforderung geschärft werden, mit der sich das Völkerrecht bei Cyberoperationen konfrontiert sieht.

---

26 *O. Diggelmann/N. Hadorn*, Gewalt- und Interventionsverbot bei Cyberangriffen, Ausgewählte Schlüsselfragen, in: C. Schubel/S. Kirste/P. C. Müller-Graff/M. Diggelmann/U. Hufeld (Hrsg.), Jahrbuch für Vergleichende Staats- und Rechtswissenschaften – 2016/2017, Baden-Baden, S. 255 (260); zu Fragen der Souveränität und Cyberspace siehe nur *N. Tsagourias*, legal status, in: N. Tsagourias/R. Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl., Cheltenham 2021, S. 9 ff.; allgemein zum Umgang mit Entterritorialisierungstendenzen siehe *K. Schmalenbach*, VVDStRL 76 (2017), 245 sowie *J. Bast*, VVDStRL 76 (2017), 277 (289 ff.).

27 Dazu nur *v. Arnauld*, Völkerrecht (Fn. 22), S. 389 Rn. 859; allgemein zum Umgang mit Entterritorialisierungstendenzen im Unions- und Völkerrecht siehe *K. Schmalenbach*, VVDStRL 76 (2017), 245 sowie *J. Bast*, VVDStRL 76 (2017), 277 (289 ff.).

28 *A. v. Arnauld*, Völkerrecht (Fn. 22), S. 389 Rn. 859.

29 *S. Shackleford/A. Craig*, Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity, in: StanfordJIL 50 (2014), 114. Zu den möglichen Anknüpfungspunkten siehe die Nachweise in Fn. 22.

30 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 abgerufen: 23.02.2023).

31 *J. Stoltenberg*, Nato will defend itself, in: Prospect, Cyber resilience vom 27.08.2019, abrufbar unter: https://www.prospectmagazine.co.uk/world/nato-will-defend-itself-summit-jens-stoltenberg-cyber-security (zuletzt abgerufen: 23.02.2023).

Cyberspace stellt das herkömmliche territoriale oder raumbezogene Denken im Völkerrecht deshalb vor Probleme, weil er sich aufgrund seiner Ubiquität der Zuordnung zu einer raumbezogenen staatlichen Jurisdiktionsgewalt jedenfalls in Teilen zu entziehen scheint. So banal diese Feststellung klingt: Die eigentliche Schwierigkeit im Umgang mit Cyberoperationen in völkerrechtlicher Hinsicht liegt in der fehlenden räumlichen Zuordnung. Dies lässt sich anhand eines einfachen Vergleichs von konventionellen und virtuellen Angriffen verdeutlichen. Konventionelle Militärschläge eines Staates A auf das Territorium eines Staates B lassen sich regelmäßig ohne Weiteres völkerrechtlich einordnen. Gleiches gilt für die Frage des Selbstverteidigungsrechts. Die Tatsache, dass moderne Kriegführung über Telekommunikations- oder Zielführungssysteme in weiten Teilen computergestützt abläuft, macht einen konventionellen Militärschlag noch nicht zu einer für die völkerrechtliche Einordnung problematischen Cyberoperation. Gleiches gilt für einen konventionellen Angriff auf Telekommunikations- oder sonstige IT-Einrichtungen. Die eigentliche Herausforderung für das Völkerrecht besteht in einem Angriff, der – ungeachtet seiner möglichen Auswirkungen auf die reale Welt – vollständig im oder durch den digitalen bzw. virtuellen Raum abläuft. Besonderes Augenmerk muss deshalb auf jenen Operationen liegen, „die Wirkungen *im* oder *durch* den Cyberraum zeitigen oder zu zeitigen bestimmt sind."[32] Wie bereits eingangs erwähnt, ist die Bandbreite möglicher Angriffe auf bzw. durch Computerbetriebssysteme mittels Viren, Würmern, Trojanischen Pferden, Logischen Bomben, Backdoor oder Denial of Service-Attacken enorm.[33] Eine ganz andere Frage ist es aber, ob derartige „Hacker-*Angriffe*" auch in völkerrechtlicher Hinsicht als Angriff einzuordnen sind, der eine entsprechende staatliche Reaktion im Wege einer militärischen Selbstverteidigung rechtfertigen würde.

32 *W. Heintschel von Heinegg*, Völkerrechtliche Fragen im Cyber- und Informationsraum, Verteidigungsausschuss des Deutschen Bundestags, Öffentliche Anhörung vom 14. Dezember 2018, Ausschussdrucksache 19(12)941 vom 08.12.2020 – 19/3494 5410, S. 1 ff.; zum Begriff des Cyber-Angriffs s.a. *R. Nguyen*, Navigating Jus Ad Bellum in the Age of Cyber Warfare, CALIF. L. REV. 101 (2013), 1079 (1085 ff., insb. 1088).

33 Zu den verschiedenen Angriffsformen siehe die Nachweise in Fn. 8.

II. Möglichkeiten und Grenzen des Selbstverteidigungsrechts bei Cyberattacken

Cyberattacken eröffnen nur dann das Recht auf Selbstverteidigung, wenn im jeweiligen Einzelfall die Voraussetzungen von Art. 51 UN-Charta erfüllt sind. Ausweislich des klaren Wortlauts setzt das Selbstverteidigungsrecht zunächst das Vorliegen eines „bewaffneten Angriffs gegen einen Mitgliedstaat der Vereinten Nationen" voraus (1.). Dieser Angriff – und das ist gerade bei Cyberattacken ein großes Problem – muss von einem Staat ausgehen oder diesem jedenfalls zugerechnet werden können (2.). Sollten beide Voraussetzungen erfüllt sein, müssen schließlich noch die Grenzen des Selbstverteidigungsrechts in quantitativer und zeitlicher Hinsicht gewahrt werden (3.).

1. Der „bewaffnete Angriff" als Ausgangspunkt

Ein „bewaffneter Angriff" bildet den Ausgangspunkt jeder staatlichen Selbstverteidigung. Es versteht sich zunächst von selbst, dass eine Selbstverteidigung von vornherein ausscheidet, wenn der vermeintliche „Angreifer" selbst im Wege der Selbstverteidigung oder anderweitig gerechtfertigt handelt. Genauer wäre es daher von einem *rechtswidrigen* bewaffneten Angriff als Grundvoraussetzung zu sprechen.[34] Allerdings liegt die völkerrechtliche Problematik weniger in der Einordnung der Rechtmäßigkeit als vielmehr in der Einordnung einer Handlung als „bewaffneter Angriff". Obwohl es die zentrale Voraussetzung ist, bleibt der Begriff des „bewaffneten Angriffs" oder der „armed attack" nämlich nach wie vor durch eine gewisse Unschärfe geprägt.[35] Eine wichtige Orientierung für die Praxis bietet die Aggressionsdefinition der Generalversammlung der Vereinten Nationen vom 14. Dezember 1974.[36] In Art. 3 dieser Resolution werden verschiedene Handlungen beispielhaft als Angriffshandlung definiert. Darunter fallen neben der Invasion oder dem Angriff der Streitkräfte eines Staates auf das Hoheitsgebiet eines anderen Staates unter anderem auch die Beschießung oder Bombardierung fremden Hoheitsgebietes, der Einsatz von Waffen jeder Art durch einen Staat gegen das Hoheitsgebiet eines anderen Staates, die Blockade von Häfen oder Küsten eines anderen Staates sowie der Angriff der Streitkräfte eines Staates auf die Land-, See- oder Luftstreitkräfte oder auf die See- und Luftflotte eines anderen

34 *v. Arnauld*, Völkerrecht (Fn. 22), S. 500 Rn. 1090.
35 *Hobe*, Völkerrecht (Fn. 13), S. 212.
36 UN Generalversammlung, A/RES/3314 (XXIX) vom 14.12.1974.

