Selen Yumak

Matrikelnummer: 2560457

Anschrift: Halberg Str. 44

66121, Saarbrücken

Masterarbeit zur Erlangung des Grades eines

„Master of Laws“ (LL.M.) am Europa-Institut der

Universität des Saarlandes

CYBERANGRIFFE IM SINNE DES VÖLKERRECHTS:

EINE UNTERSUCHUNG IM KONTEXT IUS AD BELLUM UND IUS IN BELLO

Betreut von

Univ. Prof. Dr. iur. Thomas Giegerich, LL.M. (Virginia)

Saarbrücken, 21. August 2018

av.selen_ezme@hotmail.com

Abkürzungsverzeichnis

Abs.	Absatz
APuZ	Aus Politik und Zeitgeschichte
Art.	Artikel
ASR	Responsibility of States for internationally wrongful acts (kurz: Articles on State Responsibility)
AVR	Archiv des Völkerrechts
BDGVR	Berichte der Deutschen Gesellschaft für Völkerrecht
BMI	Bundesministerium des Innern
BRJ	Bonner Rechtsjournal
bzw.	beziehungsweise
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CSIS	Center for Strategic and International Studies
DDoS	Distributed Denial of Service
ders.	derselbe
DoS	Denial of Service
Doc.	Document
DÖV	Die Öffentliche Verwaltung
ebd.	Ebenda
FAZ	Frankfurter Allgemeine Zeitung
f.	folgend
ff.	fortfolgende
Fn.	Fußnote
GA	General Assembly
GK	Genfer Abkommen vom 12. August 1949 (I-IV)
Hrsg.	Herausgeber

HuV-I	Humanitäres Völkerrecht- Informationsschriften
HVR	Humanitäres Völkerrecht
i.d.S.	in diesem Sinne
i.S.d.	im Sinne der/des
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the former Yugoslavia
IGH	Internationaler Gerichtshof
IKRK	Internationales Komitee vom Roten Kreuz
ILC	International Law Commission
IP	Internationale Politik (Zeitschrift)
IStGH	Internationaler Strafgerichtshof
IT	Informationstechnik
ITU	International Telecommunication Union
i.V.m.	in Verbindung mit
IZPB	Informationen zur politischen Bildung
JA	Juristische Arbeitsblätter
JFQ	Joint Force Quarterly
Jh.	Jahrhundert
lit.	litera (Buchstabe)
N.	Norm
NJW	Neue Juristische Wochenschrift
NZWehrr	Neue Zeitschrift für Wehrrecht
OPM	Office of Personnel Management
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PCIJ	Permanent Court of International Justice
Res.	Resolution

Rep.	Report
Rn.	Randnummer
S.	Seite
SCADA	Supervisory Control and Data Acquisition
SHAPE	Supreme Headquarters Allied Powers Europe
Sog.	sogenannte (r), (s)
SWP	Stiftung Wissenschaft und Politik
UN	United Nations
UN-Charta	Die Charta der Vereinten Nationen
US DoD	United States of America Department of Defense
usw.	und so weiter
Vgl.	vergleiche
W&F	Wissenschaft und Frieden
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
z. B.	zum Beispiel
ZEuS	Zeitschrift für Europarechtliche Studien
Ziff.	Ziffer
ZP I	Zusatzprotokoll zu den Genfer Konvention vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (Protokoll I) vom 8. Juni 1977
ZP II	Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer nicht internationaler bewaffneter Konflikte (Protokoll II) vom 8. Juni 1977
ZRP	Zeitschrift für Rechtspolitik

A. Einleitung

Seit Jahrhunderten verändert sich unsere Welt sehr schnell – von der Agrargesellschaft über die Industriegesellschaft bis hin zur heutigen Informationsgesellschaft.[1] Dementsprechend ist die Entwicklung der neuen Technologien heute fast überall zu sehen. Bemerkenswert sind die Bereiche von Kommunikation, Verkehr, Industrie, Gesundheit und Militär. Im Zentrum all dessen steht das Internet.[2]

Einerseits stehe die Technologie zugunsten der Menschlichkeit zur Verfügung, andererseits kann sie auch sehr schädlich sein. Damit werden allmählich auch bessere Waffen produziert. Die militärischen Aktivitäten der Staaten steigen an.

Es ist eine bekannte Tatsache, dass die Staaten auch die Computernetzwerke und das Internet zur Rüstung verwenden: Fälle wie der Fall „*Stuxnet*" beweisen, dass sie gerade eine Waffe sein können. In diesem Punkt stellt sich die Frage: Könnten die Kriegsszenen von Science-Fiction-Filmen im wirklichen Leben auch möglich sein?

Bisher sind die Cyberangriffe und ein möglicher Cyberkrieg vielfach in der Literatur im Lichte der abweichenden Meinungen behandelt worden; es besteht aber noch nicht Einigkeit darüber. Denn Regeln im Völkerrecht festzulegen ist nicht einfach, vielmehr wird es oft erst nach langfristigen und schwierigen Prozessen bestimmt.[3]

Diese vorliegende Studie bezieht sieht nicht auf die technische Überprüfung der Cyberangriffe wie die Merkmale von „Cyberangriffen" und „Cyberwaffen", sondern es geht um die Cyberangriffe i.S.d. Völkerrechts. In dieser Arbeit werden damit diese Fragen behandelt; *ob ein Cyberangriff gemäß Art. 2 Ziff. 4 UN-Charta als „Gewalt" angenommen werden kann, ob ein Cyberangriff gegen einen anderen Staat als ein „bewaffneter Angriff" i.S.d. Art. 39 bzw. Art. 51 UN-Charta betrachtet werden kann* und *wie das humanitäre Völkerrecht in den Fällen anzuwenden ist, bei denen die Existenz der Cyberangriffe als bewaffneter Konflikt i.S. der Genfer Konvention angesehen wird.* Anschließend wird untersucht, *ob das geltende Völkerrecht für die Cyberangriffe anwendbar ist oder ob man dafür Neuregelungen braucht.*

---

[1] In diese Richtung auch *Fink*, Recht im virtuellen Raum: Die Rechtsordnung des Cyberspace, in: Odendahl/Giegerich (Hrsg.), Räume im Völker- und Europarecht, 2014, S. 53.

[2] Siehe Anhang 1: Die Grafik über „*Proportion of youth (15-24) using the Internet, 2017*".

[3] *Krieger*, Krieg gegen Anonymus, AVR 50 (2012), S. 2.

I. Der neue Raum im Völkerrecht: Cyberspace

Nach der territorialen Souveränität hat jeder Staat die Verfügungsbefugnis über sein Staatsgebiet.[4] Jeder Staat muss dieses Recht der anderen Staaten respektieren[5] und darf den Gebrauch seines regelwidrigen Staatsgebiets gegen die anderen Staaten nicht zulassen.[6]

Der *virtuelle* Raum „Cyberspace"[7] zeigt sich anders als Staatsgebiete wie Land, Meer, Luft und Weltraum.[8] Er ist nämlich eigenständig und unabhängig.[9] Der Cyberspace enthält die Eigenschaften „*Ubiquität, Mobilität und Anonymität*"[10], weil das von den vielen namenlosen Usern genutzte Internet[11] heute weltweit erreichbar und transportierbar geworden ist. Im Zentrum dieser Technologie stehen Kontrollmechanismen, die durch Menschen entwickelt und geführt werden.[12]

Den Cyberspace nach dem Grenzübergang oder Festlandsockel zu begrenzen, ist nicht möglich. Diese Grenzlosigkeit bedeutet aber nicht, dass es ein Raum ohne staatliche Souveränität oder *res communis omnium* ist.[13] Deshalb muss dieser Begriff im Rahmen des Völkerrechts dringend definiert werden.

Es ist klar, dass man das Völkerrecht im Cyberspace anwenden kann.[14] Auf dem Warschauer Gipfel 2016 wurde auch bestätigt, dass der Cyberspace ein Bereich von Operationen ist, in dem sich die NATO ebenso effektiv verteidigen muss wie in der Luft, an Land und auf See.[15] Tallinn

---

[4] *Arnauld*, Völkerrecht, 3. Auflage, 2016, S. 347, Rn. 793. *Sog. Drei-Elementen-Lehre wurde* von *Jellinek* begründet. Demnach besteht der Staat aus drei Elementen: Nämlich *einem Staatsgebiet, einem Staatsvolk* und *einet herrschenden Staatsgewalt*. Siehe dazu *Jellinek*, Allgemeine Staatslehre, 3. Auflage, 6. Neudruck, 1959, S. 394 ff.
[5] IGH, Urteil vom 27.06.1986 (*Nicaragua II*), ICJ Reports 1986, 14, Ziff. 202.
[6] IGH, Urteil vom 09.04.1949 (*Corfu Channel II*), ICJ Reports 1949, 4, Ziff. 22.
[7] Dieser Begriff wurde zunächst in der Kurzgeschichte *Burning Chrome* (1982) von *William Gibson* benannt, aber durch seinen Roman *Neuromancer* (1984) wurde der Begriff bekannt. Siehe dazu *Schmahl*, Zwischenstaatliche Kompetenzabgrenzung im Cyberspace, AVR 47 (2009), S. 284, Fn. 1.
[8] Dieser Raum kann zeitweise sogar als *fünfte Dimension* bezeichnet werden. In diese Richtung *Heintschel von Heinegg,* Völkerrecht im Cyberraum – Das Tallinn-Handbuch und der Tallinn-2-Prozess, W&F, Dossier 79, 3(2015), S. 5.
[9] *Pichler*, Internationale Zuständigkeit im Zeitalter globaler Vernetzung, 2008, S. 14, Rn. 22.
[10] *Schmahl* (Fn. 7), S. 284 f.
[11] Die Geschichte des Internets beruht auf die militärischen Studien in USA in der 60er Jahre sogar in der 50er Jahre. Siehe zur Einzelheiten und zu ARPANET (*Advanced Research Projects Agency Network),* das der Vorläufer des Internets war. Abrufbar unter: https://de.wikipedia.org/wiki/Chronologie_des_Internets, und https://de.wikipedia.org/wiki/Arpanet (30.03.2018).
[12] *Neuneck/ Reinhold*, Die Militarisierung des Cyberspace, W&F, Dossier 79, 3 (2015), S. 4.
[13] *Heintschel von Heinegg*, Cyberspace-Ein völkerrechtliches Niemandsland? in: Schmidt-Radefeldt/Meissler (Hrsg.), Automatisierung und Digitalisierung des Krieges, 2012, S. 168. Als konkrete Beispiele: Trotz der staatsgebietslosen Eigenschaft können manche Gebiete wie *die Hohe See* oder die *Antarktis* nicht als völkerrechtliches Niemandsland oder staatsgewaltfreies Gebiet bezeichnet werden. Siehe *Schmahl* (Fn. 7), S. 288.
[14] Vgl. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN-Doc. A/68/98, 24.06.2013, Rn. 19 ff.
[15] NATO, Warsaw Summit Communiqué, 09. Juli 2016.

Manual[16] Nr. 1 ordnet diese Sache so an: *„Ein Staat kann innerhalb seines Hoheitsgebiets die Kontrolle über die Cyber-Infrastruktur und Aktivitäten ausüben.“*[17]

Abschließend lassen sich die verschiedenen Definitionen des Cyberspace darstellen. Im Wörterbuch der militärischen und assoziierten Begriffe, das von dem Verteidigungsministerium der Vereinigten Staaten am Juni 2018 veröffentlicht wurde, wird der Cyberspace als „*eine globale Domäne innerhalb des Informationsmediums, die aus der voneinander abhängigen Netzwerken von IT-Infrastrukturen und Bewohnerdaten, einschließlich aus dem Internet, den Telekommunikationsnetzen, den Computersystemen und eingebetteten Prozessoren und Controllern besteht*“, definiert.[18] Die Cyber-Sicherheitsstrategie für Deutschland 2016 definiert ihn als „*den virtuellen Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme*“.[19]

II. Terminologie

Die terminologischen Begriffe müssen klar und deutlich festgelegt werden, um die Normen und Prinzipien darzulegen. Das Völkerrecht ist eine vielfältigen Probleme erfahrende Rechtsordnung. Die Begriffsverwirrung erscheint auch in diesem Punkt als ein Teil der Völkerrechtsproblematik. Obwohl etwa das Gewaltverbot eine der Grundprinzipien des Völkerrechts ist, kann noch heute diskutiert werden, was der Begriff „Gewalt“ bedeutet. Deswegen ist klar, dass die Begriffe über Cyberangriffe im Sinne des Völkerrechts nicht deutlich sind. Sie sind sehr abstrakt; und die rechtliche Position der Cyberangriffe zu bestimmen ist nicht einfach.

Die Informationsgesellschaft ist eine Gesellschaft, die auf den Informations-Kommunikationstechnologien basiert. Fast alle Menschen in der Welt erfahren es – mit Ausnahme der unterentwickelten Länder – und die Staaten wollen immer mehr Informationen über andere Staaten und Völker bekommen, um in der internationalen Gemeinschaft vorne zu sein. Früher brauchten die Staaten den klassischen Geheimdienst zum Erreichen der Informationen, aber heute ist der Cyber-Geheimdienst populärer und einfacher geworden. In diesem Zusammenhang führen heute die Staaten Informationenoperationen, die *„den Einsatz von Information und Informationstechnologie zur Erreichung staatlicher Ziele“*[20] nötig

[16] Siehe unten B IV.
[17] Eigene Übersetzung.
[18] Eigene Übersetzung, *US DoD,* Department of Defense Dictionary of Military and Associated Terms, Juni 2018, S. 59. Abrufbar unter: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (01.07.2018).
[19] *BMI*, Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 46.
[20] *Stein/Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1.

machen. Daneben wollen die Staaten, die die Macht der Cyberangriffe gegenüber dem traditionellen Angriff bemerkt haben,[21] auch heute ihre Offensive und Defensive im Cyberspace durch die Cyberwaffen wie die Viren, USB- Sticks, Softwaren usw. verstärken. Cyber Waffen, insbesondere Hard oder Softwareprodukte, haben die Eigenschaft des „*dual use*" gegenüber den herkömmlichen Waffen. Denn sie können sowohl durch Zivilisten als auch durch das Militär angewendet werden.[22]

Jede bösartige Handlung im Cyberspace kann nicht immer als eine Bedrohung bei einem möglichen Cyberkrieg eingestuft werden. Beobachten wir die Aktionen über den Cyberspace auf der Welt, so ist festzustellen, dass es diverse Völkerrechtsverletzungen wie Cyberterrorismus, Cyberspionage, Cybercrime usw. gibt. Doch werden hier aufgrund des Themas nur Cyberangriffe in Bezug auf das Völkerrecht behandelt.

Cyber Operationen sind nach US DoD *„der Einsatz von Cyberspace-Fähigkeiten, um Ziele im Cyberspace oder durch den Cyberspace zu erreichen"*.[23] Im Tallinn Manual N. 30 ist der Cyberangriff so definiert[24]: *„Ein Cyberangriff ist eine Cyber-Operation, egal ob es sich offensiv oder defensiv richtet, die zu einer Verletzung oder den Tod der Personen oder zu einer Zerstörung der Objekte verursacht."* Die Cyber-Sicherheitsstrategie für Deutschland definiert es so: *„Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."*[25]

Wie gesehen, sind die terminologischen Erklärungen über die Cyberangriffe i.S.d. Völkerrechts sind nicht einstimmig. Dieser Umstand beeinflusst auch den Kampf gegen die Cyberangriffe und den Cyberkrieg.