Staates. Obwohl diese nach Art. 4 der Resolution nicht abschließende Liste von Handlungen eine gute erste Orientierung bieten kann, sollte man bedenken, dass sich der Aggressionsbegriff dieser Resolution nur auf die Kompetenz des UN-Sicherheitsrats nach Art. 39 UN-Charta bezieht und ausdrücklich nicht als Definition für den „bewaffneten Angriff" im Sinne des Art. 51 UN-Charta gedacht war.[37] Es besteht allerdings weitgehende Einigkeit, dass der Aggressionsbegriff zur Bestimmung eines Kernbereichs des „bewaffneten Angriffs" herangezogen und der „bewaffnete Angriff" im Übrigen durch Rechtsprechung und Praxis konkretisiert werden kann.[38] Im Allgemeinen scheint heute Folgendes anerkannt: Zunächst stellt nicht jede Gewaltanwendung einen „bewaffneten Angriff" dar, sondern nur eine solche, die als massiver, koordinierter Militärschlag gegen einen anderen Staat eine gewisse Intensität erreicht.[39] So hat auch der Internationale Gerichtshof im *Nicaragua*-Fall bloße Grenzscharmützel zwar als Verstoß gegen das Gewaltverbot, nicht aber als einen das Selbstverteidigungsrecht auslösenden „bewaffneten Angriff" eingeordnet.[40] Ob ein „bewaffneter Angriff" vorliege, sei anhand des jeweiligen Einzelfalls zu bewerten, wobei es sowohl auf das Ausmaß bzw. die Größenordnung des Anschlages („scale") als auch auf seine (Aus-)Wirkungen („effects") ankomme.[41] Wann Ausmaß und Wirkung die Schwelle des „bewaffneten Angriffs" überschreiten, ist naturgemäß eine im Einzelfall schwierig zu beurteilende Frage. So hat beispielsweise der UN-Sicherheitsrat das Ausmaß wiederholter sogenannter „gestreuter Bagatellangriffe" der PLO gegenüber Israel nicht als ausreichend angesehen.[42] Umgekehrt hat der Inter-

37 *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 17; dazu und zum Folgenden auch *v. Arnauld*, Völkerrecht (Fn. 22), S. 498 Rn. 1085.

38 *Hobe*, Völkerrecht (Fn. 13), S. 212; *T. Stein/C. v. Buttlar/M. Kotzur*, Völkerrecht, 14. Aufl., München 2017, S. 292 Rn. 784.

39 Siehe nur *Herdegen*, Völkerrecht (Fn. 13), S. 281 Rn. 22; *Hobe*, Völkerrecht (Fn. 13), S. 212 f.; *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 292 Rn. 784; teilweise anders aber *W. Heintschel von Heinegg*, in: K. Ipsen, Völkerrecht, 7. Aufl., München 2018, § 56 Rn. 6 ff.

40 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, § 195.

41 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, §§ 191, 195; IGH, *Oil Platforms* (Iran v. USA), Urteil vom 06.11.2003, ICJ-Reports 2003, 161, §§ 51 u. 64. Ausf. auch *T. Ruys*, "Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge 2010, passim.

42 UN Sicherheitsrat, S/RES/490(1981) vom 21.07.1981; S/RES/501(1982) vom 25.02.1982; S/RES/509 vom 06.06.1982; dazu *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 292 Rn. 786.

nationale Gerichtshof eine kumulative Gesamtbetrachtung nicht vollständig ausgeschlossen.[43] Generell dürfte bei hohen Opferzahlen die Schwelle zum „bewaffneten Angriff" überschritten sein. Gleichzeitig wird gerade im Hinblick auf die „Auswirkungen" der fraglichen Handlung oftmals eine hohe Hürde angesetzt, die auf eine Bedrohung der politischen Unabhängigkeit oder Souveränität des betroffenen Staates abstellt.[44] Eine derart hohe Hürde mag auf den ersten Blick unbefriedigend erscheinen. Obwohl ein klarer aggressiver Akt vorliegt, der möglicherweise auch gegen das Gewaltverbot verstößt, wird dem „Opfer" der Aggression das Recht zur Selbstverteidigung verwehrt. Diesem Umstand versuchen einige Stimmen zu begegnen, indem sie das Selbstverteidigungsrecht nicht vollständig ausschließen, sondern „nur" in der Rechtsfolge beschränken wollen. Wird nach dieser Ansicht die Schwelle des „bewaffneten Angriffs" nach Ausmaß und Wirkung nicht überschritten, dürfe der betroffene Staat auf eine „*forcible countermeasure*" unter strenger Wahrung der Verhältnismäßigkeit zurückgreifen.[45] Die Etablierung eines solchen „kleinen Selbstverteidigungsrechts"[46] ist mit Blick auf eine mögliche Eskalation des Konflikts aber mit Vorsicht zu genießen.[47] Wie auch der Internationale Gerichtshof im *Nicaragua*-Fall noch einmal betont hat, ist es das Ziel der UN-Charta, gewalttätige Auseinandersetzungen zwischen den Staaten der Vereinten Nationen im größtmöglichen Umfang auszuschließen.[48] Im Falle des Nichterreichens der Schwelle des „bewaffneten Angriffs" ist der betroffene Staat somit mangels Ausnahme vom Gewaltverbot auf friedliche Gegenmaßnahmen beschränkt.[49] In Betracht kommt neben Maßnahmen im Bereich des Diplomaten- bzw. Konsularrechts insbesondere die

43 Vgl. IGH, *Oil Platforms* (Iran v. USA), Urteil vom 06.11.2003, ICJ-Reports 2003, 161 § 64.

44 Dazu *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 292 f. Rn. 787.

45 Sondervotum B. Simma zum Urteil vom 06.11.2003, IGH, *Oil Platforms* (Iran v. USA), ICJ-Reports 2003, 161, 324 §§ 12 ff.; dazu auch *M. Kowalski*, Original Sin Reaffirmed, PolYIL 36 (2016), 37 (43 ff.).

46 Dazu *A. Verdross/B. Simma*, Universelles Völkerrecht, Theorie und Praxis, 3. Aufl., Berlin 1984, S. 289 f. § 473; *Herdegen*, Völkerrecht (Fn. 13), S. 273 ff. Rn. 25.

47 *v. Arnauld*, Völkerrecht (Fn. 22), S. 499 Rn. 1087; kritisch auch *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 8.

48 *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 294 Rn. 790 unter Hinweis auf IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 127, § 14.

49 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, §§ 191, 195; IGH, *Oil Platforms* (Iran v. USA), Urteil vom 06.11.2003, ICJ-Reports 2003, 161, § 51.

Verhängung von Wirtschaftssanktionen.[50] Eine Klassifizierung als „bewaffneter Angriff" ist also schon bei konventionellen bzw. analogen Angriffen nicht unproblematisch. Noch einmal komplizierter wird es dann, wenn Cyberattacken rechtlich eingeordnet werden sollen.