B. Cyberangriffe in Bezug auf Völkerrecht

Wegen der computergestützten Technologie, die ihre Kraft zu zeigen mit dem Golfkrieg (1990-1991) begonnen ist, ist es klar, dass die Kampftechniken durch die Computerunterstützung und die hohe Informationstechnologie eine neue Dimension erreicht haben.[26] Nach dem Bericht von

[21] Siehe unten C II 3.
[22] *Stadlmeier/Unger*, Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht, in: Schmalenbach (Hrsg.) Aktuelle Herausforderungen des Völkerrechts: Beiträge zum 36. Österreichischen Völkerrechtstag 2011, S. 66.
[23] Eigene Übersetzung, *US DoD* (Fn. 18), S. 60.
[24] Eigene Übersetzung, Tallinn Manual N. 30.
[25] *BMI* (Fn. 19), S. 46.
[26] *Schmitt*, Angriffe im Computernetz und das ius ad bellum, NZWehrr 5 (1999), S. 177; *Heintschel von Heinegg*, Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung, in: Epping/ Fischer/ Heintschel von Heinegg (Hrsg.), FS für Knut Ipsen zum 65. Geburtstag, 2000, S. 131.

CSIS steigen die Zahl der festgestellten Cyberangriffe von Jahr zu Jahr. Im Jahr 2015 lag diese Zahl bei nur 29. Im Jahr 2016 ist sie auf 38 und im Jahr 2017 auf 53 gestiegen.[27]

I. Bisherige hauptsächlichen Vorfälle

1. Estland 2007

Estland ist eine der Staaten, die die höchste Informationstechnologie auf der Welt haben. Estland, das im Jahr 1991 nach dem Zusammenbruch der früheren Sowjetunion seine Unabhängigkeit gewonnen hat, hat im Jahr 2007 mehr als drei Wochen viele Cyberangriffe auf seine Informationssysteme erlebt. Im Hintergrund dieser Angriffe gab es eine Entscheidung der estnischen Regierung vom April 2007, nämlich den Platz der Bronzeskulptur eines Soldaten der Roten Armee in Tallinn zu wechseln. Nach diesem Angriff waren die internetabhängigen Systeme – insbesondere die Webseiten der Staatsorgane und Bankenserver – von Estland wegen der DDoS-Angriffen[28] kollabiert. Obwohl feststeht, dass diese Angriffe aus Russland stammten, konnte die Identität der Angreifer nicht eindeutig festgestellt werden, und ob sie sich auf die Staatsorgane bezogen. Dieser Fall hat gezeigt, dass die Cyberangriffe für die Systeme eines Staates gefährlich sein könnten.[29]

2. Georgien 2008

Im August 2008, also während des Kaukasuskriegs, wobei Konfliktparteien Georgien und Russland sowie von Russland unterstützten Südossetien und Abchasien waren, richteten die Adresse der Cyberangriffen dieses Mal nach dem Staat Georgien, welche auch seine Unabhängigkeit wie Estland nach dem Zusammenbruch der Sowjetunion gewonnen hat.

Dieser Fall ist ähnlich wie der Fall Estland. Der ganze Internet-Service-Provider war kollabiert. Es wurde auch festgestellt, dass der Grund dafür die DDoS Angriffe aus Russland waren. Es ist zweifelhaft, ob der potentielle Angreifer oder die Angreiferinnen im Staatsdienst tätig waren oder im Auftrag von der russischen Regierung eingegriffen haben.[30]

---

[27] Significant Cyber Incidents since 2006, abrufbar unter: https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity (12.01.2018).

[28] DDoS-Angriffe bedeuten das Beseitigung der Nutzbarkeit eines Computers oder eines Netzwerks durch die Cyberangriffe aus mehreren Netzwerken. Siehe dazu *Heintschel von Heinegg,* Cyber-Bedrohungen aus dem Netz, IZPB 326 (2015), S. 25.

[29] *Keber/Roguski*, Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis, AVR 49 (2011), S. 401 f.; vgl. auch das Bekenntnis der russische Jugendorganisation „Naschi", abrufbar unter: https://www.welt.de/wirtschaft/webwelt/article3355416/Kreml-Jugend-bekennt-sich-zu-Attacke-auf-Estland.html (19.07.2018).

[30] *Keber/Roguski,* ebd., S. 402 f.

Der Zweck wäre hier, die Kommunikation des Staats von der Außenwelt abzuschneiden, das Ansehen Staates zu beschädigen und als letztes den Feind einfacher unter Kontrolle zu bekommen. Damit ist klar geworden, dass die Cyberangriffe gleichzeitig zu physischen Angriffen führen könnten.

3. Iran 2010 – Stuxnet

Im Juni 2010 legte der Computerwurm „Stuxnet" die Atomanlagen des Iran lahm, welche mit einem industriellen SCADA Kontrollsystem geschützt wurden. Das System war aus Sicherheitsgründen gegen das globale Internet geschlossen. Deswegen musste Stuxnet Cyberangriff durch einen USB-Stick, der das Virus in dem Computersystem verseuchen kann, geführt werden.[31]

Der Fall Stuxnet als der Computerwurm ist wichtiger als andere. Vor dem Angriff musste man die hohen Kenntnisse über die Systeme und die Computertechnologie haben. Das setzt eine große Finanzierung voraus. So ist davon auszugehen, dass die Cyberangriffe nicht nur eine Arbeit von Hackern sind, sondern ihn auch die Staaten organisieren.[32] Dieser Fall konnte auch wie andere nicht deutlich beleuchtet werden. Aber laut einigen Informationen stehen Israel und USA im Hintergrund des Angriffs.[33]

Durch diesen Angriff wollten sie vielleicht nur auf Atomanlagen zielen; doch könnten dadurch viele Menschen ums Leben kommen oder verletzen.[34] Dieses große Risiko ist fast identisch mit den klassischen Angriffen.[35] Es konnte nicht garantiert werden, dass diese Angriffe nicht dieselben Ergebnisse wie die *Nuklearkatastrophe von Tschernobyl (1986)* oder *Nuklearkatastrophe von Fukushima (2011)* mit sich bringen. Und sogar den schlimmsten Unfall, der in einem Atomkraftwerk passieren kann: die Kernschmelze (nuclear meltdown).

4. Aktuelle Entwicklungen nach 2010

Mit den *Snowden*[36] - Enthüllungen (ab Juni 2013) hat die Welt gelernt, dass die USA mithilfe seines Cybergeheimdienstes globale Computernetzwerke systematisch beobachtet.[37] Dieser

---

[31] *Gaycken*, Cyberwar. Das Internet als Kriegsschauplatz, 2011, S. 177.
[32] *Heintschel von Heinegg* (Fn.13), S. 159; *Gaycken*, ebd., S. 175; *Keber/Roguski* (Fn. 29), S. 404.
[33] *Fink* (Fn. 1), S. 65; FAZ Online (16.01.2011), „Israel testete Stuxnet in geheimer Atomanlage", abrufbar unter: http://www.faz.net/aktuell/politik/ausland/computerwurm-israel-testete-stuxnet-in-geheimer-atomanlage-1573182.html (14.03.2018).
[34] *Fink*, ebd., S. 65.
[35] *Plate*, Völkerrechtliche Fragen bei Gefahrenabwehrmaßnahmen gegen Cyber-Angriffe, ZRP (2011), S. 200.
[36] Zum Einzelheiten, Stichwort „*Edward Snowden*": https://de.wikipedia.org/wiki/Edward_Snowden (29.07.2018).
[37] *Neuneck/Reinhold* (Fn. 12), S. 3.

Fall zeigt, dass ein Staat aus der Ferne viele Daten von anderen Staaten sehr einfach zum Zwecke der Cyberspionage zu sammeln vermag. Aufgrund dieser Technologie kann dieses Beispiel eine neue Tür in den internationalen Beziehungen öffnen.

Man liest jeden Tag in den Nachrichten von einem neuen Cyberangriff. Die folgenden Beispiele, die nach 2010 stattgefunden haben, verdeutlichen es: Im Ukraine-Russland Konflikt wurden die Cyberangriffe wie im Georgien-Fall vorgeblich von Russland gegen Ukraine insbesondere auf den Regierungswebseiten verübt.[38] Mithilfe von Cyberangriffen gegen die Sony Pictures (US-Tochterunternehmen von Sony) wurden die unveröffentlichten Filme und die anderen Daten im Jahr 2014 gestohlen. Es wurde behauptet, dass Nordkorea hinter dem Angriff stehe.[39] Im Jahr 2015 richtete sich ein Cyberangriff auch gegen das Computernetzwerk des Deutschen Bundestages. Nach der Meinung von Experten wurde das gesamte System dadurch defekt.[40] Schließlich wurde im Jahr 2015 ein Cyberangriff aus China durchgeführt, um Personalinformationen der US-Bundesverwaltung (OPM) zu bekommen.[41]

II. Bedrohungspotential und Angriffsformen

Im Alltagsleben benutzen immer mehr Privatpersonen, Unternehmen und öffentliche Institutionen sowie Streitkräfte eines Staats das Internet.[42] Es besteht aber in diesem Punkt das Gefahrenpotenzial bzw. „Sicherheitslücken des Cyberspace".[43] Die Bedrohungen sind vielfältig: Cyberkriminalität, Terrorismus und Cyberspionage sowie Sabotage gegen Infrastrukturen.[44] Somit ist die Gefahr der Cyberangriffe nicht außer Acht zu lassen.

Mit den Cyberangriffen sind Unterbrechung, Verfälschung, Reduzierung oder Eliminierung der Informationen oder Zerstörung der Computersysteme möglich.[45] In der Literatur werden drei verschiedenen Angriffe genannt: Die ersten sind „*syntaktische Angriff*" wie DoS Angriffe, Viren, Würmer, Trojanische Pferde, Logische Bomben, welche Funktionsfähigkeit der Computerbetriebssysteme stören; zweitens es geht um „*semantische Angriffe*", die wie Defacement, Video Morphing in Computersystemen stehende Informationen verfälschen, um

[38] *Schmahl*, Cybersecurity, BDGVR, 47 (2016), S. 160.
[39] *Schmahl*, ebd., S. 161, *Heintschel von Heinegg* (Fn. 28), S. 23.
[40] *Heintschel von Heinegg*, ebd., S. 23.
[41] Vgl. https://www.sueddeutsche.de/digital/us-bundesverwaltung-millionen-us-amerikaner-von-cyber-angriff-betroffen-1.2559663 (19.07.2018).
[42] Siehe Anhang 2: Die Grafik über „*Time spent per day on the Internet, 2018*".
[43] *Heintschel von Heinegg* (Fn. 28), S. 23.
[44] *Schaller*, Internationale Sicherheit und Völkerrecht im Cyberspace SWP-Studie, 2014, S. 5.
[45] *Schmitt* (Fn. 26), S. 178.

in das System einen Fehler hinzuzufügen. Als letztes kommen „*gemischte Angriffe*“ in Betracht, die aus zwei genannten Angriffen bestehen.[46]

Angriffsformen der Cyberangriffe gliedern sich in nicht-intrusive und intrusive Methoden. Falls der Cyberangriff als nicht-intrusiv eingestuft ist, kommt der Eingriff von außen, die Systemfunktion zu stören (wie im Fall von Estland oder Georgien). Im Gegensatz dazu entstehen intrusive Angriffe durch den Eintritt ins Computersystem. Damit wird das Steuerungssystem durch das Schadprogramm verändert oder zerstört (wie der Fall Stuxnet).[47]

In den modernen Gesellschaften haben die Infrastrukturen nunmehr große Bedeutung. Und sie sind mit Hochtechnologie in Betrieb. Ein Angriff gegen eine kritische Infrastruktur kann zu empfindlichem Schäden wie Personen- und Sachschaden führen, wenn z. B. Atomkraftwerke oder Chemiefabriken von fremden Computersystemen zur Explosion gebracht werden. Gleichfalls Zugentgleisungen oder die Flugzeugunfälle kommen in Betracht.[48] Hierbei sind als wichtige Infrastruktur-Bereiche folgende zu erwähnen: Energie- und Trinkwasserversorgung, Gesundheitswesen, Banken- und Finanzsektor[49], Information und Kommunikation.[50] Die kritischen Infrastrukturen nach der Europäischen Kommission sind entsprechend wie folgt verfasst: „*materielle und informationstechnologische Einrichtungen, Netze, Dienste und Anlagegüter, deren Störung oder Vernichtung gravierende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche Wohlergehen der Bürger sowie auf das effiziente Funktionieren der Regierungen in den Mitgliedstaaten hätte sind“.*[51] Diese solche Infrastrukturen basieren auf Computerprogrammen, die meistens eine Internetverbindung voraussetzen. Ebenfalls werden einige öffentliche Dienste im Internet geboten wie z. B. in Deutschland *e-government* oder *e- justice*[52] oder in der Türkei die einzige Webseite „*e-Devlet“*, in dem fast alle öffentlichen Dienste personalisiert abrufbar sind.[53] Und die entwickelten Länder

[46] *Bens*, Cyberwar und völkerrechtliches Selbstverteidigungsrecht, BRJ 2 (2011), S. 149; *Schulze*, Cyber – „War“-Testfall der Staatenverantwortlichkeit, 2015, S. 24.
[47] *Keber/Roguski* (Fn. 29), S. 405 f.
[48] *Ziolkowski*, Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen, HuV-I 21 (2008), S. 203.
[49] Siehe Anhang 3: Die Grafik über „*Penetration of mobile banking, 2018*“.
[50] *Heintschel von Heinegg* (Fn. 28), S. 24.
[51] KOM (2004) 702 „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung” zählt die kritischen Infrastrukturen*: Energieanlagen und -netze, Kommunikations- und Informationstechnologien, Gesundheitswesen, Lebensmittel, Verkehr, Erzeugung, Lagerung und Beförderung gefährlicher Güter, Staatliche Einrichtungen*; vgl. auch Green Paper, 17.11.2005, Doc. COM (2005), 576 final.
[52] *Ziolkowski* (Fn. 48), S. 204.
[53] Für die englischen Informationen über e-Devlet abrufbar unter: https://www.turkiye.gov.tr/bilgilendirme?konu=siteHakkinda.

haben hochentwickelte Infrastrukturen gegen die anderen Länder. Das heißt, dass diese hochentwickelten Länder unter mehr Risiken stehen.
Die Technologie ist nicht stabil, sie entwickelt sich von Tag zu Tag. Keiner weiß, welcher Staat welche Technologie hat. Deshalb bemühen sich die Staaten, hinsichtlich der anderen Sicherheitsnetze immer einen Schritt voraus zu sein. Das bringt mit sich, dass es sich bei den internationalen Beziehungen immer mehr um nicht auf Vertrauen basierenden Beziehungen handelt.

III. Bisherige völkerrechtlichen Entwicklungen

England hat im Jahr 2010 die Cyberangriffe in dem Bericht „Die nationale Sicherheitsstrategie" mit Terrorismus, unkonventionelle Angriffe mit chemischen, nuklearen oder biologischen Waffen sowie mit großen Unfällen Großunfälle oder Naturkatastrophen als eine der wichtigsten Gefahr betrachtet.[54] Dieses Verständnis zeigen auch die USA in ihrem Bericht „Die nationale Sicherheitsstrategie" vom Jahr USA 2017 und fügt hinzu: *„Amerikas Antwort auf die Herausforderungen und Chancen der Cyber-Ära wird unseren zukünftigen Wohlstand und unsere Sicherheit bestimmen."*[55] Demzufolge wurde das United States Cyber Command (USCYBERCOM) am 21. Mai 2010 beauftragt, Operationen im Cyberspace durchzuführen. Am 4. April 2018 hat USCYBERCOM den vollständigen und unabhängigen Kommando-Status bekommen.