Können Cyberattacken einen „bewaffneten Angriff" im Sinne des Art. 51 UN-Charta darstellen? Zur Beantwortung sei zunächst auf ein Gutachten des Internationalen Gerichtshofs verwiesen, wonach die Ausübung des Rechts auf Selbstverteidigung nicht von der Art der Waffe abhängt, mit der ein Angriff verübt wurde.[51] Dies entspricht auch der Staatenpraxis, wonach auch chemische, biologische oder atomare Attacken als „bewaffnete Angriffe" qualifiziert werden können.[52] Eine andere Frage ist hingegen, ob der Wortlaut von Art. 51 UN-Charta ein physisches Element in Bezug auf die Waffe fordert oder ob auch rein elektronische oder virtuelle Waffen erfasst sind.[53] Die Formulierung „bewaffnet" bzw. „armed" spricht eher gegen eine unmittelbare Erfassung nicht-physischer Waffen. Dies darf aber nicht zu einem Ausschluss des Selbstverteidigungsrechts führen, da die Anwendung des naturgegebenen Selbstverteidigungsrechts nicht davon abhängen kann, wie ein möglicher Angriff verursacht bzw. ein entstandener Schaden vermittelt wurde. Dementsprechend kann auch ein rein virtueller Angriff grundsätzlich zu einer entsprechenden bzw. analogen Anwendung von Art. 51 UN-Charta führen.[54]

Damit ist aber noch lange nicht geklärt, unter welchen Voraussetzungen eine Cyberattacke einen „bewaffneten *Angriff*" darstellt, der eine Selbstverteidigung rechtfertigen würde. Entsprechend der allgemeinen Annäherung an den Begriff kommt es nach überwiegender Auffassung auch bei Cyberattacken auf Ausmaß und Wirkung an.[55] Damit eine Cyberattacke die Schwelle

50 *v. Arnauld*, Völkerrecht (Fn. 22), S. 499 Rn. 1087 u. S. 256 f. Rn. 421; s.a. *H. Krieger*, Krieg gegen anonymous, AvR 50 (2010), 1 (14 ff.); speziell zu Wirtschaftssanktionen s.a. *G. Hafner*, Völkerrechtliche Grenzen und Wirksamkeit von Sanktionen gegen Völkerrechtssubjekte, ZaöRV 76 (2016), 391.

51 IGH, *Legality of the Threat of Use of Nuclear Weapons* (Advisory Opinion), Gutachten vom 08.07.1996, ICJ-Reports 1996, 226, §§ 38 f.

52 Dazu *M. N. Schmitt* (Hrsg.), Tallinn Manual 2.0 on the international law applicable to cyber operations, Cambridge 2017, S. 340 Rule 71 Erläuterung 4 m.w.N.

53 Für eine Erfassung *v. Arnauld*, Völkerrecht (Fn. 22), S. 498 f. Rn. 1086; ausf. auch *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 43 m.w.N.

54 *Hobe*, Völkerrecht (Fn. 13), S. 248; zum Argument der Wortherkunft s.a. *Roscini*, Cyber operations (Fn. 13), S. 297 (301 ff.).

55 Einen Überblick über andere Kriterien bieten *L. A. Petersen*, Cyberangriffe - Definition, Regulierung, Pönalisierung, Göttinger Rechtszeitschrift 1/2020, 25 (28 ff.) sowie *S. Pan-*

eines „bewaffneten Angriffs" im Sinne des Art. 51 UN-Charta (analog) überschreitet, müssen ihre physischen Auswirkungen, das heißt insbesondere die hervorgerufenen Schäden, mit denen eines konventionellen „bewaffneten Angriffs" vergleichbar sein.[56] Insoweit werden also in erster Linie die Auswirkungen der virtuellen Attacke auf die reale Welt in den Blick genommen und daraufhin geprüft, ob sie in Ausmaß und Wirkung einem konventionellen Angriff entsprechen. Das Tallinn Manual, ein internationales Handbuch für rechtlich zulässige Methoden der Kriegführung, welche nun auch Regeln über die Anwendung des Völkerrechts auf Cyberoperationen zum Inhalt hat,[57] bietet für diesen Vergleich eine nicht abschließende Liste von Kriterien an, die neben dem Grad des Schadens auch einige qualitative Elemente der Cyberoperation in den Blick nimmt. Im Einzelnen nennt das Manual severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement und presumptive legality.[58] Neben dieser Liste, die das Tallinn Manual in erster Linie nur auf das Gewaltverbot nach Art. 2 Ziff. 4 UN-Charta bezieht, bietet es auch im Zusammenhang mit dem Selbstverteidigungsrecht und der dort relevanten Einordnung als „bewaffneter Angriff" einige Hilfestellung.[59] In Anlehnung an die auch bei konventionellen Angriffen herangezogene Aggressionsdefinition können Cyberoperationen gegen die militärische Infrastruktur eines Staates, welche die Verteidigungsbereitschaft erheblich einschränken, als bewaffneter Angriff eingeordnet werden. Ein einfaches Beispiel wäre ein Cyberangriff gegen die IT eines Kriegsschiffes oder Kampfflugzeugs als Vorbereitung für einen konventionellen Angriff.[60] Ist allerdings die Verteidigungsbereitschaft nicht unmittelbar be-

---

grazzi, Self-defence against Cyberattackt?, Digital and kinetic defence in light of article 51 UN-Charter, Policy Brief, ICT for Peace Foundation, Genf 2021, S. 12 ff., abrufbar unter: https://ict4peace.org/wp-content/uploads/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf (zuletzt abgerufen: 23.02.2023).

56 Siehe nur *v. Arnauld*, Völkerrecht (Fn. 22), S. 498 f. Rn. 1086; *Hobe*, Völkerrecht (Fn. 13), S. 248; *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 42 f. m.w.N. Ausf. auch *Focarelli*, Self-defence (Fn. 1), S. 317 (326 ff.) sowie *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 339 ff. Rule 71 ff.

57 *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 1 ff.

58 *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 333 ff. Rule 69 Erläuterung 9 f.

59 *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 339 ff. Rule 71; siehe zum Zusammenhang von Gewaltverbot und bewaffneten Angriff auch *Focarelli*, Self-defence (Fn. 1), S. 317 (327 f.).

60 *Herdegen*, Völkerrecht (Fn. 13), S. 283 Rn. 24; zu möglichen Formen und Abstufungen s.a. *Focarelli*, Self-defence (Fn. 1), S. 317 (329 ff.) sowie *F. M. E. Oorsprong/P. A. L. Ducheine/ B. M. J. Pijpers*, Armed attack in Cyberspace, Clarifying and Assessing when Cyber-

troffen, wird auch die Schwelle zum „bewaffneten Angriff" regelmäßig nicht überschritten sein. Dies gilt insbesondere für rein netzinterne Vorgänge, wie beispielsweise im Falle des bloßen Ausspähens von Daten oder der kurzfristigen Blockade von Regierungsseiten.[61] Obwohl diese und ähnlich gelagerte Situationen also nicht zur Selbstverteidigung ermächtigen, können sie gleichwohl als Verstoß gegen das Interventionsverbot zu qualifizieren sein und dementsprechend friedliche Gegenmaßnahmen ermöglichen.[62]

Anders sieht die Situation wiederum aus, wenn man Cyberattacken auf zivile Einrichtungen oder Objekte betrachtet. Denkbare Szenarien sind insbesondere Cyberoperationen, die kritische Infrastruktur ins Visier nehmen. Für Deutschland nennt § 2 Abs. 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), auf welches auch die Cybersicherheitsstrategie des BMI Bezug nimmt,[63] als kritische Infrastrukturen:

> Einrichtungen, Anlagen oder Teile davon,
> 1. die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und
> 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Cyberoperationen gegen derartige Einrichtungen, die zu nicht unerheblichen Verletzungen, Todesfällen oder substanziellen Sachschäden oder Zerstörun-

---

Attacks Trigger the Netherlands' Right of Self-Defence, Amsterdam Law School Legal Studies Research Paper No. 2021–29, S. 16 ff.

61 *v. Arnauld*, Völkerrecht (Fn. 22), S. 498 f. Rn. 1086 sowie *Hobe*, Völkerrecht (Fn. 13), S. 248, jeweils m.w.N. Ausf. zur völkerrechtlichen Einordnung von Cyber-Spionage *R. Buchan/I. Navarette*, Cyber espionage and international law, in: N. Tsagourias/R. Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl., Cheltenham 2021, S. 231 ff.

62 Ausf. *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 168 ff. Rule 32 sowie S. 312 ff. Rule 66; s.a. *K. Ziolkowski*, Peacetime Cyber Espionage – New Tendencies in Public International Law, in: K. Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, Tallinn 2013, S. 425 (457 ff.) sowie *T. D. Gill*, Non-Intervention in the Cyber-Context, in: K. Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, Tallinn 2013, S. 217 ff.

63 BMI, Cybersicherheitsstrategie für Deutschland 2021, S. 15 f., 52 u. 81, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf (zuletzt abgerufen am 23.03.2023).

gen führen, können ebenfalls als „bewaffneter Angriff" im Sinne des Art. 51 UN-Charta eingeordnet werden.[64] Fehlt es an derartigen klaren oder unmittelbaren Folgen, kann die Abgrenzung schwierig sein. Beispielsweise hat ein Cyberangriff auf internationale Finanzmärkte zweifelsfrei enorme wirtschaftliche Folgen, führt aber nicht zwangsläufig zu unmittelbaren physischen Schäden. Letztlich kommt es auf eine einzelfallbezogene Betrachtung an, bei der grundsätzlich alle vorhersehbaren Effekte sowohl im unmittelbar betroffenen Staat als auch in Drittstaaten berücksichtigt werden müssen.[65] Umstritten bleibt dabei, inwieweit die Intention des Angreifers zu berücksichtigen ist.[66] Letztlich bleiben aber Ausmaß und Wirkung der Cyberoperation und ihre Vergleichbarkeit zu einem konventionellen Angriff entscheidend. Dabei ist auch in Rechnung zu stellen, dass in der globalisierten Welt Cyberattacken auf die kritische Infrastruktur eines Landes schnell überregionale oder sogar weltweite Auswirkungen haben können. Umgekehrt sollte mit Blick auf die hohe Bedeutung des Gewaltverbots nicht vorschnell ein „bewaffneter Angriff" angenommen werden.

Als erstes Zwischenergebnis lässt sich aber somit festhalten, dass Cyberattacken, sofern sie nach Ausmaß und Wirkung mit einem konventionellen Angriff vergleichbar sind, einen „bewaffneten Angriff" im Sinne des Art. 51 UN-Charta darstellen können. Damit ist aber nur die Grundvoraussetzung des Selbstverteidigungsrechts erfüllt. Die eigentliche Herausforderung in faktischer und völkerrechtlicher Hinsicht liegt darin, zu beurteilen, von wem der Angriff ausgegangen ist und gegen wen sich dementsprechend auch eine Gegenmaßnahme zu richten hat.

2. Die eigentliche Herausforderung: Rückverfolgbarkeit und Zurechnung

Wie soeben dargestellt, kann schon die Qualifizierung einer Cyberattacke als „bewaffneter Angriff" eine im Einzelfall schwierig zu beantwortende

64 *Focarelli*, Self-defence (Fn. 1), S. 317 (330 ff.) sowie *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 43; s.a. *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 341 ff. Rule 71, Erläuterungen 8 und 12 ff.

65 Ausf. *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 342 ff. Rule 71, Erläuterung 12 ff. sowie *Dornbusch*, Kampfführungsrecht (Fn. 1), S. 20, 24 f., 81 ff., 102 ff. und 228 f.

66 In IGH, *Oil Platforms* (Iran v. USA), Urteil vom 06.11.2003, ICJ-Reports 2003, 161, § 64 spricht der IGH von „the specific intention of harming"; dazu *S. Kolossa*, Der Cyberraum – Chance, Gefahrenraum und Waffe?, HuV 1 (2018), 151 (166) sowie *M. Roscini*, World Wide Warefare – Jus ad bellum and the Use of Cyber Force, in: A. v. Bogdandy/R. Wolfrum, Max Plank Yearbook of United Nations Law, Vol. 14 (2010), S. 85 (115 f.).

rechtliche Frage darstellen. Doch selbst wenn ein Staat unzweifelhaft von einer Cyberoperation betroffen ist und er sie aufgrund ihrer Auswirkungen zu Recht als „bewaffneten Angriff" einordnet, steht der Staat vor dem nicht unerheblichen Problem, gegen wen er seine Gegenmaßnahmen richten soll. Die damit angesprochenen Fragen der Identifizierung des Angreifers sowie der Zurechnung zu einem Staat sind nicht nur in völkerrechtlicher, sondern auch und vor allem in technischer Hinsicht mit Schwierigkeiten verbunden.[67]

So wird bei Cyberoperationen regelmäßig zunächst die technische Frage der schwierigen bis unmöglichen Rückverfolgbarkeit des Angriffs die eigentliche Herausforderung darstellen.[68] Die Funktionsweise des Cyberspace als weltweit verzweigtes Netzwerk lässt dem Angreifer zahllose technische Wege, entweder Ursprung und Route seines Angriffs komplett zu verbergen oder aber auch falsche Fährten zu legen. Selbst wenn eine Cyberattacke über Leitungen oder Computer eines bestimmten Staates verübt wurde, ist das zwar ein Indiz, aber noch kein vollständiger Nachweis darüber, ob dieser Staat tatsächlich der Ursprungsort des Angriffs war.[69] Eine große Rolle spielt auch der Faktor Zeit. Während die Attacke selbst in der Regel nur wenige Augenblicke dauern wird, können ihre Wirkungen unter Umständen erst mit Verzögerung eintreten oder aber erst später als Folge einer Cyberattacke erkennbar werden.[70] Ein letztes in der Regel kaum zu überbrückendes Problem ist schließlich die sogenannte „Mensch-Maschine-Gap".[71] Selbst wenn sich der Weg eines Angriffs vollständig und innerhalb angemessener Zeit zu einem bestimmten Server oder Computer zurückverfolgen lässt

67 Zum Unterschied von Identifizierung und Zurechnung sowie dem technisch-politischen Rahmen siehe nur *Roscini*, World Wide Warefare (Fn. 66), S. 85 (96 ff.) sowie *N. Tsagourias*, Cyber attacks, self-defence and the problem of attribution, Journal of Conflict and Security Law Vol. 17 (2012), 229 (230 u. 233 ff.).

68 Dazu ausf. *Schulze*, Cyber-„War" (Fn. 6), S. 36 ff.; s.a. *Heintschel von Heinegg*, Cyberspace (Fn. 21), S. 159 (171); *Kolossa*, Cyberraum (Fn. 66), 167 sowie die Nachweise in Fn. 67.

69 *Kolossa*, Cyberraum (Fn. 66), 167; s.a. *Schmitt (Hrsg.),* Tallinn Manual on the International Law Applicable to Cyber warfare, Cambridge 2013, S. 34 ff. Rule 7 ff. sowie *S. Pangrazzi*, Self-defence against Cyberattacks?, Digital and kinetic defence in light of article 51 UN-Charter, Policy Brief, ICT for Peace Foundation, Genf 2021, S. 17 f., abrufbar unter: https://ict4peace.org/wp-content/uploads/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf (zuletzt abgerufen: 23.02.2023).

70 *Schulze*, Cyber-„War" (Fn. 6), S. 46 f.; zum Problem der Verzögerung auch *C. Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace, Für klare Regeln und mehr Verantwortung, SWP-Studie 2014/S 18 vom 23.10.2014, S. 21 f.