Die USA vertreten dabei die Auffassung, dass das Selbstverteidigungsrecht gegen der Gefahren im Cyberspace zweifelsfrei anwendbar sei.[56] Es ist unklar, ob die USA, die unabhängig von der internationalen Gemeinschaft handeln, in solchem Fall dem Grundsatz der Verhältnismäßigkeit beachten.[57]

Russland hat den Entwurf „Convention on International Information Security" im Jahr 2011 in der Vereinten Nationen vorgebracht.[58] Dies zielte darauf, dass die Staaten mehr Verantwortung für die Schutz- und Sicherungspflicht übernehmen sollten.[59] Aber dieser Entwurf wurde

---

[54] A Strong Britain in an Age of Uncertainty: The National Security Strategy, 2010, S. 3, abrufbar unter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (20.04.2018).
[55] The White House National Security Strategy of the United States of America, December 2017, S. 12, eigene Übersetzung, abrufbar unter: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf, S. 12 (20.04.2018).
[56] *Fink* (Fn. 1), S. 69.
[57] Siehe *Plate* (Fn. 35), S. 201.
[58] Der Entwurf „Convention on Internationalen Information", abrufbar unter: http://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf (20.04.2018).
[59] *Fink* (Fn. 1), S. 69.

abgelehnt. China war auch Befürworter dieses Entwurfs.[60] Beide Staaten denken daran, dass das Internet keine unkontrollierte und freie Zone sein dürfe. Vielmehr sollte dafür staatliche Kontrolle geführt werden.[61] Im Gegensatz dazu vertreten Europa und Nordamerika, dass es dabei um eine freie und offene Cyberspace gehe.[62]

Deutschland hat seine Politik in Bezug auf Cyberangriffe mit „Cyber-Sicherheitsstrategie für Deutschland" Politik bestimmt und bereitet sich nicht nur für die Defensive, sondern auch für die Handlungen *„in gegnerischen Netzen"* vor.[63]

Früher herrschte die Meinung vor, dass die Cyberangriffe nur durch die entwickelten Länder durchgeführt werden könnten. Aber heutzutage haben Cyberangriffe wie der aus Nordkorea gegen Sony im Jahr 2014 gezeigt, dass auch die unterentwickelten Länder in der Lage sind, Cyberangriffe zu führen.[64] Es ist deshalb davon auszugehen, dass jeder Staat eigene Maßnahmen trifft und eine eigene Strategie entwickelt. Doch besteht darüber noch nicht Einigkeit im Völkerrecht. Doch wäre Uneinigkeit fatal für das Völkerrecht und den internationalen Frieden.

Obwohl man seit vielen Jahren weiß, dass die computergestützte Informationstechnologie eine Bedrohung für die Staaten sein kann, waren die Staaten insbesondere nach dem Stuxnet-Fall (2010) beunruhigt und haben begonnen, die Maßnahmen gegen die Cyberangriffe zu diskutieren. In ähnlicher Weise behandeln die internationalen Organisationen die Cyberangriffe als das Diskussionsthema. Beispielweise wurde „*die Intrusion Software*" im Jahr 2013 als „*die potentielle Rüstungstechnologie*" in das *Wassenaar-Abkommen für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien* aufgenommen.[65]

Die Generalversammlung hat im Jahr 1998 bei der Resolution von „*Entwicklungen im Bereich der Information und Telekomunikation im Kontext der internationalen Sicherheit*" darauf aufmerksam gemacht, dass die Mitgliedstaaten die Sicherheit im Informationsbereich mit einer breiten internationalen Zusammenarbeit zu gewährleisten hätten.[66] Die Europäische Union hat

---

[60] Siehe Anhang 4: Die Grafik über „*Internet use: regional overwiew, 2018*".
[61] *Bothe*, Stellungnahme zu Rechtsfragen des Cyberwars für den Verteidigungsausschuss des Deutschen Bundestages, Ausschussdrucksache 18 (12) 633, 17.2.2016, S. 3. Siehe auch Anhang 5: Die Grafik über „*Freedom on the Internet 2017*".
[62] *Heintschel von Heinegg* (Fn. 28), S. 27; siehe z. B.: Art. 10 des Grundgesetzes in Deutschland.
[63] *Wiegold*, Cyberwar: Bundeswehr meldet „Anfangsbefähigung zum Wirken", augengeradeaus.net, 05.06.2012.
[64] *Heintschel von Heinegg* (Fn. 28), S. 26.
[65] *Neuneck/Reinhold* (Fn. 12), S. 3.
[66] UN-GA „Developments in the field of information and telecommunications in the context of international security", 04.12.1998, UN Doc. A/RES/53/70.

dagegen ihren Kampf gegen die Cyberangriffe mit „Cyber Europe 2010“ gestartet und weitergeführt.[67] Die EU sieht auch die Cyberangriffe als eine Bedrohung in der internationalen Gemeinschaft an.[68]

IV. NATO

Die Praxis der NATO wäre ein gutes Bespiel für den Kampf gegen die Cyberangriffe.[69] Nach dem Estland-Fall (2007) hat die NATO ihr Interesse über die Cyberangriffe erweitert und dafür neue Entscheidungen getroffen. Im Jahr 2008 wurde die erste Cyber-Verteidigungspolitik der NATO verabschiedet und im Anschluss daran NATO Cooperative Cyber Defence Centre of Excellence Tallinn (CCDCOE) gegründet. Danach hat die NATO ihren Beitrag hinsichtlich Cyberangriffe immer weiterentwickelt. Im Jahr 2010, als der Fall „Stuxnet“ geschah, stellte die NATO beim Lissabon-Gipfel fest, dass Cyberangriffe immer mehr Regierungsbehörden und Infrastrukturen der Staaten mit ansteigendem Tendenz gefährden. Es bestehe daher die Notwendigkeit, die Nato-Kräfte dazu einzusetzen.[70]

Im Jahr 2011 wurde die zweite Cyber-Verteidigungspolitik des NATO angekündigt. Infolgedessen wurde beim Brüsseler Gipfel 2018 die Entscheidung getroffen, dass ein neues Cyberspace Operation Center als Teil der erweiterten Kommandostruktur der NATO notwendig sei.[71]

Nach dem Bemühen der NATO hat die Literatur zwei Handbücher verfasst. Diese Handbücher (*Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013 und *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017) wurden auf Einladung des NATO CCDCOE von einer unabhängigen internationalen Expertengruppe verfasst. Das Ziel war, über die Anwendbarkeit des geltenden Völkerrechts über die Cyberangriffe zu forschen.[72] Sie sind zwar kein offizielles NATO-Dokument, aber dafür kann

---

[67] Siehe zur ersten gesamteuropäische Simulation „Cyber Europe 2010“, abrufbar unter: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce2010 (24.07.2018).

[68] Schlussfolgerungen des Europäisches Rates zu den Themen Migration, Sicherheit und Verteidigung, Arbeitsplätze, Wachstum und Wettbewerbsfähigkeit, Innovation und Digitales sowie zu weiteren Themen, 28. Juni 2018, S. 6: *„Der Europäische Rat betont, dass die Fähigkeiten zur Abwehr von Cybersicherheitsbedrohungen, die ihren Ursprung außerhalb der EU haben, gestärkt werden müssen, und fordert die Institutionen und Mitgliedstaaten der EU auf, die in der Gemeinsamen Mitteilung genannten Maßnahmen umzusetzen, einschließlich der Arbeit an der Zuordnung von Cyberangriffen und der praktischen Anwendung der Cyber Diplomacy Toolbox“.*

[69] Vgl. *Heintschel von Heineg,* (Fn. 8), S. 5; siehe auch *Cyber Security Strategy Documents*, abrufbar unter: https://ccdcoe.org/cyber-security-strategy-documents.html (29.07.2018).

[70] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Adopted by Heads of State and Government in Lisbon, 19/20.11.2010.

[71] Zur Einzelheiten, Cyber defense, abrufbar unter: https://www.nato.int/cps/en/natohq/topics_78170.htm (27.07.2018).

[72] *Heintschel von Heinegg* (Fn. 8), S. 5.

es als ein detaillierter Kommentar zur Diskussion über Cyberangriffe i. S. d. Völkerrechts bezeichnet werden.[73] Im Tallinn-Handbuch sind die Regeln in Bezug auf *ius ad bellum* und *ius in bello* niedergelegt.

Art. 38 IGH- Statut[74] zählt die Völkerrechtsquellen. Das Tallinn-Handbuch ist i. d. S. natürlich nicht verbindlich. Da es von der internationalen Expertengruppe geschrieben wurde, ist es aber wertvoll. Man kann in der Praxis und den Entscheidungen darüber diskutieren, ob dieses Handbuch zumindest als eine Hilfsquelle angesehen werden könnte.

Ist wegen eines Cyberangriffs einen Staat zur Verantwortung zu ziehen, so kann Art. 5 des NATO-Vertrags berufen werden. Falls der Cyberangriff gegen einen NATO-Mitgliedstaat als ein bewaffneter Angriff angenommen wird, wird es nach diesem Artikel so betrachtet, dass dieser Cyberangriff sich gegen alle NATO-Mitgliedstaaten richtete. Somit könnten notwendige Maßnahmen durch NATO-Mitgliedstaaten getroffen werden.[75]

C. Cyberangriffe im Lichte des Ius ad bellum

I. Überblick zur Staatenverantwortlichkeit

Die „Völkerrechtssubjektivität“[76] als Träger von völkerrechtlichen Rechte und Pflichten setzt die Deliktsfähigkeit voraus.[77] Auf diese Weise können die Verantwortlichkeit der Staaten gegen völkerrechtswidrige Verhalten in Betracht kommen. Diese Verantwortlichkeit ergibt sich aus dem »Völkergewohnheitsrecht«[78] und seine Grundlagen basieren auf dem Grundsatz von »souveräner Gleichheit der Staaten«.[79]

Eigentlich wollte die ILC die Staatenverantwortlichkeit auf das Vertragsrecht zu verschieben; aber es hatte keinen Erfolg. Die UN-Generalversammlung hat sich im Jahr 2001 entsprechend

---

[73] Vgl. *Bothe* (Fn. 61), S. 3 und siehe *Heintschel von Heinegg,* ebd., S. 5: *„…Die Abschnitte über das völkerrechtliche Gewaltverbot und das Selbstverteidigungsrecht wurden als Anerkennung der so genannten Bush-Doktrin diffamiert, obgleich die den Regeln beifügten Kommentierungen das gesamte Spektrum der diesbezüglich vertretenen Positionen widerspiegeln. Daher kann keine Rede davon sein, die besonderen Charakteristika des Cyberraums seien zu dem Zweck missbraucht worden, einer präemptiven Gewaltanwendung das Wort zu reden.“*

[74] Die Völkerrechtsquellen werden in Art. 38 Abs. 1 IGH – Statut aufgelistet: Völkerrechtliche Verträge, Völkergewohnheitsrecht, allgemeine Rechtsgrundsätze und als die Hilfsquellen richterliche Entscheidungen sowie Lehrmeinung.

[75] *Bothe* (Fn. 61), S. 7.

[76] Internationale Beziehungen dominieren das Völkerrecht. So sind die Staaten Hauptakteure. Deshalb werden sie als „*originäre*“ bzw. „*geborene*“ Völkerrechtssubjekte dargestellt. Siehe *Herdegen*, Völkerrecht, 16. Auflage, 2017, S. 74; *Stein/von Buttlar/Kotzur,* Völkerrecht, 14. Auflage, 2017, S. 79, Rn. 244.

[77] *Hobe*, Einführung in das Völkerrecht, 10. Auflage, S. 314; *Arnauld* (Fn. 4), S. 22, Rn. 58.

[78] *Schöbener*, Verantwortlichkeit, völkerrechtliche, in: ders. (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, 2014, S. 485, *Stein/von Buttlar/Kotzur* (Fn. 76), S. 415, Rn. 1101.

[79] *Stein/von Buttlar/Kotzur,* ebd., S. 416, Rn. 1103, Art. 2 Ziff. 1 UN-Charta: *„Die Organisation beruht auf dem Grundsatz der souveränen Gleichheit aller ihrer Mitglieder“.*

mit der Resolution 56/83[80] befasst. Trotz dieser Versuche bleibt ASR einerseits eine unverbindliche Völkerrechtsquelle.[81] Auf der anderen Seite sind sie ein wichtiger Teil des Völkergewohnheitsrechts geworden.[82]

Eine der wichtigsten Fragen der Arbeit ist die völkerrechtliche Betrachtung der Cyberangriffe im Sinne des Gewaltverbots. Im Art. 1 ASR wird geregelt: „*Jede völkerrechtswidrige Handlung eines Staates hat die völkerrechtliche Verantwortlichkeit dieses Staates zur Folge.*“ Das Gewaltverbot ist die Primärpflicht der Staaten.[83] Im Weiteren wird nach Art. 2 ASR bestimmt: „*Eine völkerrechtswidriges Handlung eines Staates liegt vor, wenn ein Verhalten in Form eines Tuns oder eines Unterlassens: a) dem Staat nach dem Völkerrecht zurechenbar ist und b) eine Verletzung einer völkerrechtlichen Verpflichtung des Staates darstellt.*“ Handelt es sich um eine Verletzung gegen das Völkerrecht, so haben die Staaten zuerst die Pflicht, den Konflikt widergutzumachen (die Sekundärpflicht der Staaten).[84]

Nach der Beweislage wird die Zurechnungsfähigkeit der Staaten ermittelt, aber die Cyberangriffe hinterlassen sich kein Indiz, und sogar ihre Bestimmung ist schwierig. Ohne Beweis macht ein Verdacht gegen einen Staat keinen Sinn vor dem Gericht.

Die heutige Informationstechnologie bietet auch die Irreleitungsmöglichkeit der Identität im Internet.[85] Jeder Computer hat eine sog. IP-Adresse.[86] Es geht aber auch um die Möglichkeit, mithilfe von sog. Zombie-Programmen die anderen IP-Adresse und die Daten zu verfälschen. Dadurch können die von Ferne kontrollierten Computer für illegale Zwecke genutzt werden.[87] Da zwar bei Cyberangriffen die Identität des Angreifers oder der Angreiferinnen festzustellen problematisch ist, ist aber der geografischer Ort festzulegen möglich.[88] Nach Tallinn Manual N. 8 ist die Feststellung des Ursprungsgebiets der Cyberangriffe nicht genug, den Angriff zu dem Staat diesem Territorialgebiet zuzurechnen. Wie bei den Fällen Estland oder Georgien gezeigt, ist, auch wenn der Angriffsort schon bestimmt ist, der Angriff dem Staat vorzuwerfen nicht direkt möglich. Außerdem nach dem Art. 11 ASR bedeutet das Annehmen des Verhaltens

[80] Verantwortlichkeit der Staaten für völkerrechtswidrige Handlungen vom 12. Dezember 2001, zitiert auf Deutsch aus Sartorius II, Internationale Verträge Europarecht Textsammlung, Lieferung 58, März 2016, Nr. 6.
[81] *Schöbener* (Fn. 78), S. 485.
[82] *Stein/Marauhn* (Fn. 20), S. 3 f.
[83] *Arnauld* (Fn. 4), S. 160. Rn. 377.
[84] IGH, Urteil vom 13.09.1928 (*Chorzów III*), PCIJ Series A No. 17, Ziff. 29 und 47. Siehe zur Sekundärpflicht der Staaten *Arnauld*, ebd., S. 160, Rn. 377.
[85] *Ziolkowski* (Fn. 48), S. 204.
[86] IP-Adresse (Internet Protocol Adresse) werden zur Identifizierung der internetabhängigen Geräte wie das Computer genutzt. Es ist notwendig, um zwischen Computern eine Kommunikation anzuknüpfen. Zur Einzelheiten, *Hoeren/Bensinger* (Hrsg.), Haftung im Internet, 2014, S. 186 f.
[87] *Ziolkowski* (Fn. 48), S. 204 f.
[88] *Heintschel von Heinegg* (Fn. 13), S. 172.

durch einen verantwortungsvollen Staat, dass dieses fragliche Verhalten von diesem Staat ausging.

Die Grenzen der Technologie sind heutzutage sehr weit. Kostenfreie oder billige Nutzung des Internets ermöglicht, die Cyberangriffe einfacher zu führen.[89] In diesem Punkt ist fragwürdig, ob ein Staat wegen der Cyberangriffe von nicht-staatlichen Personen oder Gruppen schuldig ist, ob der durch diesen Angriff verletzte Staat dagegen vom Selbstverteidigungsrecht Gebrauch machen darf.[90] Beispielsweise hat die russische Jugendorganisation „Naschi" den Angriff übernommen, aber Russland war für diese Handlung nicht verantwortlich..

Nach Art. 8 ASR hat der Staat die Verantwortung gegen das Handeln von den nichtstaatlichen Aktoren, wenn die völkerrechtswidrige Handlung unter der Kontrolle dieses Staates begangen wird. Das umfasst sowohl die operationale Kontrolle als auch effektive Kontrolle des Staates.[91] Nach IGH ist die Verantwortung in diesem Fall nur unter der „effektiven Kontrolle" eines Staates möglich.[92] aber in der Judikatur gibt es auch die Auffassung, die die „operationale Kontrolle" einer Staat als genügend betrachtet.[93] Es ist heute die Tatsache, dass die Staaten nun mit den nicht-staatlichen Akteure wie den Hackern zusammenarbeiten, im Cyberspace anzugreifen.[94] Als Beispiel dafür können die Fälle von Estland und Georgien gegeben werden.

Wie schon erwähnt, die Zurechenbarkeit erscheint als das größte Problem für die Cyberangriffe. Zur Anwendung der völkerrechtlichen Regeln ist es zweifellos notwendig;[95] andernfalls findet das Völkerrecht als die Rechtsordnung keine Anwendung.

II. Cyberangriffe und ihre Zusammenhänge mit dem Gewaltverbot

1. Die Entwicklung und allgemeine Grundsätze des Gewaltverbots

> ***„Der Streit der Staaten kann (…), insofern die besonderen Willen keine Übereinkunft finden, nur durch Krieg entschieden werden."[96]***

Obwohl das Völkerrecht weitgehend die Lösungswege für die internationalen Streitigkeiten ordnet, können die Staaten noch heute die „Gewalt" – sei es die klassische Form, seien es die

[89] *Ziolkowski* (Fn. 48), S. 204.
[90] Siehe zur diese Diskussion, Tallinn Manual, S. 58 f.
[91] *Stadlmeier/ Unger* (Fn. 22), S. 70.
[92] *Herdegen* (Fn. 76), S. 265, Rn. 24.
[93] ICTY, Urteil vom 15.07.1999, Prosecutor v. Tadic. Case IT-94-1-T, Judgment and Opinion; *Stadlmeier/Unger*, (Fn. 22), S. 70.
[94] *Heintschel von Heinegg* (Fn. 28), S. 23.
[95] *Krieger* (Fn.3), S. 3.
[96] *Hegel*, Grundlinien der Philosophie des Rechts, §334, 1986, S. 500.

anderen Formen – anwenden, um ihre internationalen Konflikte zu beenden. So sucht das *ius ad bellum* die Antwort, ob der Staat militärische Gewalt anwenden darf (sog. „ob" Frage).[97]

Theologen des Mittelalters wie *Augustinus v. Hippo, Thomas von Aquin* entwickelten die Theorie des gerechten Krieges (*bellum iustum*). Es gibt aber nach dieser Theorie keinen Maßstab, wonach ein Staat den Krieg erklärt.[98] Der Ausdruck von *Carl von Clausewitz* wäre ein Wegweiser dieser Theorie: *„Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen."*[99]

Die Haager Abkommen, deren erstes im Jahr 1899 und das zweite im Jahr 1907 verabschiedet wurden, zeigen sich als ein wichtiger Schritt für die Völkerrechtsgeschichte i.S.d. humanitären Völkerrechts. In diesen Abkommen wurde das Gewaltverbot nicht geregelt. Sie beziehen sich das auf das Recht im Krieg (*ius in bello*) und die friedliche Streitbeilegung. Es geht um nur einen Artikel in dem zweiten Abkommen (sog. *Drago-Porter-Konvention*), der das eingeschränkte Gewaltverbot hinsichtlich der Eintreibung von Vertragsschulden vorgesehen ist.[100]

Die Satzung des Völkerbundes wurde im Jahr 1920 verfasst und diente als der einzige Völkerbund bis zum 1946. Der Bund hat eigentlich die Absicht, den Krieg einzudämmen. Die Satzung hat deswegen versucht, ein Schritt weiter zur Seite des Gewaltverbots zu gehen. Es war aber nicht genug. Sie konnte nicht für das allgemeine Kriegsverbot sprechen. Vielmehr hat sie *„den Aufschub des Kriegs"* vorgesehen.[101]

Mit dem *Briand-Kellog-Pakt* wurde endlich das allgemeine Kriegsverbot geregelt. Es hat aber weder die Durchsetzungskraft noch Schutzmechanismen gegen anderen Gewaltakte außer Krieg.[102] Trotzdem ist dieser Pakt ohne Zweifel als ein wichtiger Wendepunkt zu betrachten.[103]

---

[97] *Arnauld* (Fn. 4), S. 516, Rn. 1151.
[98] *Stein/von Buttlar/Kotzur* (Fn. 76), S. 285, Rn. 768; *Randelzhofer*, Art. 2 Ziff. 4, in: Simma (Hrsg.), Charta der Vereinten Nationen, 1991, S. 69, Rn. 3.
[99] *Clausewitz*, Vom Kriege, 1987, S. 13.
[100] *Arnauld* (Fn. 4), S. 457, Rn. 1026.
[101] *Randelzhofer* (Fn. 98), S. 70, Rn. 7; Art. 12 Abs. 1 der Satzung des Völkerbundes: *„Alle Bundesmitglieder kommen überein, eine etwa zwischen ihnen entstehenden Streitfrage, die zu einem Bruche führen könnte, entweder der Schiedsgerichtsbarkeit oder der Prüfung durch den Rat zu unterbreiten.* ***Sie kommen ferner überein, in keinem Fall vor Ablauf von drei Monaten nach dem Spruch der Schiedsrichter oder dem Berichte des Rates zum Kriege zu schreiten****".*
[102] *Stein/von Buttlar/Kotzur* (Fn. 76), S. 287, Rn. 772.
[103] *Dörr,* Gewalt und Gewaltverbot im modernen Völkerrecht, APuZ B 43 (2004), S. 14.

Das Gewaltverbot ist mit Recht einer *der wichtigsten jungen Errungenschaften*[104] des Völkerrechts des 20. Jh. Es ist neu, weil das Gewaltverbot oder wenigstens das Kriegsverbot nicht von der Charta der Vereinten Nationen (UN-Charta) deutlich vorgesehen wurde.[105]

Nach der Auflösung des Völkerbundes wurden die Vereinten Nationen im Jahr 1945 gegründet und endlich das allgemeine Gewaltverbot ist im Art. 2 Ziff. 4 UN-Charta zum Ausdruck gebracht. Diese Form gilt auch für heute. Dies wird als ein wichtiger Schritt angesehen, die von der internationalen Gemeinschaft anerkannt wird.[106] Das Völkerrecht umfasst somit nicht nur das Kriegsverbot, sondern auch das Gewaltverbot.

Der erste Zweck der Vereinten Nationen ist nach dem Art. 1 Ziff. 1 UN-Charta: *„den Weltfrieden und die internationale Sicherheit zu wahren"*. Aus diesem Grund sieht der Art. 2 Ziff. 4 UN-Charta „*das allgemeine Gewaltverbot"* vor.[107]

Das Gewaltverbot hat *den gewohnheitsrechtlichen Ursprung*[108] und es orientiert sich am „*ius cogens*".[109] Es geht also dabei um eine zwingende Völkerrechtsnorm. Dieses Verbot gilt nicht nur für die Mitglieder der Vereinten Nationen, sondern auch für alle Staaten auf der Welt. Ebenfalls bringt das Gewaltverbot eine „*erga omnes"*[110]-Pflicht.[111]

2. Anwendungsschwierigkeiten des Art. 2 Ziff. 4 UN-Charta

Ein Gewaltverbot ist ohne Zweifel nötig, den Zweck der Vereinten Nationen in Bezug auf die internationale Sicherheit zu erfüllen. Fast alle Staaten auf der Welt sind heute Mitglieder der Vereinten Nationen. Wenn es so ist, warum stellt dann das Gewaltverbot heute noch ein so großes Problem dar? Das Gewaltverbot bringt viele Probleme mit sich und die Anwendungsschwierigkeiten wie „die Bedeutung der Androhung von Gewalt?", „die Begrenzung des Art 2 Ziff. 4 UN-Charta hinsichtlich des Anwendungsbereichs in

---

[104] *Dörr*, ebd., S. 14.
[105] Vgl. *Randelzhofer* (Fn. 98), S. 69, Rn. 3.
[106] *Dörr* (Fn. 103), S. 14.
[107] Siehe dazu *Hobe* (Fn. 77), S. 251.
[108] *Nicaragua II* (Fn. 5), Ziff. 188 ff.; IGH, „Mauer "-Gutachten vom 09.07.2004, Ziff. 87.
[109] Siehe auch Art. 53 des Wiener Übereinkommens über das Recht der Verträge von 1969, Sartorius II (Fn. 80), Nr. 320.
[110] Die manche Völkerrechtsnormen verpflichten die ganze internationale Gemeinschaft (Erga-Omnes-Wirkung), siehe IGH, Urteil vom 05.02.1970 (Barcelona Traction II), ICJ Reports 1970, 3, Ziff. 33., Vgl. auch *Funke*, Erga omnes-Pflichten, in: Schöbener (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, 2014, S. 83f. Jede ius cogens Norm hat die erga omnes Wirkung; aber jede erga omnes wirkende Norm ist nicht immer ius cogens. Siehe dazu *Funke*, Ius cogens-Normen, in: Schöbener (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, 2014, S. 250.
[111] *Schöbener*, Gewaltverbot, universelles, in: ders. (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, 2014, S. 127.

internationalen Beziehungen“ und „der Unterschied zwischen Gewaltanwendung und präventivem Selbstverteidigungsrecht“.

Wie beim jeden Rechtsgebiet spielt die Terminologie eine maßgebende Rolle im Völkerrecht. Der Begriff „Gewalt“ bezieht sich an erster Stelle auf bewaffnete militärische Gewalt *(auf Englisch armed force)*.[112] Gleichfalls die Definition des Begriffs „Waffen“ existiert in der UN-Charta nicht.[113] Die Vereinten Nationen wollte dieses Defizit mit der Resolution *„Definition der Aggression“* ebenso mit der *„Friendly Relations“*- Declaration zu beseitigen. Dies hatte aber das Problem nicht gelöst.[114]

Außer der militärischen bzw. konventionellen Gewalt geht es auch um andere nicht-klassische Formen wie die Cyberangriffe. Falls man den terminologischen Begriff „Gewalt“ nur als militärisch i. S. v. militärischer Praxis versteht, so finden andere nicht-physische Formen keine Anwendung. Wenn ein Instrument außer konventionellen Mitteln als Waffe eingesetzt wird, wäre das Verständnis, das unter der Waffe nur militärische Geräte versteht und demgemäß die anderen Instrumente nicht als Waffe zu qualifizieren, nicht sachgerecht.[115] Aufgrund dieser terminologischen Unbestimmtheit muss der Art. 2 Ziff. 4 UN-Charta dafür entsprechend nochmal interpretiert werden, um dieses Problem zu bewältigen.[116] Die Entwicklungen in der heutigen Zeit erfordern diese Methode.[117] Die UN-Charta braucht auch eine Änderung, weil die UN-Charta, deren 73. Geburtstag in diesem Jahr gefeiert wird, die heutigen Bedürfnisse der Staaten erfüllen muss.[118] Die Cyberangriffe nach Infrastrukturen bewiesen, dass sie für die Menschenleben und Gesellschaft gefährlich sein könnten.[119]

3. Lassen die Cyberangriffe sich als Gewalt im Sinne des Art. 2 Ziff. 4 UN-Charta betrachten?

Ob Cyberangriffe gegen das Gewaltverbot verstoßen können oder nicht, ist eine aktuelle und umstrittene Frage des heutigen Völkerrechts. Außer dieser Frage ist es eine Tatsache, dass viele Staaten entsprechende Maßnahmen gegen die Cyberangriffe suchen. Da es zurzeit sehr wenige

---

[112] *Keber/Roguski* (Fn. 29), S. 406 f.
[113] Vgl. auch IGH, Gutachten vom 08.07.1996 (*Nuclear Weapons*), ICJ Reports 1996, 226, Ziff. 39.
[114] GA Res. 3314 (XXIX) „Definition der Aggression“ vom 14.12.1974, Sartorius II (Fn. 80), Nr. 6; GA Res. 2625 (XXV) „Friendly Relations“- Deklaration vom 24.10.1970, Sartorius II (Fn. 80), Nr. 4; *Randelzhofer* (Fn. 98), S. 72, Rn. 14.
[115] Vgl. *Stein/Marauhn* (Fn. 20), S. 4; *Arnauld* (Fn. 4), S. 460, Rn. 1032.
[116] In diesem Punkt ist der Art. 32 „*Ergänzende Auslegungsmittel*“ des Wiener Übereinkommens über das Recht der Verträge vom 23.05.1969 zu berücksichtigen, Sartorius II (Fn. 80), Nr. 320.
[117] IGH, Urteil vom 13.07.2009 (*Costa Rica v. Nicaragua*), ICJ Reports 2009, S. 213, Ziff. 66.
[118] Dieses Thema wird seit Jahren diskutiert. Siehe dazu: https://www.unric.org/de/aufbau-der-uno/46 (20.04.2018).
[119] Vgl. Ziolkowski (Fn. 48), S. 208.

Bemühungen dazu gibt, braucht die internationale Gemeinschaft Rechtsregeln für die Cyberangriffe i.S.d. Völkerrechts.

Einerseits können die Fälle wie Estland 2007 als eine Verletzung des Interventionsverbots nach dem Art. 2 Ziff. 7 UN-Charta gesehen werden, andererseits können die Fälle wie Stuxnet 2010 nicht direkt als einen Verstoß gegen Interventionsverbot akzeptiert werden. Der Stuxnet-Fall vom Jahr 2010 hat seine vernichtende Wirkung wie bei den Fällen von herkömmlichen Waffen bewiesen. Trotz dieser Tatsache wird diskutiert, ob die Schwelle des Gewaltverbots in diesen Fällen noch überschritten wird.[120] Obwohl eine Verletzung gegen das Gewaltverbot in der gleichen Zeit eine Handlung gegen das Interventionsverbot darstellt, ist aber nicht jeder Verstoß gegen das Interventionsverbot als eine Verletzung des Gewaltverbots anzusehen.[121]

Es gibt verschiedene Meinungen über den Platz der Cyberangriffe im Völkerrecht. Die erste Meinung geht davon aus, dass der Cyberkrieg heute eine große Bedrohung für die Menschlichkeit sei. Unsere Infrastrukturen sind in diesem Sinne in Gefahr. Der bekannteste Vertreter dieser Ansicht ist *Richard A. Clarke*. Die andere Meinung glaubt daran, dass die erste Meinung zu Unrecht dramatisiert werde. Ein möglicher Cyberkrieg wäre nach dieser Ansicht nur eine Vorstellung, die zur Erwerbsgrundlage für die Cybersicherheitsindustrie und Hochtechnologiewaffen führt. Der bekannteste Vertreter dieses Standpunktes ist *Thomas Rid*.[122]

Der andere entscheidende Punkt ist Art. 41 der UN-Charta, in dem die von dem Sicherheitsrat außer der Waffengewalt ergriffenen Maßnahmen geregelt werden. Darin ist als Maßnahme die vollständige oder teilweise Unterbrechung der Kommunikationsverbindungen vorgesehen. Wenn man IT – ebenso das Internet und die Computerdaten – als ein Kommunikationsmittel betrachtet, dann sind die Cyberangriffe i.S.d. UN-Charta nicht als bewaffnete Angriffe zu akzeptieren. Aber die betreffenden Maßnahmen *„unter Ausschluss von Waffengewalt“* zeigen sich auch bei kritischen Infrastrukturen. Tallinn Manual N. 5 überträgt die Verantwortung den Staaten, dass ein Staat die Anwendung seiner Cyber-Infrastruktur gegen andere Staaten nicht erlaubt.