71 Dazu und zum Folgenden *Schulze*, Cyber-„War" (Fn. 6), S. 47.

und somit der Ursprungsort feststeht, ist damit noch nicht geklärt, welcher Mensch an diesem Computer saß und in welcher Funktion er tätig wurde.[72] Diese Frage wird sich in der Praxis regelmäßig auch nicht oder jedenfalls nicht innerhalb kurzer Zeit klären lassen. In technischer Hinsicht besteht damit eine nur schwer zu überwindende Einschränkung für das Selbstverteidigungsrecht. Kann der Angreifer nicht zweifelsfrei identifiziert werden, ist eine Verteidigung schon rein praktisch ausgeschlossen. Ob und vor allem wie dieser technischen Unzulänglichkeit mit neuen Ansätzen und Mitteln des Völkerrechts begegnet werden kann, wird im Rahmen des Ausblicks am Ende des Beitrags erläutert. Zunächst soll die Problematik der Rückverfolgbarkeit aber zurückgestellt werden und der Fokus auf den weiteren Voraussetzungen und Grenzen des Selbstverteidigungsrechts liegen.

Ungeachtet der schwierigen Rückverfolgbarkeit muss sich die Selbstverteidigung grundsätzlich gegen den Staat richten, der den Angriff verübt hat oder dem ein eventuelles Handeln privater Gruppen oder Akteure zugerechnet werden kann. Einen Sonderfall bildet die umstrittene Selbstverteidigung gegen private Akteure, die unabhängig von einem Staat handeln, namentlich terroristische Gruppen. Auch Cyberangriffe können logischerweise von Staaten oder privaten Akteuren ausgeführt werden, wobei Handlungen von nichtstaatlichen Akteuren sicherlich die größte Herausforderung darstellen. In Bezug auf konventionelle bzw. analoge „bewaffnete Angriffe" hat der Internationale Gerichtshof im *Nicaragua*-Fall geäußert, dass die Entsendung bewaffneter Banden im Sinne des Art. 3 lit. g der Aggressionsdefinition einem Staat zugerechnet und somit zu einem Selbstverteidigungsrecht führen kann.[73] Für eine Zurechnung darf der Staat aber nicht nur als bloßer finanzieller oder logistischer Unterstützer erscheinen. Vielmehr muss er im Sinne einer Tatherrschaft so über die Handlungen der privaten Gruppen bestimmen, dass sie gewissermaßen als sein „verlängerter Arm" agieren.[74] Besteht keine solche Verbindung, scheidet eine Selbstverteidigung unmittelbar gegen Angriffe von privaten Akteuren grundsätzlich aus. Dieses Verständnis hat sich im Nachgang zu den Terroranschlägen vom 11. September 2001 aber teilweise

72 *Heintschel von Heinegg*, Cyberspace (Fn. 21), S. 159 (172); *Kolossa*, Cyberraum (Fn. 66), 167.

73 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, § 195.

74 *v. Arnauld*, Völkerrecht (Fn. 22), S. 499 f. Rn. 1088 f.; s.a. *Herdegen*, Völkerrecht (Fn. 13), S. 284 Rn. 25 f. sowie *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 293 Rn. 788 f.

gewandelt.[75] Während der Internationale Gerichtshof wohl weiter an der herkömmlichen Sichtweite festhält,[76] gehen der UN-Sicherheitsrat, die Staatengemeinschaft und wohl auch der überwiegende Teil der Literatur davon aus, dass auch private Gewaltanwendung einen „bewaffneten Angriff" darstellen kann, sofern sie das Ausmaß einer staatlichen Militäraktion erreicht. In diesem Fall würde sich die Selbstverteidigung gegen den Staat richten, der den Angreifern einen Unterschlupf – man spricht auch von einem „*safe haven*" – gewährt hat.[77]

Obwohl gerade diese letzte Ansicht nicht unumstritten ist, können die grundlegenden Gedanken der Zurechnung auch zur rechtlichen Einordnung von Cyberattacken herangezogen werden. Wenn eine Gruppe oder einzelne Personen einen Cyberangriff als verlängerter Arm eines Staates ausführen, ist auch insoweit eine Zurechnung möglich. Bei Cyberangriffen, die Private vom Territorium eines Staates verüben, ohne dass dieser den Angriff ausdrücklich autorisiert hat oder ihn jedenfalls duldet, bleibt die Lage umstritten.[78] Problematisch ist vor allem, wann dem Staat, von dessen Territorium ein Angriff verübt wird, in rechtlicher Hinsicht ein Vorwurf gemacht werden kann, der auch ein Selbstverteidigungsrecht des angegriffenen Staates rechtfertigen würde. Da dies auch mit der bereits problematisierten technischen Rückverfolgbarkeit zusammenhängt, werden beide Aspekte noch einmal am Ende des Beitrags im Zusammenhang mit den künftigen Entwicklungslinien des Völkerrechts aufgegriffen. Zunächst kann aber als zweites Zwischenergebnis festgehalten werden, dass eine Selbstverteidigung auch bei privaten Cyberattacken nicht von vornherein ausgeschlossen ist.

3. Grenzen des Selbstverteidigungsrechts

Wenn Cyberattacken also ungeachtet der schwierigen Rückverfolgbarkeit ein staatliches Selbstverteidigungsrecht legitimieren können, bleibt noch zu klä-

75 Hier und im Folgenden *Kolossa*, Cyberraum (Fn. 66), 166 und *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 344 Rule 71, Erläuterung 18, jeweils m.w.N.

76 IGH, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) Gutachten vom 09.07.2001, ICJ-Reports 2004, 136, § 139; IGH, *Armed Activities on the Territory of the Congo*, Merits, Urteil vom 19.12.2005, ICJ-Reports 2005, 168, §§ 146 f. u. 160.

77 *Hobe*, Völkerrecht (Fn. 13), S. 213; ausf. *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 316 ff. Rn. 841 ff. u. 298 ff. Rn. 800.; s.a. die Nachweise in Fn. 75; kritischer *v. Arnauld*, Völkerrecht (Fn. 22), S. 271 ff. Rn. 1120 ff.

78 Zu der Übertragbarkeit der Gedanken und dem Meinungsstand siehe nur *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 344 u. 347 Rule 71, Erläuterungen 16 ff. u. 23 ff.

ren, wie die konkrete Verteidigungshandlung ablaufen muss. Dies führt zu der abschließenden Frage, welchen Grenzen das staatliche Selbstverteidigungsrecht aus Art. 51 UN-Charta unterliegt.

Entsprechend seiner Zielsetzung, einen „bewaffneten Angriff" auf das eigene Territorium *abzuwehren*, eröffnet das Selbstverteidigungsrecht nicht die Möglichkeit für eine Vergeltung. Es richtet sich alleine gegen einen aktuell andauernden bzw. *gegenwärtigen* Angriff. Eine Selbstverteidigung ist daher grundsätzlich nur möglich, wenn der Angriff bereits begonnen hat und noch nicht abgeschlossen ist. Dieses Gegenwärtigkeits- oder auch Unmittelbarkeitskriterium kann sowohl in Bezug auf den Beginn als auch das Ende des Angriffs bzw. der Selbstverteidigung problematisch sein. Zunächst ist das Kriterium nicht im Sinne einer strengen „Unverzüglichkeit" zu verstehen. So geht die Gegenwärtigkeit regelmäßig nicht verloren, wenn ein Staat sich erst mit seinen Verbündeten abstimmt oder andere notwendige Vorbereitungshandlungen für einen Gegenschlag trifft.[79] Mit anderen Worten: Es besteht hinsichtlich des Endes der Gegenwärtigkeit ein gewisser Spielraum. Umstritten ist, inwieweit dies auch beim Angriffsbeginn der Fall ist. Dies betrifft insbesondere die sogenannte „antizipatorische Selbstverteidigung", also eine Verteidigung gegen einen unmittelbar bevorstehenden Angriff. Regelmäßig dürfte es einem Staat nicht zuzumuten sein, so lange abzuwarten, bis der Angriff tatsächlich begonnen hat. Um die damit verbundene Missbrauchsgefahr zu begrenzen, wird zur Bestimmung der Frage, wann die Unmittelbarkeit noch gewahrt ist, auf die sogenannte *Caroline*- oder *Webster*-Formel abgestellt. Demnach muss der Staat, der sich auf die Selbstverteidigung beruft, nachweisen, dass der Angriff unmittelbar bevorstand, überwältigend war und dass keine Wahl der Mittel und keine Zeit für weitere Beratungen blieb.[80] Die Beurteilung, wann diese Kriterien erfüllt sind, hängt naturgemäß vom jeweiligen Einzelfall ab. Letztlich spricht einiges dafür, dem angegriffenen Staat auch hier einen – begrenzten – Beurteilungsspielraum zuzugestehen. Andernfalls könnte der Angreifer allein die Regeln des Spiels bestimmen.

Das Erfordernis der Gegenwärtigkeit kann bei Cyberangriffen eine nicht unerhebliche Hürde darstellen. Wie bereits geschildert, spielt der Zeitfaktor eine wichtige Rolle bei Cyberattacken. Einerseits läuft die Angriffshandlung sehr schnell ab. Ihre Folgen können aber unter Umständen erst viel später

79 *v. Arnauld*, Völkerrecht (Fn. 22), S. 500 f. Rn. 1091 f.; *Hobe*, Völkerrecht (Fn. 13), S. 213; *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 294 f. Rn. 792 f.

80 Dazu und zum Folgenden *v. Arnauld*, Völkerrecht (Fn. 22), S. 501 Rn. 1093 sowie *Hobe*, Völkerrecht (Fn. 13), S. 213 f., jeweils m.w.N.

eintreten oder erkannt werden. Auch kann es eine lange Zeit dauern, bis der Angriff zurückverfolgt und so das Ziel der Selbstverteidigung identifiziert ist. Die soeben geschilderten Gedanken, also insbesondere die Möglichkeit einer antizipatorischen Selbstverteidigung und die Notwendigkeit, dem angegriffenen Staat eine gewisse Vorbereitungs- und Nachforschungszeit einzuräumen, dürften grundsätzlich auch bei Cyberoperationen anwendbar sein, wobei die Einzelheiten weiter umstritten sind.[81] Auch bei Cyberoperationen ist zur Wahrung der Unmittelbarkeit aber entscheidend, dass der zeitliche und inhaltliche Bezug von Angriff und Verteidigungshandlung nicht vollständig verloren geht.[82] In Anbetracht der schwierigen Rückverfolgbarkeit macht dies möglicherweise eine weitergehende Flexibilisierung des Unmittelbarkeitskriteriums erforderlich. Andererseits darf wiederum die drohende Missbrauchsgefahr nicht unterschätzt werden.

Als weitere Grenze des Selbstverteidigungsrechts muss der Grundsatz der Verhältnismäßigkeit beachtet werden. Obwohl diese Voraussetzung sich nicht aus dem Wortlaut des Art. 51 UN-Charta ergibt, hat der Internationale Gerichtshof sie mit Blick auf die gewohnheitsrechtlichen Grundlagen des Selbstverteidigungsrechts ausdrücklich auch für Art. 51 UN-Charta bestätigt.[83] Eine Verteidigungshandlung muss demnach erforderlich sein, es darf also kein milderes, gleich wirksames Mittel geben. Zudem darf die ergriffene Maßnahme nicht außer Verhältnis zu Umfang und Auswirkung des Angriffs stehen, sie muss also angemessen sein.[84] Beide Fragen sind naturgemäß nicht allgemein, sondern nur anhand eines konkreten Einzelfalls zu beantworten. Dabei dürfen nur rechtliche, nicht aber politische Kriterien eine Rolle spielen. Wichtige Gesichtspunkte sind u.a. die Art und Intensität des Angriffs sowie der Bewaffnung, das Ausmaß erwarteter Schäden auf beiden Seiten und die möglichen Auswirkungen auf Drittstaaten. Eine strenge Symmetrie zwischen

81 Zum Meinungsstand *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 350 ff. Rule 73; s.a. *Focarelli*, Self-defence (Fn. 1), S. 317 (332 ff.).

82 Vgl. *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 295 Rn. 793.

83 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, § 194; IGH, *Legality of the Threat of Use of Nuclear Weapons* (Advisory Opinion), Gutachten vom 08.07.1996, ICJ-Reports 1996, 226, § 41; IGH, *Oil Platforms* (Iran v. USA), Urteil vom 06.11.2003, ICJ-Reports 2003, 161, §§ 43, 73 f. u. 76.

84 *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 57 f.; dazu und zum Folgenden auch *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn. 38), S. 295 ff. Rn. 794 ff.

Angriff und Verteidigung gibt es dabei nicht. Der verteidigende Staat darf auf die effektive und endgültige Beendigung des Angriffs zielen.[85]

Gerade der letztgenannte Aspekt ist für Cyberoperationen besonders relevant. So kann ein angegriffener Staat auf einen Cyberangriff durchaus mit einem konventionellen Gegenschlag reagieren. Umgekehrt ist auch ein Cyber-Gegenschlag als Reaktion auf einen konventionellen Schlag denkbar.[86] Wiederum sind allein die rechtlichen Kriterien der Erforderlichkeit und Angemessenheit maßgeblich. Bezüglich der Erforderlichkeit ist bei der Reaktion auf Cyberangriffe insbesondere zu bedenken, ob ein milderes Mittel, also beispielsweise rein defensive Maßnahmen wie Firewalls oder Ähnliches ausreichend sind.[87] Stehen im konkreten Fall keine milderen Mittel zur Verfügung, sind – unter Wahrung der Angemessenheit – durchaus auch offensive Gegenmaßnahmen denkbar. Diese Maßnahmen können nach dem Wortlaut von Art. 51 UN-Charta wie bei konventionellen Angriffen einzeln oder auch kollektiv, also zum Beispiel auch im Rahmen der NATO, getroffen werden.[88] Zu beachten ist allerdings, dass die Beweislast sowohl für die Gegenwärtigkeit als auch für die Verhältnismäßigkeit bei dem Staat liegt, der sich auf das Selbstverteidigungsrecht beruft.[89]

Als letzte Grenze des Selbstverteidigungsrechts ist schließlich die Anzeigepflicht gegenüber dem UN-Sicherheitsrat zu beachten. Dies ist eine echte Rechtspflicht und sichert das Monopol, welches dem Sicherheitsrat zur Wahrung des Weltfriedens zukommt. Das Selbstverteidigungsrecht endet nach dem klaren Wortlaut von Art. 51 UN-Charta, sobald der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat. Allerdings führt ein Unterlassen der Anzeige auch nach dem Internationalen Gerichtshof nicht zur Rechtswidrigkeit einer Selbstverteidigungshandlung.[90] Obwohl in der Anzeigepflicht damit vor al-

85 *v. Arnauld*, Völkerrecht (Fn. 22), S. 503 Rn. 1097; s.a. *A. Randelzhofer*, in: Simma, Charta der Vereinten Nationen, Kommentar, München 1991, Art. 51 Rn. 37.

86 *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 349 Rule 72, Erläuterung 5.

87 *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 349 Rule 72, Erläuterung 3.

88 Dazu auch *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 354 f. Rule 75 sowie *Focarelli*, Self-defence (Fn. 1), S. 317 (336 f.).

89 IGH, *Oil Platforms* (Iran v. USA), Urteil vom 06.11.2003, ICJ-Reports 2003, 161, §§ 57 u. 76; *A. Randelzhofer/G. Nolte*, in: Simma/Khan/Nolte/Paulus (Fn. 14), Art. 51 Rn. 45 f.