Im Rahmen der Reformüberlegungen von UN-Charta wird diskutiert, ob auch die Cyberangriffe als Waffengewalt eingestuft werden sollten. Hierbei ist aber nicht zu vergessen,

[120] Vgl. *Hobe* (Fn. 77), S. 253.
[121] *Arnauld* (Fn. 4), S. 459, Rn. 1031.
[122] *Glenny*, Das Ende der Nettigkeiten, IP 6 (2012), S. 81 f.

dass es hier ein Detail gibt: Als die UN-Charta im Jahr 1945 unterschrieben war, konnte man nicht im Lichte von heutigen Informationssystemen Regelungen verfassen.[123]

Nach einer Meinung in der Literatur wird die These vertreten, dass nicht das Angriffsmittel, sondern die Wirkung des Cyberangriffs maßgebend sei (*Effekt-Äquivalenz*).[124] Also können die Cyberwaffen im Vergleich zu konventionellen Waffen „*vergleichbare Schäden* " verursachen.[125] Es wird auch als *„scale and effects"* (Umfang und Wirkung) bezeichnet.[126] Tallinn Manual N. 11 nimmt dieses Kriterium an. Nach Experten des Tallinn-Handbuchs finden die Angriffe, die keine beträchtlichen Schäden verursachen, keinen Platz im Rahmen des Begriffs „Gewaltanwendung".[127] In diesem Zusammenhang kann man sicherlich sagen, dass Stuxnet als Gewalt und Aggressionsmittel genutzt wurde, weil ihre höchstwahrscheinlichen Schäden im Falle der Explosion der Kernkraftwerke aufgrund *„scale and effects"* ohne Unterschied mit den konventionellen Waffen entstanden.

Zwischen den Cyberangriffen und konventionellen Angriffen handelt es sich um einige Unterschiede: Erstens, Cyberangriffe können mit Lichtgeschwindigkeit realisiert werden. Ihre Effekte sind mit konventionellen Waffen[128] vergleichbar. Zweitens, die Kosten der Cyberangriffe sind geringer als die der konventionellen Waffen (Low- Cost[129]). Letztendlich ist es nicht einfach, diese wegen der Handlung zuzurechnen und die Absicht des Gegners festzustellen.[130]

Der Vergleich zwischen den Cyberangriffen und biologischen und chemischen Waffen (BC-Waffen) und die Atomwaffen[131] ist auch wichtig. BC-Waffen sind keine konventionellen Waffen, aber sie haben vernichtende Wirkung. Nach der herrschenden Meinung wird der Gebrauch von BC-Waffen als Gewaltanwendung i.S.d. Art. 2 Ziff. 4 UN-Charta betrachtet. Denn sie bedrohen das Leben der Menschen.

---

[123] *Keber/Roguski* (Fn.29), S. 407.
[124] *Keber/Roguski,* ebd., S. 408.
[125] *Stein/Marauhn* (Fn. 20), S. 7.
[126] *Bothe* (Fn. 61), S.1.
[127] *Heintschel von Heinegg* (Fn. 8), S. 6.
[128]Siehe, Konvention über bestimmte konventionelle Waffen (Convention on Certain Conventional Weapons, CCW) – 1980; Ottawa-Konvention über das Verbot von Antipersonenminen (Ottawa Treaty) – 1997, Sartorius II (Fn. 80), Nr. 58.
[129] Vgl. *Lacho/Richardson*, Terrosit Use of the Internet The Real Story, JFQ 45, 2 (2007), S. 100 f.
[130] *Todd*, Armed Attack in Cyberpace: Deterring Asymmetric Warfare with an Asymmetric Definiton, Air Force Law Review 64, 2009, S. 68 f.; vgl. auch *Keber/Roguski* (Fn. 29), S. 399.
[131] Vgl. Biowaffenkonvention (Biological Weapons Convention) – 1972, Sartorius II (Fn. 80), Nr. 64; Chemiewaffenkonvention (Chemical Weapons Convention) – 1993, Sartorius II (Fn. 80), Nr. 63; Atomwaffensperrvertrag (Nuclear Non-Proliferation Treaty) – 1968, Sartorius II (Fn. 80), Nr. 60.

Es ist heute klar, dass die Flugzeuge durch Cyberangriffe abgestürzt werden könnten. So lassen sich auch die Atomkraftwerke dadurch zur Explosion bringen. In diesem Punkt kommt eine Frage in Betracht: Warum könnte die Auffassung bezüglich der BC-Waffen nicht auch für die Cyberangriffe angenommen werden?[132]

III. Ausnahmen von Gewaltverbot im Sinne der Cyberangriffe

„summum ius summa iniuria"[133]

Das Gewaltverbot als ein absolutes Prinzip im Völkerrecht zu denken, ist nicht immer richtig. In einigen Fällen ist erlaubt, die Gewalt durch einen Staat oder die Staaten anzuwenden, sonst widerspricht dieses Prinzip dem Gerechtigkeitsgedanken.

1. Der Selbstschutz von Staaten gegen Cyberangriffe

a. Das Selbstverteidigungsrecht

Die erste Ausnahme des Gewaltverbots wird im Art. 51 der UN-Charta und im Art. 21 ASR gefunden. Das Selbstverteidigungsrecht findet ihre Grundlagen erst *im Caroline-Fall* v. 1837.[134] Für diesen Fall hat der ehemalige amerikanische Außenminister *Daniel Webster* die Voraussetzungen über das Selbstverteidigungsrecht so formuliert *(sog. Webster-Formel)*: *eine unmittelbare, überragende Notwendigkeit zur Selbstverteidigung, die keine Wahl der Mittel und keine Zeit zu weiterer Überlegung lässt.*[135]

Diese Ausnahme beruht auf die Souveränität der Staaten. Indem die Staaten ihr Selbstverteidigungsrecht in Anspruch nehmen, machen sie ihr Souveränitätsrecht geltend und schützen damit ihre Souveränität. Im Art. 51 UN-Charta steht, dass dieses Recht *naturgegeben* ist. Das Selbstverteidigungsrecht stellt also die *völkergewohnheitsrechtliche* Besonderheit dar.[136]

Um das Selbstverteidigungsrecht auszuüben, muss es zunächst einmal einen bewaffneten Angriff geben. Im Anschluss daran muss dieser Angriff aktuell sein. Danach hat der betroffene Staat den Fall dem Sicherheitsrat mitzuteilen. Letztendlich muss die Ausübung des

---

[132] Ziolkowski (Fn. 48) S. 206; *Heintschel von Heinegg* (Fn. 26), S. 138.
[133] *Cicero*, De Officiis. I, 10, 33. Siehe auch *Dörr* (Fn. 103), S. 15.
[134] Über den Caroline Fall siehe *Kreß/Schiffbauer*, Erst versenkt, dann zu Völkerrecht erhoben, JA 2009, 611 ff.; *Heintschel von Heinegg*, Casebook Völkerrecht, 2005, S. 202 ff.
[135] *Kreß/Schiffbauer*, ebd., S. 612; siehe Tallinn Manual Nr. 14 und 15.
[136] *Hobe* (Fn. 77), S. 260; *Arnauld* (Fn. 4), S. 480, Rn. 1075.

Selbstverteidigungsrechts verhältnismäßig sein.[137] Es darf *unmittelbar* und gegen den *gegenwärtigen* und *rechtswidrigen* bewaffneten Angriff des Feindstaates verwendet werden.[138]

Dieses Recht hat den *subsidiären* Charakter; denn die Anwendung dieses Recht *„…bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat (Art. 51 UN-Charta)"* gilt. Erforderliche Maßnahmen als die Grundvoraussetzung des Selbstverteidigungsrechts werden von dem Sicherheitsrat bestimmt.[139] Das bedeutet, dass die Anwendung der Selbstverteidigung aufgrund dessen zeitlich beschränkt ist.

Aus dem Wortlaut des Artikels ergibt sich, dass sowohl die *individuelle* und als auch *kollektive* Selbstverteidigung[140] nur für einen *„bewaffneten Angriff"* gilt. Die UN-Charta benutzt den Begriff „bewaffneter Angriff" im Art. 51 anstatt des Begriffs „Gewalt" im Art. 2 Nr. 4. Der Begriff „bewaffneter Angriff" wird in engerem Sinne gegenüber dem Begriff „Gewalt" interpretiert. Unter dem Begriff „bewaffneter Angriff" versteht man eine massive und klassische militärische Aktion. Die Staaten dürfen also nicht bei jedem Angriff für das Selbstverteidigungsrecht sprechen. Nur bei solchen militärischen Angriffen findet das Selbstverteidigungsrecht eine Anwendung.[141]

Der Art. 3 der GA. Res. *„Definition der Aggression"* 3314 (XXIX), die auf dem Gedanken vom „*Schutz der Souveränität, der territorialen Unversehrtheit und politischen Unabhängigkeit der Staaten*"[142] beruht, ist das wichtigste Instrument zur Interpretation der Definition des Begriffs „bewaffneter Angriff".[143] Die UN-Generalversammlung hat dabei versucht, den Begriff „Angriffshandlungen" zu beschreiben. Doch sind die beiden Begriffe nicht identisch. Man kann daher die bewaffneten Angriffe nicht als gleichartig mit den Angriffshandlungen ansehen.[144]

Für das Selbstverteidigungsrecht muss zunächst einmal nachgewiesen werden, welcher Staat den Angriff ausgeübt hat. Also die Frage hinsichtlich der Zurechenbarkeit kommt in erster Linie in Frage.[145] Und das Selbstverteidigungsrecht muss ohne Zweifel in Bezug auf den Angreifer

[137] *Hobe,* ebd., S. 259.
[138] *Arnauld* (Fn. 4), S. 483, Rn. 1082 ff.
[139] *Arnauld*, ebd., S. 479 f., Rn. 1074.
[140] Kollektive Selbstverteidigungsrecht wird auch in Tallinn Manual Nr. 16 zum Ausdruck gebracht.
[141] *Stein/von Buttlar/Kotzur* (Fn. 76), S. 292, Rn. 784; *Herdegen* (Fn. 76), S. 262. Rn. 22.
[142] Art. 1 der GA. Res. 3314 (XXIX); *Stein/Marauhn* (Fn. 20), S. 4 f.
[143] *Nicaragua II* (Fn. 5), Ziff. 195.
[144] *Keber/ Roguski* (Fn. 29), S. 414.
[145] IGH, Urteil vom 06.11.2003 (*Oil Platforms II*), ICJ Reports 2003, 161, Ziff. 71 f.

geübt werden.[146] Beim Art. 51 UN-Charta ist nicht klar, ob das Selbstverteidigungsrecht nur gegen die Staaten anwendbar ist. Die Praxis der Vereinten Nationen zeigt uns, dass die nichtstaatlichen Akteure die Urheber sein könnten. Das Selbstverteidigungsrecht beschränkt sich heute also nicht nur auf Staaten.[147]

Im Lichte dieser Entwicklungen lässt sich sagen, dass eine Notwendigkeit besteht, die UN-Charta zu reformieren.[148]

b. Lässt Art. 51 UN-Charta sich an dieser Stelle anwenden?

Die Frage lautet: Wie soll man das Thema behandeln, wenn die sog. klassischen Waffen bei den physischen Angriffen nicht benutzt wurden? Hierbei ist davon auszugehen, dass das Selbstverteidigungsrecht in extremen Fällen – wie bei den durch ohne klassischen Waffen geführten Cyberangriffe entstandene gleichmäßige Wirkung – in Betracht kommt.[149]

Nach dem Tallinn Manual N. 13 steht das Selbstverteidigungsrecht der Staaten zur Verfügung, wenn ein Cyberangriff eine massive Wirkung wie in Fälle des bewaffneten Angriffs hat. Diese Intensität im Hinblick auf den Begriff des bewaffneten Angriffs hängt von „*scale and effects*“ ab.[150] Dieser „*scale and effects*“ Maßstab eröffnet einen großen Ermessensspielraum während der Bestimmung der Schwelle des bewaffneten Angriffs. Aufgrund dieser von Staat zu Staat unterschiedlich bewertenden Situation wird das Selbstverteidigungsrecht missbraucht.[151] Nach der Rechtsprechung des IGH müssen die bewaffneten Angriffe in großem Umfang durchgeführt werden, damit der verletzte Staat für sich das Selbstverteidigungsrecht beanspruchen kann. Die Angriffe, die unter der Schwelle bleibend betrachtet werden, genügen also nicht.[152]

In der Literatur gibt es die Auffassung, die Angriffe, die unter der Schwelle des bewaffneten Angriffs i.S.d. Art. 51 UN-Charta bleiben, als Thema des *„kleinen Selbstverteidigungsrechts“* zu betrachten.[153] Nach dieser Meinung kann man das Selbstverteidigungsrecht gegen die Cyberangriffe, die unter der Schwelle des bewaffneten Angriffs bleiben, anwenden.

---

[146] *Keber/Roguski* (Fn. 29), S. 416; *Stein/Marauhn* (Fn. 20), S. 35.
[147] Siehe dazu S/Res/1368 (2001) und S/Res/1373 (2001); *Hobe* (Fn. 77), S. 258; *Heintschel von Heinegg*, § 52 Ausnahmen vom Gewaltverbot, in: Ipsen (Hrsg.), Völkerrecht, 2014, S. 1088, Rn. 24; vgl. auch „Mauer“ – Gutachten (Fn. 117), Ziff. 139.
[148] *Oellers-Frahm*, Der IGH und die Lücke zwischen Gewaltverbot und Selbstverteidigungsrecht – Neues im Fall „Kongo gegen Uganda?“, ZEuS 1 (2007), S. 78.
[149] Randelzhofer (Fn. 98), S. 74, Rn. 20.
[150] *Nicaragua II* (Fn. 5), Ziff. 195.
[151] *Bothe* (Fn. 61), S. 6.
[152] *Oil Platforms II* (Fn. 145), Ziff. 51; *Nicaragua II* (Fn. 5), Ziff. 191, 195. Siehe auch *Arnauld* (Fn. 4), S. 481, Rn. 1079.
[153] *Arnauld*, ebd. S. 481, Rn. 1079.

Das Gefahrenpotenzial der Cyberangriffe wird immer höher geschätzt. Ein gutes Beispiel dafür ist der Stuxnet-Fall vom Jahr 2010. In der Expertengruppe des Tallinn Manual war umstritten, ob die Cyberangriffe als ein bewaffneter Angriff bewertet werden können.[154] Und die Expertengruppe hatte keine Einstimmigkeit, ob der Stuxnet-Fall die Qualität des bewaffneten Angriffs habe.[155] Nach der überwiegenden Meinung in der Lehre sollte man die Vernichtung von Nuklearanlagen aufgrund dieses Potenzials als einen „bewaffneten Angriff" bezeichnen.[156]

Im Jahr 2012 hat der ehemalige Verteidigungsminister der Vereinigten Staaten Leon Panetta in einem Gespräch gesagt, dass die USA unter „*Cyber-Pearl Harbor*" stünden. Solche computergestützten Angriffe hätten die USA deswegen das Recht, sich entgegenzustellen, um die USA zu verteidigen.[157] Obwohl im Völkerrecht keine Einigkeit über die Cyberangriffe besteht, genügt allein nach der Ansicht der USA eine „Bedrohung" für die Selbstverteidigung. Außerdem sehen die USA keinen Unterschied zwischen der „Gewaltanwendung" und „dem bewaffneten Angriff, also das Selbstverteidigungsrecht kann danach bei jeder Form von Gewaltanwendung ausgeübt werden.[158]

Es ist möglich, dass die computergestützten Angriffe, vor allem aber Angriffe gegen Infrastrukturen, große und unersetzliche Schaden zufügen können. So wird heute diskutiert, welche Maßnahmen die Staaten dazu treffen. Denn es geht um in erster Linie Menschenleben. Nach Professor *Yoram Dinstein* kann das Selbstverteidigungsrecht in Anspruch genommen werden, wenn der scheinbare bewaffneten Angriff deutlich entsteht.[159]

Das Selbstverteidigungsrecht kann nur zweifelsfrei gegen bestimmten Angreifer in Anspruch genommen. Wie oben dargelegt, ist es bei den Cyberangriffen kaum möglich.[160]

In diesem Punkt wäre hilfreich, das Vorsorgeprinzip zu diskutieren. Das Vorsorgeprinzip ist einer der wesentlichen Prinzipien des Umweltvölkerrechts. In diesen Fällen, in denen die Verwirklichung der negativen Schäden auf dem ernsten Zweifel beruht, kann dieses Prinzip einen Anwendungsbereich finden. Da kann der wissenschaftliche Beweis dieser negativen

---

[154] *Bothe* (Fn. 61), S. 6.)
[155] *Bothe*, ebd., S. 6.
[156] *Plate* (Fn. 35), S. 200.
[157] Panetta Warns of Dire Threat of Cyberattack on U.S., The New York Times, 11. 10. 2012, abrufbar unter: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?ref=world. (10.07.2018)
[158] *Heintschel von Heinegg* (Fn. 8), S. 5.
[159] *Schmitt* (Fn. 26), *S.* 193.
[160] *Plate* (Fn. 35), S. 200.