90 IGH, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA), Merits, Urteil vom 27.06.1986, ICJ-Reports 1986, 14, § 235; dazu auch *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 356 Rule 75, Erläuterung 1.

lem die Subsidiarität des Selbstverteidigungsrechts zum Ausdruck kommt, bleibt es in der Praxis gleichwohl höchst relevant. Schließlich wird der Sicherheitsrat oftmals blockiert sein oder aus anderen Gründen seine Aufgabe nicht oder jedenfalls nicht innerhalb kurzer Zeit wahrnehmen können.[91] Im aktuellen Ukraine-Krieg zeigt sich diese Blockade besonders deutlich, da Russland nicht nur der Aggressor, sondern auch ständiges Mitglied im UN-Sicherheitsrat mit Vetorecht ist. Der Resolutionsentwurf zur Beendigung des Ukraine-Krieges vom 25.02.2022 scheiterte am russischen Veto.[92] Dass die Generalversammlung am 02.03.2022 und 24.03.2022 mit zwei Resolutionen das Vorgehen Russlands als völkerrechtswidrige Aggression eingeordnet und den unverzüglichen Abzug der russischen Truppen gefordert hat,[93] vermag wegen der fehlenden völkerrechtlichen Verbindlichkeit von Resolutionen der Generalversammlung die Blockade nicht zu überwinden. Gleichwohl ist die Verabschiedung mit einer Mehrheit von 141 bzw. 140 Stimmen eine nicht zu unterschätzende politische Botschaft der Weltgemeinschaft, die sich gegen die russische Aggression stellt.[94]

Ungeachtet einer Blockade dürfte im Allgemeinen, insbesondere bei einzelnen Cyberattacken, bei denen aus den geschilderten Gründen der Faktor Zeit in mehrfacher Hinsicht entscheidend ist, die Rolle des Sicherheitsrats in der Zukunft eher gering bleiben. Wegen der Schnelligkeit von Cyberattacken, erlangt auch die sonst schwierige Frage, ob die vom Sicherheitsrat ergriffenen Maßnahmen auch ausreichend waren,[95] keine allzu große Bedeutung. Unabhängig von der künftigen Rolle Russlands in der UN dürfte die Rolle des Sicherheitsrats jedenfalls bei einzelnen kurzfristigen Cyberattacken schon rein faktisch eher gering bleiben. In rechtlicher Hinsicht bleibt es aber dabei, dass der Sicherheitsrat nach Art. 51 UN-Charta auch bei Cyberattacken zwingend zu unterrichten ist. Ergreift der Sicherheitsrat in der Folge erfolgreich Maßnahmen zur Friedenssicherung, endet das Selbstverteidigungsrecht. Eine andere Frage ist es, ob der Sicherheitsrat in seiner heutigen Organisation und Zusammensetzung den aktuellen Herausforderungen des Friedenssicherungsrechts gerade mit Blick auf Cyberspace noch gerecht werden kann.

---

91 Siehe nur *Randelzhofer*, in: Simma (Fn. 85), Art. 51 Rn. 36.

92 UN-SC, Pressemitteilung SC/14808 vom 25.02.2022, abrufbar unter: https://www.un.org/press/en/2022/sc14808.doc.htm (zuletzt abgerufen: 23.02.2023).

93 UN Generalversammlung, A/RES/ES-11/1 vom 02.03.2022 und A/RES/ES-11/2 vom 24.3.2022.

94 So auch *Schmahl*, Angriffskrieg (Fn. 4), 971.

95 Siehe nur *Stein/v. Buttlar/Kotzur*, Völkerrecht (Fn, 38), S. 297 Rn. 798.

C. Zusammenfassung und Ausblick

An dieser Stelle soll es aber nicht um die Zukunft der Friedenssicherung im Rahmen der UN und die künftige Rolle Russlands im internationalen System gehen. Stattdessen sollen zum Abschluss noch einmal die wesentlichen Erkenntnisse zusammengefasst und ein kleiner Ausblick auf künftige Entwicklungen im Zusammenspiel von Cyberspace und Völkerrecht gewagt werden.

Cyberspace stellt das klassische Völkerrecht wegen seiner weltweiten netzwerkartigen Struktur und seiner Ungebundenheit an einen bestimmten Standort vor nicht unerhebliche Herausforderungen. Gleichwohl – und das ist der erste wichtige Punkt – führt dies nicht dazu, dass Cyberspace ein rechtsfreier Raum wäre. Vielmehr können die Regeln des Völkerrechts auch auf Cyberattacken angewendet werden. Cyberangriffe können und sollten aber nicht pauschal in eine bestimmte völkerrechtliche Kategorie eingeordnet werden. Vielmehr ist entsprechend der Abstufungen der UN-Charta im Einzelfall zu prüfen, ob sich eine Cyberattacke als Verstoß gegen das Interventionsverbot, als unzulässige Gewaltanwendung oder als bewaffneter Angriff einordnen lässt.[96] Wie dargestellt, können Cyberangriffe einen „bewaffneten Angriff" im Sinne des Art. 51 UN-Charta darstellen, wenn sie in Ausmaß („*scale*") und Wirkung („*effect*") mit einem konventionellen Schlag vergleichbar sind. Unter strenger Achtung von Unmittelbarkeit und Verhältnismäßigkeit ist dann eine Selbstverteidigung mit digitalen oder konventionellen Mitteln möglich. Ist die Schwelle eines „bewaffneten Angriffs" nicht erfüllt, ist dem betroffenen Staat das Selbstverteidigungsrecht verwehrt. Wegen des regelmäßig durch die feindliche Cyberoperation vorliegenden Verstoßes gegen das Interventionsverbot ist es dem Staat aber unbenommen, friedliche völkerrechtliche Gegenmaßnahmen zu ergreifen.

In beiden Fällen steht der Staat jedoch regelmäßig vor dem Problem der schwierigen bis unmöglichen Rückverfolgbarkeit von Cyberoperationen. Die Antwort auf die Frage, ob und wie völkerrechtliche Instrumente zur Überwindung dieser in erster Linie technischen Herausforderung genutzt werden können, ist eine der großen Aufgaben für die Weiterentwicklung des Völkerrechts. Einige der Ansätze, die in diesem Zusammenhang diskutiert werden, sollen zum Abschluss vorgestellt werden.

96 *Hobe*, Völkerrecht (Fn. 13), S. 247; *Y. Dinstein*, Computer Network Attacks and Self-Defense, International Law Studies 76 (2002), 99 ff.

Zu diesem Zweck bietet es sich an, noch einmal auf den geschilderten Fall zurückzukommen, bei dem ein Cyberangriff zweifelsfrei von Computern oder Servern eines bestimmen Staates verübt wurde, aber die handelnde Person entweder gar nicht zu identifizieren oder aber ihr Verhältnis zum Staat nicht eindeutig ist. Ist die Person zu identifizieren, dürfte gleichwohl eine Zurechnung zum jeweiligen Staat schwer möglich sein. Die nach der bisherigen Rechtsprechung geforderte „Entsendung" oder „*effective control*" wird sich regelmäßig nicht ohne Weiteres nachweisen lassen, zumal der betroffene Staat den Cyberangriff kaum offen zugeben wird. Eine Möglichkeit wäre nun, in Bezug auf Cyberangriffe die Zurechnungskriterien generell zu lockern. Ähnliches wäre auch bei den Grenzen des Selbstverteidigungsrechts denkbar. Beispielsweise könnte das Gegenwärtigkeitskriterium mit Blick auf den Zeitfaktor bei Cyberangriffen großzügiger gehandhabt werden. Allerdings ist bei jeder extensiven Auslegung des Selbstverteidigungsrechts die mögliche Missbrauchsgefahr mitzubedenken. Die Grundidee der Nachkriegsordnung durch die Vereinten Nationen ist die Sicherung des Weltfriedens durch ein möglichst weitreichendes Gewaltverbot.[97] Vor diesem Hintergrund sollten Modifikationen der Tatbestandsvoraussetzungen oder Zurechnungskriterien nur mit äußerster Vorsicht vorgenommen werden.[98]