Schäden für die Gegenmaßnahmen hier nicht abgewartet werden, weil die möglichen Ergebnisse wie die Explosion der Atomkräfte sehr schwer sein können. In diesem Rahmen können die Staaten präventive Vorsorgemaßnahmen treffen. Also dieses Prinzip ergibt sich vor dem schädlichen Fall.[161]

Wegen des Bedrohungspotenzials von computergestützten Angriffen gegen kritische Infrastrukturen – wie beim Stuxnet-Fall – ist dabei logisch, das Vorsorgeprinzip für die Cyberangriffe anzuwenden.[162]

Aufgrund der Unbestimmtheit des Begriffs „bewaffneter Angriff" handelt es sich um in der Lehre die Versuche, die den Begriff im Rahmen des Art. 51 definieren wollen. Es gibt darüber drei verschiedenen Auffassungen.

aa. Folgentheorie

Die Folgentheorie geht davon aus, dass wenn die Cyberangriffe eine vergleichbare bzw. identische Wirkung wie die klassischen Waffen haben, werden sie dann als „bewaffneter Angriff" im Sinne des Art. 2 Ziff. 4 UN-Charta eingestuft.[163] Dabei nennt man die sechs Kriterien von Schmitt[164], um die Cyberangriffe als Gewalt i.S.d. UN-Charta anzunehmen:

- *Härte (severity):* An erster Stelle ist festzulegen, ob die schädigende Bedrohung für die Menschen oder Sachen eine Bedeutung hat.
- *Unmittelbarkeit (immediacy):* Es muss klargestellt werden, dass die schädliche Folge des Angriffs sich aus dem Angreifer ergibt.
- *Abhängigkeit (directness):* Es muss ein Kausalzusammenhang zwischen den Einsatz und den Schäden bestehen.
- *Eindringen in fremde Hoheitsgebiete (invasiveness):* Es ist festzusetzen, ob der Angriff geografisch im Gebiet des betroffenen Staates stattfindet.
- *Messbarkeit (measurability):* Die schädliche Wirkung des Angriffs muss einfacher als andere Formen messbar sein.
- *Präsumptive Rechtsmäßigkeit (Presumptive legitimacy):* Letztendlich ist zu untersuchen, dass ob diesen Cyberangriff die Voraussetzungen eines bewaffneten

[161] Vgl. *Arnauld* (Fn. 4), S. 394, Rn. 888 ff.*; Krieger* (Fn. 3), S. 4 ff.
[162] Vgl. *Krieger*, ebd., S. 4 ff.; *Schaller* (Fn. 44), S. 23; *Schmahl* (Fn. 38), S. 189.
[163] *Bens* (Fn. 46), S. 151.
[164] *Schmitt* (Fn. 26), S. 184 f.

Angriffs trägt. Denn die Bewertung der Cyberangriffe als ein bewaffneter Angriff ist in der Regel eine Ausnahme.

Hierbei kann man kritisieren, dass es keinen Maßstab gibt, die Wirkung und Folgen festzulegen. Die Fälle Estland v. 2007 und Stuxnet v. 2010 erscheinen diskussionswürdig in diesem Sinne. Daneben wurden im Tallinn Manual zwei Kriterien vorgesehen: *militärische Charakter (military charakter)* und *staatliche Beteiligung (state involvement)*.[165]

bb. Domänentheorie

Der Ausgangspunkt dieser Ansicht orientiert sich nicht an Schäden, sondern an dem Zielcomputer. So kommen auf diese Weise „die kritischen Infrastrukturen" in Frage.

Die kritischen Infrastrukturen spielen – wie schon erwähnt – insbesondere eine große Rolle für das Menschenleben und das Gesundheitswesen sowie für die Energieversorgung.

In dieser Theorie geht es um eine „präventive Selbstverteidigung", weil hier auf den Schutz der kritischen Strukturen gezielt wird. Verfolgt wird diese Theorie überwiegend von amerikanischen Autoren.[166]

cc. Instrumententheorie

Im Zentrum dieser Ansicht steht das beim Angriff benutzte Mittel. Nach der Instrumententheorie ist zu klären, ob der Cyberangriff als eine Waffe i.S.d. konventionellen Waffen anzusehen ist oder nicht.

Manchmal kann man die Cyberangriffe mit klassischen Waffen oder die klassischen Waffen mithilfe der Cyberangriffe Gebrauch machen. In diesen Fällen werden die Cyberangriffe deutlich als ein Mittel für den bewaffneten Angriff benutzt.

Für diese Theorie ist nicht die Folge oder der Zielcomputer wichtig. Entscheidend ist vielmehr, ob der Cyberangriff als ein Instrument zum Zwecke der Schadenszufügung verübt wird. Somit wird der Cyberangriff wie eine Waffe i.S.d. Art. 2 Ziff. 4 UN-Charta benutzt, um die Computersysteme zu stören. Diese Theorie setzt also einerseits ein Cyberangriff als Cyberwaffen und andererseits durch diesen bewussten Angriff verursachte Schäden voraus.[167]

Wie gesehen, die Theorien unterscheiden sich voneinander. Während die Folgentheorie »die Wirkung des Angriffs« wichtig ist, ist der »Adressat des Angriffs« nach der Domänentheorie

[165] Tallinn Manual S. 48 ff.
[166] Vgl. *Bens* (Fn. 46), S. 152 f.
[167] Vgl. *Bens*, ebd., S. 153.

maßgebend. Die Folgentheorie ist nach meiner Meinung akzeptabler als andere. Wie *Schmitt* zutreffend geschrieben: *„Ein Angriff, der speziell auf die unmittelbare physische Beschädigung materiellen Vermögens bzw. auf die Verletzung oder Tötung von Menschen abzielt, entspricht der Anwendung von Waffengewalt und wird von dem Gewaltverbot erfasst.“*[168]

c. Verhältnismäßigkeit

Das Selbstverteidigungsrecht darf nur im Rahmen der Verhältnismäßigkeit ausgeübt werden. Die auf das Selbstverteidigungsrecht basierenden Gegenmaßnahmen dürfen keinen Gegenschlag oder Racheakt zeigen. Sie müssen sich vielmehr an der Annullierung des Angriffs orientieren. Deswegen ist relevant, ob die Selbstverteidigung als nötig erscheint und ob sie verhältnismäßig ist.[169] Im Völkerrecht bedeutet das Selbstverteidigungsrecht nicht, den angreifenden Staat zu bestrafen.[170]

Im Rahmen der Verhältnismäßigkeit hat der angegriffene Staat einen Ermessensspielraum über die Methode und die Intensivität gegen den Angriff.[171] Zum Beispiel bei den Cyberangriffen können die Staaten dagegen computergeschützten Gegenmaßnahmen treffen (sog. Hackback).[172] Es gibt aber auch die Staaten, die keine Technologie oder kein Geld dafür haben. Bei solchen Fällen haben die Staaten keine andere Möglichkeit, konventionelle Waffen im Rahmen der Selbstverteidigung zu benutzen.[173] Wenn die Cyberangriffe beachtliche physischen Schäden verursachen oder ihre schädlichen Zwecke eindeutig sind, dann kann man einfacher beurteilen, ob diese Selbstverteidigung verhältnismäßig ist oder nicht.[174]

Nach Art. 51 ASR fordert die Staatenverantwortlichkeit auch die Verhältnismäßigkeit. Die Maßnahmen gegen die Cyberangriffe müssen unter dem Maßstab des Gewaltverbots beobachten und menschenrechtsfreundlich sein.[175]

Der computergestützte Angriff kann manchmal über einen Server, der in einem dritten neutralen Staat steht, durchgeführt werden. Prinzipiell handelt es sich um kein Verteidigungsrecht gegen den neutralen Staat. Falls der neutrale Staat nicht in der Lage ist, den

[168] *Schmitt* (Fn. 26), S. 183.
[169] *Nuclear Weapons* (Fn. 113), Ziff. 30.
[170] *Hobe* (Fn.77), S. 260.
[171] *Hobe*, ebd., S. 259.
[172] *Plate* (Fn. 38), S. 200.
[173] *Keber/ Roguski* (Fn. 29), S. 416; *Stein/Marauhn* (Fn. 20), S. 9; *Schaller* (Fn. 44), S. 20.
[174] Vgl. *Stein/Marauhn*, ebd., S. 12 f.
[175] *Schaller* (Fn. 44), S. 25.

Angriff außer Kraft zu setzen, dann kann man in diesem Fall das Verteidigungsrecht des geschädigten Staates diskutieren.[176]

2. Die kollektive Sicherheit gegen Cyberangriffe

Nach dem Art. 24 Abs. 1 und dem Art. 12 UN-Charta übernimmt der Sicherheitsrat die Hauptverantwortung zur Wahrung des Weltfriedens und der internationalen Sicherheit. Im Art. 25 UN-Charta wird zum Ausdruck gebracht: *„Die Mitglieder der Vereinten Nationen kommen überein, die Beschlüsse des Sicherheitsrats im Einklang mit dieser Charta anzunehmen und durchzuführen."*

Wenn der betroffene Staat gemäß Art. 51 UN-Charta Maßnahmen im Sinne des Selbstverteidigungsrechts trifft, dann ist er gemäß Art. 51 S. 2 UN-Charta verpflichtet, sie den Sicherheitsrat mitzuteilen. Diese Verpflichtung der Staaten kann für das Handeln des Sicherheitsrats maßgeblich sein, und mit dieser Mitteilung kann die kollektive Sicherheit in Gang gesetzt werden.[177]

Der Sicherheitsrat kann auch selbst, also ohne Mitteilung eines Mitgliedsstaates, von einer Notwendigkeit der kollektiven Sicherheit ausgehen. Dafür setzt der Art. 39 UN-Charta „*eine Bedrohung oder einen Bruch des Friedens oder eine Angriffshandlung*"[178] voraus. Hierbei ist GA. Res. 3314 (XXIX) v. 1974 mit dem Titel „Definition der Aggression" von Bedeutung.[179] Der Art. 1 dieser Resolution dieser Resolution definiert den Begriff „Aggression". Diese Definition sieht jede durch einen Staat angewendete Waffengewalt, die gegen die Souveränität, die territoriale Unversehrtheit oder die politische Unabhängigkeit eines anderen Staates gerichtet ist, als mit der Charta der Vereinten Nationen unvereinbar. Man bemerkt an dieser Stelle, dass dieser Orientierungspunkt dem Art. 2 Ziff. 4 UN-Charta ähnelt.[180]

Die Vereinten Nationen hat keine eigene Streitkraft. Aus den Art. 43-48 UN-Charta ergeben sich daher die Rechtsgrundlage zum Einsatz der Streitkräfte im Dienste von Vereinten Nationen.

---

[176] Vgl, *Dietz*, Der Krieg der Zukunft und das Völkerrecht der Vergangenheit?, DÖV 12 (2011), S. 471 f.
[177] *Hobe* (Fn. 77), S. 260.
[178] Zur Feststellung der Sicherheitsrat nach Kapitel VII „Maßnahmen bei Bedrohung oder Bruch des Friedens und bei Angriffshandlungen" siehe S/ Res/1373 (2001); S/Res/1540 (2004); S/Res/2178 (2014).
[179] *Stein/Marauhn* (Fn. 20), S. 4; *Arnauld* (Fn. 4), S. 462, Rn. 1036; *Randelzhofer* (Fn. 98), S. 74, Rn. 19.
[180] Art. 1 GA. Res. 3314 (XXIX): *„Aggression bedeutet Anwendung von Waffengewalt durch einen Staat gegen die Souveränität, die territoriale Unversehrtheit oder politische Unabhängigkeit eines anderen Staates oder auf eine andere mit der Charta der Vereinten Nationen nicht vereinbare Art und Weise";* siehe auch *Randelzhofer*, ebd., S. 74, Rn. 19.

Wie oben erwähnt, lässt das Selbstverteidigungsrecht sich nur bei dem bewaffneten Angriff anwenden; aber die Angriffe können manchmal unter der Schwelle des bewaffneten Angriffs liegen. In solchen Fällen kann nur der Sicherheitsrat entscheiden, ob auf den Angriff reagiert werden muss.[181]

Die Entscheidung des Sicherheitsrats über die kollektive Sicherheit hängt von dem Begriff des bewaffneten Angriffs nicht ab. Während bei einem bewaffneten Angriff physische Schäden maßgebend sind, führt der Sicherheitsrat dagegen zur Berufung der kollektiven Sicherheit nur eine Bewertung, ob es um „eine Bedrohung oder ein Bruch des Friedens oder eine Angriffshandlung" geht.[182] Deswegen kann man sagen, dass der Sicherheitsrat sich für die kollektive Sicherheit über die Cyberangriffe unabhängig von der Begriffe-„Gewalt" oder „bewaffnete Angriff" entscheiden kann.[183]

Durch die kollektive Sicherheit unternehmen die internationalen Organisationen, sich für den Frieden zwischen Mitgliedern einzusetzen.[184] Wenn eine Bedrohung oder ein Bruch des Friedens oder eine Angriffshandlung vorliegt, hat der Sicherheitsrat verschiedene Möglichkeiten nach Kapitel VII der UN-Charta dazu. Nämlich »Aufforderung zur vorläufigen oder notwendigen Maßnahmen« und »Empfehlungen abzugeben« sowie »Beschlüsse zu verkünden«.[185] Während der Sicherheitsrat darüber entscheidet, muss er auf das Verhältnismäßigkeitsprinzip achten, und dabei müssen militärische Maßnahmen als *ultima ratio* getroffen werden.[186]

Der Sicherheitsrat nutzt dieses Recht der kollektiven Sicherheit nach dem Art. 30 i.V.m. 27 Abs. 3 UN-Charta. Es kann aber durch das Veto-Recht, welches den fünf ständigen Mitgliedern zur Verfügung steht, blockiert werden. Dabei sind sicherlich die politischen Interessen dieser Mitglieder entscheidend. In der Praxis ist es daher nicht immer möglich, die kollektive Sicherheit ohne dem Veto-Recht anzurufen.[187] Daher ist es in der Praxis nicht immer möglich.

GA trägt auch – wie der Sicherheitsrat – nach dem Art. 11 UN-Charta die Verantwortung, den Weltfrieden und die internationale Sicherheit zu wahren. Da hat die GA in seiner „Uniting for

---

[181] *Oellers-Frahm* (Fn. 148), S. 72.
[182] *Schmitt* (Fn. 26), S. 194.
[183] *Schmitt,* ebd., S. 195.
[184] *Arnauld* (Fn. 4), S. 467, Rn. 1045.
[185] *„…die beteiligten Parteien auffordern, den von ihm für notwendig oder erwünscht erachteten vorläufigen Maßnahmen Folge zu leisten" (Art. 40 UN-Charta)* oder *Empfehlungen (Art. 39 UN-Charta)* oder *„Maßnahmen - unter Ausschluß von Waffengewalt -"* (Art. 41 UN-Charta) oder *„mit Luft-, See- oder Landstreitkräften die erforderlichen Maßnahmen"* (Art. 42 UN-Charta).
[186] *Stein/von Buttlar/Kotzur* (Fn. 76), S. 323, Rn. 853.
[187] *Herdegen* (Fn. 76), S. 257, Rn. 10.

Peace-Resolution“[188] zugestimmt, dass die primäre Verantwortung dafür beim Sicherheitsrat liegt. Aber die GA hat auch festgestellt, dass, wenn der Sicherheitsrat wegen des Missbrauchs vom Veto-Recht seine Verantwortung über den Weltfrieden und die internationale Sicherheit nicht übernehmen kann, kommt die GA über die notwendigen Aufgaben und gegebenenfalls mit der Anwendung militärischer Gewalt in Gang.[189]

Bei der kollektiven Sicherheit geht es um zwei wichtige Fragen im Sinne von Cyberangriffe: Erstens welche Cyberangriffe können im Lichte der Formel als „eine Bedrohung oder ein Bruch des Friedens oder eine Angriffshandlung“ in Betracht kommen? Im Anschluss daran lautet die zweite Kernfrage: Dürfen die Maßnahmen nach dem Kapitel VII der UN-Charta getroffen werden?[190]

Nach dem Wortlaut der Art. 39 UN-Charta und der Art. 1 GA. Res. 3314 (XXIX) ist eine »durch Waffen geschehene Gewalt« notwendig, für einen Bruch des Friedens oder eine Angriffshandlung zu sprechen.[191] Das führt dazu, dass die Cyberangriffe erstens mit der „Waffengewalt“ gleichgestellt werden müssen, um diese Angriffe im Rahmen der Angriffshandlung betrachten zu können.

Bei der kollektiven Sicherheit handelt es sich um nicht immer „Waffengewalt“. Bei der „Gefahrensituationen“ kann der Sicherheitsrat seine Tätigkeit auch wegen der Bedrohung des Friedens ausüben. In diesen Fällen wird die Bedrohung bzw. Gefahrensituation mit einer weiten Auslegung festgestellt. In diesem Sinne könnten die Cyberangriffe wie die Angriffe gegen Infrastrukturen als eine Bedrohung des Friedens angesehen werden.[192]

Da die Cyberangriffe im Cyberspace geschehen, vermag der Sicherheitsrat nach dem Art. 41 UN-Charta, die nichtmilitärischen Maßnahmen über das Netzwerk und Telekommunikationssysteme durchzuführen. Aber wenn die Cyberangriffe physische Schäden wie z.B. Menschenverletzungen durch eine Explosion im Atomkraftwerk verursachen, kommen die militärischen Maßnahmen nach dem Art. 42 UN-Charta in Betracht.[193] Alle diese Variationen sind im heutigen Völkerrecht vorstellbar. Beispielsweise nach Tallinn Manual Nr.

---

[188] UN- GA “Resolution adopted by the General Assembly 377 (V). Uniting for Peace”, 03.11.1950, UN Doc. A/RES/5/377.
[189] Vgl. *Hobe* (Fn. 77), S. 274 f; *Schöbener*, Uniting for Peace-Resolution (1950), in: ders. (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, 2014, S. 481 ff.
[190] *Dittmar*, Angriffe auf Computernetzwerke - Ius ad bellum und ius in bello, 2005, S. 170.
[191] *Dittmar*, ebd., S. 181; *Heintschel von Heinegg,* § 53 Wahrung und Wiederherstellung des Weltfriedens und der internationalen Sicherheit durch Systeme kollektiver Sicherheit, in: Ipsen, Völkerrecht, 6. Auflage, München, 2014, S. 1105, Rn. 10; *Schmitt* (Fn. 26), S. 189.
[192] *Dittmar*, ebd., S. 182.
[193] *Dittmar*, ebd., S. 183.

18 hat der Sicherheitsrat für diese Vorstellungen Befugnis, dass also die Experten von *Tallin* glauben, dass die kollektive Sicherheit gegen die Cyberangriffe anwendbar ist.

IV. Zwischenfazit

Das Völkerrecht hat sich als ein Rechtsgebiet mit eigener Systematik und Methodik fortzuentwickeln. Ansonsten ergeben sich daraus sog. Lücken und Defizite im Hinblick auf Anwendbarkeit des Völkerrechts. Wegen des Mangels an Durchsetzungskraft und wegen des Fehlens einer zwingenden Gerichtsbarkeit sowie mangels eines Gesetzgebungsorgans zur Durchsetzung von Entscheidungen wird diskutiert, ob das Völkerrecht als eine eigene Rechtsordnung eingestuft werden sollte. Die Lehre geht nunmehr auf diesen Streit nicht ein, da das Völkerrecht seinen Platz in der Rechtswissenschaft als eigene Rechtsdisziplin durch neue Institutionen verstärkt hat.[194]

Das klassische Völkerrecht hat einen „genossenschaftlichen", „schwach organisierten" und „indirekten" sowie „politischen" Charakter. Berücksichtigt man diese Besonderheiten und dieses Verständnisses des Völkerrechts, so kann man feststellen, dass es nicht einfach wäre, neue Institutionen in Gang zu setzen.[195]

Der Art. 2 Ziff. 4 UN-Charta, also die heutige Rechtsgrundlage des Gewaltverbots, wird überwiegend im engeren Sinne interpretiert. Das gilt danach nur für die kinetischen Waffen. Es ist deshalb davon auszugehen, dass Gewohnheitsrecht mit der Zeit seinen Beitrag bezüglich der Cyberangriffe leisten wird.[196] Das ist höchstwahrscheinlich, da die Technologie in Hinblick auf die Rüstung im Cyberspace eine Gefahr für die Staaten darstellt.

Der Art. 38 Abs. 1 lit. b IGH-Statut definiert das Völkergewohnheitsrecht als „*Ausdruck einer allgemeinen, als Recht anerkannten Übung"*. Es muss also dafür eine „allgemeine Übung" (objektives Element – *consuetudo*) und eine „Rechtsüberzeugung" (subjektives Element – *opinio iuris*) dafür bestehen.[197] Es ist auch heute vorstellbar, dass das Selbstverteidigungsrecht gegen die Cyberangriffe die allgemeine Übung von den Staaten braucht. Es könnte dadurch als eine Verletzung gegen das Gewaltverbot im Völkerrecht betrachtet werden. Diese Praxis wird aber in völkergewohnheitsrechtlicher Hinsicht einen Platz gefunden werden.[198]

---

[194] *Herdegen* (Fn. 76), S. 8 f.; *Wiegandt*, Internationale Rechtsordnung oder Machtordnung? ZaöRV 71 (2011), S. 31 ff.; *Hobe* (Fn. 77), S. 9.
[195] Zur Einzelheiten, *Arnauld* (Fn. 4), S. 14 ff.
[196] Vgl. *Schmitt* (Fn. 26), S. 188.
[197] *Herdegen* (Fn. 76), S. 147, Rn. 1; *Arnauld* (Fn. 4), S. 104, Rn. 250.
[198] *Stein/Marauhn* (Fn. 20), S. 13.

Falls die Websites (wie beim Estland-Fall) blockiert werden oder die Server beeinträchtigt werden, so kommt ein Verstoß gegen das Gewaltverbot nicht in Frage. Es geht um hierbei vielmehr einen Verstoß gegen das Interventionsverbot.[199] Der Estland-Fall hat uns gezeigt, dass die Cyberangriffe einerseits Störungen wie Blockierung von Bankennetzwerken verursachen. Die Cyberangriffe können sogar durch physische Störungen gefährlicher sein. Ein gutes Beispiel dafür kann man das Sterben eines Patienten mangels Strom im Krankenhaus geben. Der Stuxnet-Fall hat daneben bewiesen, dass die Cyberangriffe andererseits die wesentlichen Infrastrukturen neutralisieren, sogar den Unfall oder die Explosion verursachen. Bisher hatte man außer Stuxnet solche Cyberangriffe, die lebensgefährliche Wirkung haben, nicht erlebt. Das bedeutet aber nicht, dass es nicht in der Zukunft eintreten kann. Es geht vielmehr ein großes Potenzial im Hinblick auf die Cyberangriffe.

Es ist kaum möglich, dass ein Staat die Verantwortung wegen eines Cyberangriffs übernimmt, da diese Annahme zur haftungsbegründenden Völkerrechtsverletzung gegen das Hoheitsrecht des angegriffenen Staates führen würde. Aufgrund des völkerrechtlichen Gewaltverbots sollte man keine endgültige Zurechnung eines Staates erwarten; denn die angreifenden Staaten sich bei Cyberangriffe sehr einfach hinter der Privaten verstecken können.

Bis heute gibt es keinen konkret wirkenden Cyberangriff wie die herkömmlichen Waffen. Beim Stuxnet-Fall geht es um nur einen Versuch, der schon die Gefahrenpotenzial bescheinigt hat. Aber wir wissen jetzt nicht, was uns in der Zukunft wartet. Die Staaten sollten sich daher darum bemühen, dass sie zur Vermeidung von potentiellen Schäden miteinander kooperieren. Sie sollten ferner für eine konkrete Lösung im Rahmen des *ius ad bellum* arbeiten, Denn nicht nur die Staaten wären Opfer von Cyberangriffen, sondern auch die computergestützten Angriffe könnten für die anderen Völkerrechtssubjekte bedrohlich sein. Zum Beispiel ein eventueller Cyberangriff gegen die New Yorker Börse[200] hätte eine negative Wirkung auf die ganze Ökonomie in der Welt.

Wie schon geschrieben, kann sich der betroffene Staat verteidigen, wenn der Cyberangriff die Schwelle des bewaffneten Angriffs, welche die physische Wirkung gegen auf die Sachen und Menschen wie die konventionellen Waffen machen kann, erreicht. In diesem Zusammenhang ist davon auszugehen, dass ein Flugzeug, das durch ferngesteuerte Geräte zum Abstürzen gebracht wird, als ein bewaffneter Angriff betrachtet werden kann. Somit geht es um einen Angriff gegen die Sachen und Menschenleben wie bei den klassischen Angriffen im Sinne des

[199] *Arnauld* (Fn. 4), S. 154, Rn. 360 und S. 460, Rn. 1033.
[200] *Heintschel von Heinegg* (Fn. 28), S. 25.

Völkerrechts. Ein Flugzeug des Feindes mit derselben Methode abzustürzen wäre hingegen als einen Gegenschlag zu betrachten.

Der wichtigste Zweck im Völkerrecht ist es, auf der Welt den (ewigen) Frieden widerzustellen. Die physischen Schäden, egal ob konventionelle oder BC-Waffen oder Cyberangriffe verursachten, stellen immer eine Bedrohung dar. Aus diesem Grund, falls die schädliche Wirkung wegen Cyberangriffe gleich wie mit den konventionellen Angriffen wäre, wäre dabei naturgemäß die Anwendbarkeit des Selbstverteidigungsrechts anzunehmen. Sonst könnte die Selbstverteidigung seinen Grundgedanken in der internationalen Gemeinschaft verlieren.

Zusammenfassend lässt sich sagen, dass die Cyberangriffe als „bewaffnete Angriff" bezeichnet werden können, falls sie den Infrastrukturen einem vergleichbaren massiven Schaden, wie die Fälle von mit konventionellen Waffen durchgeführten militärischen Aktionen, zufügen. Dabei ist irrelevant, ob die Infrastrukturen militärisch oder nichtmilitärisch sind.[201]

D. Cyberangriffe und *ius in bello*

I. Bedeutung und Anwendungsbereich des *ius in bello*

„In the 21st Century, bits and bytes can be as threatening as bullets and bombs. "[202]

Ius in bello oder mit anderen Worten Kriegsrecht, Recht der bewaffneten Konflikte, humanitäres Völkerrecht, beschäftigt sich mit dem bei den bewaffneten Konflikten anzuwendenden Recht und sucht die Antworten, wie die Kriegsführung begrenzt werden muss.[203] Seine geschichtliche Entwicklung geht auf die Hälfte des 19. Jahrhunderts zurück, wobei die Grundlagen für das humanitäre Völkerrecht durch die Verabschiedung der IV. Haager Abkommen v. 1907 und Genfer Abkommen (1949 I-IV) sowie zwei Zusatzprotokollen (1977 I-II) geschaffen wurden. Diese Abkommen haben gewohnheitsrechtlichen Charakter.[204]

Während die Rechtsmäßigkeit der militärischeren Gewalt für *ius ad bellum* wichtig ist, ist beim humanitären Völkerrecht die Rechtsmäßigkeit der Gewalt nicht maßgebend. Das HVR prüft nicht, ob der bewaffnete Konflikt im rechtlichen Rahmen des *ius ad bellum* bleibt.

---

[201] *Arnauld* (Fn. 4), S. 481, Rn. 1078; *Herdegen* (Fn. 76), S. 264, Rn. 23.
[202] Remarks on the Department of Defense Cyber Strategy, As Delivered by Deputy Secretary of Defense William J. Lynn, III, National Defense University, Washington, D.C. 14.07.2011, abrufbar unter: http://archive.defense.gov/speeches/speech.aspx?speechid=1593 (20.05.2018). Das wäre auf Deutsch so lautet: »*Im 21. Jahrhundert können Bits und Bytes genauso bedrohlich sein wie Kugeln und Bomben*«.
[203] *Arnauld* (Fn. 4), S. 516, Rn. 1151.
[204] *Arnauld*, ebd., S. 521, Rn. 1158.

Die wesentlichen Grundsätze des HVR, das darauf abzielt, Menschen in bewaffneten Konflikten zu schützen, sind „*Menschlichkeit, militärische Notwendigkeit und Verhältnismäßigkeit.*“[205] Man versteht „verwundete oder kranke Kämpfende, Personen, die infolge des Konflikts ihrer Freiheit beraubt wurden, und die Zivilbevölkerung sowie das Sanitäts- und Seelsorgepersonal“ gehören zu dem Schutzbereich des HVR.[206]

Die Angriffe dürfen nur nach militärischen Zielen durchgeführt werden, und es ferner muss immer zwischen Zivilbevölkerung und Kombattanten unterschieden werden, um die Zivilbevölkerung und zivilen Objekte zu schützen. Über die Methoden und Mittel der bewaffneten Konflikte kann man nicht eine freie Entscheidung treffen. Während der militärischen Gewalt dürfen z. B. insbesondere keine „verbotene Mittel“ wie chemische Waffen benutzt werden. Dafür hat das HVR die Aufgabe, solche Methoden zu beobachten.[207]

Genfer Abkommen und ZP I erklären das HVR bei internationalen bewaffneten Konflikten und ebenfalls der gemeinsame Art. 3 Genfer Abkommen I-IV und ZP II erklären das HVR bei nicht-internationalen bewaffneten Konflikte für anwendbar. *„Unter dem in bewaffneten Konflikten anwendbaren humanitären Völkerrecht, internationales Vertrags- oder Gewohnheitsrecht, das darauf ausgerichtet ist, humanitäre Probleme, die direkte Folge internationaler wie nicht internationaler bewaffneter Konflikte sind, zu lösen“*.[208]

Früher gab es keine Gerichtsbarkeit für die Kriegsverbrechen außer Ad-hoc-Strafgerichte. Dieses Fehlen ist erst am 01. Juli 2002 mit dem Haagener Internationalen Strafgerichtshof beseitigt. Für die Gerichtsbarkeit gelten nur „Völkermord“, „Verbrechen gegen die Menschlichkeit und „Kriegsverbrechen sowie „Verbrechen der Aggression“. Aber was noch wichtiger ist, ist die Erweiterung der Effektivität des HVR. Falls es um „schwere Verstöße“ gegen das HVR geht, dann kommen die Kriegsverbrechen i.R.d. HVR in Betracht.[209] Dafür sieht Art. 8 IStGH-Statut entsprechend einen Katalog über die Kriegsverbrechen vor.