Diskutiert wird in diesem Zusammenhang insbesondere eine Modifikation der Zurechnung im Wege einer Beweislastumkehr. Vor dem Hintergrund, dass die klassischen Zurechnungskriterien im Recht der Staatenverantwortlichkeit für die deliktische Haftung geschaffen wurden, könnte man tatsächlich überlegen, eine derartige Modifikation für jene Fälle anzunehmen, bei denen der Ursprung der Cyberattacke zweifelsfrei einem Staatsgebiet zugeordnet werden kann. Da es bei Cyberoperationen bzw. deren Abwehr weniger um eine *Haftung für* als um eine *Prävention von* Schäden geht, wäre es durchaus denkbar, die Zurechnung in solchen Szenarien widerleglich zu vermuten. Konkret würde dies bedeuten, dass ein Cyberangriff widerleglich dem Staat zugerechnet wird, von dessen Territorium der Angriff ausgeht.[99]

97 Vgl. Art. 1 Nr. 1 und 4, Art. 2 Nr. 4 und Art. 103 UN-Charta; zur historischen Entwicklung siehe nur *Hobe*, Völkerrecht (Fn. 13), S. 26 ff. u. S. 205 ff.

98 So auch *S. Pangrazzi*, Self-defence against Cyberattacks?, Digital and kinetic defence in light of article 51 UN-Charter, Policy Brief, ICT for Peace Foundation, Genf 2021, S. 19 ff., abrufbar unter: https://ict4peace.org/wp-content/uploads/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf (zuletzt abgerufen: 23.02.2024); s.a. *Krieger*, anonymous (Fn. 50), 1 (11 ff.).

99 *Heintschel von Heinegg*, Cyberspace (Fn. 21), S. 159 (172); s.a. *Schaller*, Internationale Sicherheit (Fn. 70), S. 23 ff. m.w.N.

Der Staat würde – vorläufig – als verantwortlich für den Angriff angesehen, weil er den Missbrauch seines Netzwerks geduldet bzw. nicht verhindert hat. Ein Ansatzpunkt für ein Selbstverteidigungsrecht gegenüber diesem Staat wäre die grundsätzliche Pflicht jedes Staates, dafür zu sorgen, dass von seinem Staatsgebiet keine Angriffe auf andere Staaten ausgehen.[100] Eine Selbstverteidigung wäre aber regelmäßig auch dann nur *erforderlich*, wenn der Staat, von dessen Territorium der Angriff ausging, nicht willens oder in der Lage war gegen die privaten Akteure vorzugehen. Aus diesem Grund müsste dem betreffenden Staat zunächst die Möglichkeit eröffnet werden, sich zu erklären und selbst geeignete Maßnahmen durchzuführen.[101] Aufgrund ihrer Widerlegbarkeit ist die Vermutung im Ergebnis aber eben nicht mehr als eine Umkehr der Beweislast. Darüber hinaus ist eine derartige Umkehr der Beweislast nicht nur im Hinblick auf ihre Vereinbarkeit mit den grundsätzlichen Regeln der Staatenverantwortlichkeit,[102] sondern auch und vor allem im Hinblick auf eine drohende Eskalation bedenklich.[103] Schließlich hilft eine Beweislastumkehr nicht weiter, wenn der Ursprung eines Angriffs gar nicht einem bestimmen Staatsterritorium zugeordnet werden kann.[104]

Das Problem, wie mit dem Umstand der fehlenden Kenntnis über den Ursprung von Cyberattacken umgegangen werden soll, bleibt also weiterhin bestehen. Ein vielversprechender Ansatz könnte hier in der Orientierung am Umweltvölkerrecht liegen, welches ebenfalls mit dem Problem des „Nicht-Wissens" umgehen muss. Im Umweltrecht wird mit guten Gründen das Vorsorgeprinzip (sog. „*precautionary principle*") zur Anwendung gebracht. Demnach müssen Aktivitäten, die schädlich für die Umwelt sind, vermieden und Maßnahmen zur Prävention getroffen werden, und zwar gerade auch dann, wenn Ungewissheit über Kausalität und Auswirkungen der möglicher-

100 Vgl. IGH, *Corfu Channel Case* (United Kingdom v. Albania), Procedures, Urteil vom 25.03.1948, ICJ-Reports 1948, 15; s.a. *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 30 ff. Rule 6 und S. 43 ff. Rule 7 sowie *K. Ziolkowski*, General Principles of International Law as Applicable in Cyberspace, in: K. Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, Tallinn 2013, S. 135, 165 ff. u. 185 ff.

101 *Kolossa*, Cyberraum (Fn. 66), 167; s.a. *Schmitt* (Hrsg.), Tallinn Manual 2.0 (Fn. 52), S. 347 Rule 71, Erläuterung 25.

102 Insoweit kritisch *C. Droege*, Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians, IRCC 94 (2012), 533 (543 f.).

103 Ebenso *Dornbusch*, Kampfführungsrecht (Fn. 1), S. 131 f. u. 229.

104 *Heintschel von Heinegg*, Cyberspace (Fn. 21), S. 159 (172).

weise schädlichen Handlungen besteht.[105] Interessant ist in diesem Zusammenhang Punkt 15 der rechtlich nicht bindenden Rio-Deklaration von 1992, der ausdrücklich dazu auffordert, wissenschaftliche Unsicherheit („*scientific uncertainty*") *nicht* als Vorwand für das Unterlassen wesentlicher präventiver Maßnahmen zur Verhinderung potenzieller zukünftiger Umweltschäden zu nehmen.[106]

Dieser Grundgedanke könnte auch für Cyberoperationen fruchtbar gemacht werden. Nicht mehr der Angriffspunkt wäre entscheidend für die Zuordnung einer Cyberattacke zu einem Aggressor-Staat, sondern es käme im Wesentlichen auf den Schutz vor den mit ihr einhergehenden Auswirkungen an. Vorsorge könnte im internationalen Bereich ein Verbot möglicher schädigender Handlungen zum Inhalt haben, was etwa in ein umfassendes Entwicklungs-, Herstellungs- und Nutzungsverbot für Cyberwaffen münden könnte.[107] Für die Staaten selbst könnte dies allerdings auch bedeuten, dass sie in ihrem eigenen regulativen Netzwerk sicherstellen müssten, dass entsprechende Missbrauchshandlungen des Cyberspace ausgeschlossen würden. Auf völkerrechtlicher Ebene ließe sich insofern an die Etablierung eines Kodex von jedenfalls (halb)verbindlichen Grundsätzen zur Erhöhung der Cybersicherheit denken, deren Einbezug Staaten nur durch strikte Regeln innerstaatlicher Rechtssetzung Folge leisten könnten. Da weder nach nationalem noch nach internationalem Recht die letztlich technischen Probleme der Rückverfolgung vollständig lösbar sind, erscheint ein derartiger Perspektivwechsel von der Repression auf die Prävention besonders vielversprechend.

105 Ausf. *Schulze*, Cyber-„War" (Fn. 6), S. 212 ff. sowie *T. Marauhn*, in: K. Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, Tallinn 2013, S. 465 ff., insb. S. 474 ff.

106 Rio Deklaration über Umwelt und Entwicklung vom 14.06.1992, ILM 31 (1992), 876.

107 Dazu und zum Folgenden auch ausf. *Schulze*, Cyber-„War" (Fn. 6), S. 216 ff.; s.a. *Krieger*, anonymous, 1 (4 ff.).