II. ″Der bewaffnete Konflikt″ im Sinne des humanitären Völkerrechts und Cyberangriffe

Nach den zwei Begriffen „Gewalt“ und „bewaffneter Angriff“ kommt „bewaffneter Konflikt“ hierbei als der dritte Begriff. *Ipsen* definiert den bewaffneten Konflikt„ *„wenn eine*

[205] *Arnauld*, ebd., S. 516 f. Rn. 1152.
[206] *IKRK*, Das humanitäre Völkerrecht- Antworten auf Ihre Fragen, 2006, S. 16. Abrufbar unter: https://www.drk-mittelhessen.de/fileadmin/Bilder_und_Videos/PDFs/Das_DRK/Materialien/Allgemein/Das_Humanitaere_Voelkerrecht__Antworten_auf_Ihre_Fragen.pdf. (25.07.2018).
[207] *IKRK*, ebd., S. 6.
[208] *IKRK*, ebd., S. 4.
[209] *Arnauld* (Fn. 4), S. 587, Rn. 1336.

Konfliktpartei Waffengewalt gegen den völkerrechtlich geschützten Bereich des Konfliktgegners einsetzt und dieser Waffeneinsatz ihr als Völkerrechtssubjekt zurechenbar ist".[210] Jede Partei des Konflikts darf also selbst die Methodik in Bezug auf die Gewalt auswählen, solange sie die Regelungen des humanitären Völkerrechts beachtet.[211]

Gemäß Art. 36 ZP I muss jede Vertragspartei die neuen Waffen untersuchen lassen, ob sie mit dem betreffenden ZP oder mit der anderen Völkerrechtsregelung, die für die Vertragspartei gültig, vereinbar sind.

Die Regelungen im HVR werden entweder durch die Kodifizierung oder durch die Praxis von Staaten bestimmt.[212] Der IGH liefert dafür ein gutes Beispiel. Das Gutachten über die nuklearen Waffen sagt, dass das HVR auch für diese Waffen anwendbar ist, obwohl das HVR keine Regelungen darüber umfasst.[213] In diesem Zusammenhang ist zu diskutieren, ob ein Cyberangriff als eine neue Waffe akzeptiert werden könnte und ob diese Annahme/Anpassung für möglich gehalten würde oder – wie das neue Zusatzprotokoll vorsieht – ob es eine Notwendigkeit besteht, neue Regelung für die Cyberangriffe i.S.d. HVR zu bestimmen.[214]

Wie schon ausgeführt wurde, sind Cyberwaffen keine Waffen im Sinne der klassischen Bedeutung, sie haben aber trotzdem schädliche Wirkung.[215]

Die Definition des Art. 49 Abs. 1 ZP I hinsichtlich des Begriffs „Angriffe" umfasst sowohl »die offensive« als auch »die defensive Gewaltanwendung« gegen den Gegner. Dieser Begriff hat einen eigenen Charakter.[216] Der Begriff „Gewaltanwendung" wird hier als ein »bewaffneter Konflikt« eingestuft und dementsprechend stellt der »bewaffnete Konflikt« die „Waffengewalt" dar.

Das humanitäre Völkerrecht schützt die Zivilbevölkerung und die zivilen Objekte gegen die Gewaltanwendung. Wenn die Schäden i.S.d. HVR durch die Cyberangriffe entstanden sind, dann sollte man es im HVR betrachten.[217] Wenn die Folgen eines Cyberangriffs innerhalb der Grenzen des HVR bleiben, dann steht die Ablehnung wegen des Qualifizierungsmangels des

---

[210] *Ipsen*, § 59 Anwendungsbereiche und Grundstruktur des Rechts des bewaffneten Konflikts, in: ders. (Hrsg.), Völkerrecht, 6. Auflage, München, 2014. S. 1200, Rn. 7.
[211] *Heintschel von Heinegg* (Fn. 26), S. 132.
[212] *IKRK* (Fn. 206), S. 20.
[213] *Dittmar* (Fn. 190), S. 202 f.; *Nuclear Weapons* (Fn. 113), Ziff. 85.
[214] *Stadlmeier/ Unger* (Fn. 22), S. 70 f.
[215] *Stadlmeier/ Unger*, ebd., Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht, in: Schmalenbach (Hrsg.), Aktuelle Herausforderungen des Völkerrechts: Beiträge zum 36. Österreichischen Völkerrechtstag 2011, S. 71.
[216] *Heintschel von Heinegg* (Fn. 13), S. 162.
[217] *Heintschel von Heinegg*, ebd., S. 163 f.

Angriffs in Bezug auf die Verantwortlichkeit mit der Philosophie des HVR nicht im Einklang. Daher wird beim Art. 51 Abs. 2 S. 2 des ZP I zum Ausdruck gebracht, dass *„die Anwendung oder Androhung von Gewalt mit dem mit dem hauptsächlichen Ziel, Schrecken unter der Zivilbevölkerung zu verbreiten, ist verboten“*. So gesehen tritt hier keine Form der Gewaltanwendung in Erscheinung. Dabei ist vielmehr »der humanitäre Zweck« entscheidend.

Die Angriffe im HVR können nur mit militärischen Zielen geführt werden, dürfen nicht nach Zivilisten richten. Nach Art. 52 ZP I gehören die Objekte, *„…die auf Grund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den in dem betreffenden Zeitpunkt gegebenen Umständen einen eindeutigen militärischen Vorteil darstellt”* zu den militärischen Zielen. Unter den militärischen Zielen im Sinne von computergestützten Angriff könnten entsprechend *„alle computergestützten Systeme, die wirksam zu militärischen Handlungen beitragen und deren Zerstörung einen eindeutigen militärischen Vorteil darstellt, wie z. B. Führungs-, Kontroll- und Aufklärungssysteme, Flugabwehrsysteme oder Logistiksysteme“* verstanden werden.[218]

III. Einschränkungen von Computernetzwerkoperationen durch *ius in bello*

Die Frage, ob die Cyberangriffe als ein bewaffneter Konflikt i.R.d. HVR anzusehen ist, ist an dieser Stelle zu beantworten. Wenn ja, kommt an zweiter Stelle das anwendbare humanitäre Völkerrecht in Frage.

Natürlich kann man nicht pauschal sagen, dass jeder Cyberangriff zu einem bewaffneten Konflikt führt.[219] Im Lichte dieser vorstehenden Feststellungen kann man sagen, dass die Cyberangriffe mangels des klassischen physischen Gewaltcharakters nicht als eine Waffe i.S.d. HVR verstanden werden. Bringen die Cyberangriffe schädliche Folgen mit sich, so ist im heutigen HVR anzunehmen, dass solche Angriffe im Lichte des *ius in bello* bewertet werden sollten.[220]

Der Stuxnet-Fall hat uns gezeigt, dass das humanitäre Völkerrecht bei den computergestützten Angriffen eine wichtige Rolle spielen kann. Zum Beispiel ein Cyberangriff, der Explosion eines Kernkraftwerks verursacht hat, verstößt gegen das HVR, weil er der Zivilbevölkerung und den

[218] *Dittmar* (Fn. 190), S. 293.
[219] *Dittmar*, ebd., S. 201.
[220] *Bothe* (Fn. 61), S. 8; *Ziolkowski* (Fn. 48), S. 209.

Sachen erhebliche Schäden zugefügt hat. Es kann die Schäden der Zivilbevölkerung und der zivilen Objekte gegen HVR bewirken.

Hingegen sind unklassifizierte bzw. »unterschiedslose Angriffe« nach dem Art. 51 Abs. 4 des ZP I verboten. Der auf das Kernkraftwerk gerichtete Angriff kann deshalb i.R.d. Art. 51 Abs. 4 des ZP I betrachtet werden, obwohl das Ziel des Angriffs nicht direkt militärisch ist. Der Fall „Stuxnet" kann ferner im Rahmen des Art. 56 Abs. 1 Satz 1 des ZP I, wobei der *„Schutz von Anlagen und Einrichtungen, die gefährliche Kräfte Enthalten"* geregelt ist, betrachtet werden.

Die unterschiedslosen Angriffe, *„bei denen Kampfmethoden oder -mittel angewendet werden, die nicht gegen ein bestimmtes militärisches Ziel gerichtet werden können"*, sind nach Art. 51 Abs. 4 lit. b ZP I verboten. Die Cyberangriffe haben meistens Auswirkung auf viele Netzwerke, Server und auf Computer-Nutzer. Es lässt sich daher nicht sagen, dass die durch computergestützten Angriffe entstandenen Effekte nur im militärischen Bereich bleiben[221]; vielmehr haben sie den „dual use"-Charakter. Die Auswirkungen können also sowohl von den Zivilisten als auch von dem Militär erfahren werden.

Weiterhin werden in den Art. 38 und 39 des ZP I das Verbot der Benutzung von anerkannten Kennzeichen wie das Schutzzeichen des roten Halbmonds oder des roten Kreuzes und der Nationalitätszeichen von neutralen Staaten vorgesehen. Hier wird der Zweck verfolgt, den Missbrauch der geschützten Kennzeichen zu verhindern. Man darf also unter den Cyberangriffen diese gesicherten Kennzeichen – wie z.B. einen Virus per E-Mail mit dem Rote-Kreuz-Zeichen zu schicken – nach diesen Artikeln nicht benutzen.[222]

In ähnlicher Weise ist „das Verbot der Heimtücke" im Art. 37 ZP I geregelt. Diese Regelung kann wie z.B. in solchen Fällen, in denen sich falsche Informationen im Internet ausbreiten lassen, damit das Vertrauen der Gegner missbraucht wird, Anwendung finden. Denn die Intensität des Zwecks erreicht die schädlichen Handlungen i.S.v. HVR.[223] Dieses Verbot unterscheidet sich von den erlaubten Kriegslisten (Art. 37 Abs. 2 ZP I). Durch die Kriegslisten setzt man sich zum Ziel, das Vertrauen der Gegner in die Irre – nicht aber heimtückisch – zu führen. Letztendlich darf man die im Cyberspace vorhandene Mittel in der zivilen Gesellschaft nicht zum Zwecke der Verbreiterung von Schrecken benutzen.[224]

[221] *Stadlmeier/ Unger* (Fn. 22), S. 72.
[222] *Ziolkowski* (Fn. 48), S. 209.
[223] *Ziolkowski*, ebd., S. 209 f.
[224] Art. 51 Abs. 2 S. 2 ZP I „Die Anwendung oder Androhung von Gewalt mit dem hauptsächlichen Ziel, Schrecken unter der Zivilbevölkerung zu verbreiten, ist verboten", siehe auch *Ziolkowski* (Fn. 48), S. 210.

Spricht man über die internationalen bewaffneten Konflikte, so muss die Verantwortlichkeit der Streitkräfte als ein Thema des HVR in Frage kommen. Es ist auffällig, dass in den Cyberangriffen andere Akteuren wie „Hacker" anstatt Soldaten die entscheidende Rolle spielen.[225] Und die Verfolgung oder Feststellung dieser Akteure ist schwierig. Aufgrund dessen ist Gegenmaßnahmen zu ergreifen kaum möglich. Aber die Staaten müssen nicht darauf verzichten. Wie im Art. 58 ZP I geschrieben, haben die Staaten bei solchen Fällen das Recht, „die notwendigen Maßnahmen" zu treffen.[226]

Wie oben i.R.d. *ius ad bellum* erwähnt, hier ist auch zu diskutieren, ob eine neue Regelung i.S.d. *ius in bello* als notwendig erscheint. Arnauld hat in diesem Punkt zutreffend die aktuelle Situation wie folgt zum Ausdruck gebracht*: „Die zunehmende Verlagerung von Konflikten in Computernetzwerke fordert eine Neuvermessung des HVR. Zwar lassen sich die meisten Fragen durch Anwendung der etablierten Grundsätze zufriedenstellend beantworten, insbesondere aber die verschwimmenden Grenzen zwischen kombattanten und Zivilpersonen sowie zwischen militärischer und ziviler Infrastruktur erfordern eine Anpassung an die Besonderheiten von Cyberoperationen."*[227]

IV. Zwischenfazit

Richten die Cyberangriffe sich nur gegen die militärischen Ziele, wobei die Ziele aus militärischen Netze und Infrastrukturen sowie aus computergestützten Systemen bestehen, ist das HVR bei solchen Fällen für anwendbar zu erklären. Es ist aber nicht immer möglich, weil die computergestützten Angriffe überwiegend im Cyberspace stattfinden.

Bei einem bewaffneten Konflikt ist es in der Regel möglich, auf die kritischen Infrastrukturen abzuzielen. Zwar können die militärischen Ziele dabei nicht verfolgt werden, sie haben aber einen schädlichen Einfluss auf das Leben der Menschen. Beispielsweise könnten die Schäden in der Energieversorgung eine wesentliche Rolle für die Bevölkerung spielen. Ihre Folgen sollten daher unter Kriegsverbrechen fallen.

Das Recht auf Leben, das ein fundamentales Recht ist, kann bei einem Versuch, ein Flugzeug mithilfe ferngesteuerter computergestützter Geräten zum Absturz zu bringen oder bei der Explosion eines Kernkraftwerks oder beim Stromausfall eines Krankenhauses gefährdet

[225] *Bothe* (Fn. 61), S. 8.
[226] *Bothe*, ebd., S. 8.
[227] *Arnauld* (Fn. 4), S. 529, Rn. 1181.

werden. Auf diese Weise erscheinen die Cyberangriffe als ein wichtiges Thema des HVR, indem sie die oben ausgeführten Grundprinzipien und Werte des HVR verletzen.

E. Ergebnisse der Studie

1- Wie Herr *Randelzhofer* richtig formuliert: „*Krieg ist eine Erscheinungsform menschlichen Verhaltens und Recht ist ein wichtiges Mittel, menschliches Verhalten zu regeln.*“[228] Die heutigen Rechtsregeln waren seit langer Zeit nur eine Phantasie. Die heutigen Rechtsregeln haben sich nach den Bedürfnissen der Menschen und Gesellschaft entwickelt und ihre gegenwärtige Form erhalten. Die neuen Entwicklungen in der Technologie, nämlich die „Cyberwelt“ und „Cyberangriffe“, stellen sich wie bei allen Bereichen des menschlichen Lebens als neue Bedürfnisse in der Rechtswissenschaft heraus.

Im Cyberspace muss man die betreffenden Rechtsregeln, die heutzutage noch als Phantasie angesehen werden könnten, haben. Ansonsten werden die heutigen Bedürfnisse des Völkerrechts nicht befriedigt. Das führt danach zur Defizite und Rechtslücken, also zur ungelösten Problemen. Beispielsweise wenn die Cyberangriffe aufgrund der Rechtslücken als zulässig betrachtet werden, dann lassen sich die Staaten für unerwünschte Folgen bereitstellen.

2- Egal ob durch eine neue Konvention oder durch die Anwendung der vorhandenen Völkerrechtsnormen, das Problem der Cyberangriffe im Rahmen des Völkerrechts zu lösen, braucht man dabei nicht nur die Juristen, sondern auch den Beitrag von Experten im Bereich des Cyberspaces. Denn indem die Experten hinsichtlich des Gefahrenpotenzials von computergestützten Angriffen beraten, können mögliche Schutzregeln zu diesem Potenzial von internationaler Gemeinschaft einfacher im Dienste von internationaler Sicherheit und Weltfrieden verfasst werden.

Das Problem der Cyberangriffe im Völkerrecht setzt eine interdisziplinäre Behandlung voraus. Obwohl das Völkerrecht einer der schwierigsten Bereiche zur Festlegung der neuen Regeln ist, ist liefert Tallinn-Handbuch, das durch die Expertengruppe vorbereitet wurde, ein gutes Bespiel. Es ist zwar unverbindlich, es kann aber gute Referenz sein.

3- Die Cyberangriffe sind eigentlich optimal für Staaten, die heimtückisch noch einen Schritt weiter gehen wollen, da solche Angriffe deutlich ökonomischer, schneller und resultativer als die konventionellen Angriffe sind. Dazu kann man die Spuren von Cyberangriffe verstecken. Aus diesem Grund versuchen solche Staaten, ihre Fähigkeiten im Cyberspace von Tag zu Tag

[228] *Randelzhofer* (Fn. 98), Art. 2 Ziff. 4, S. 69, Rn. 1.

zu verbessern. Nach bösen Erfahrungen im Cyberspace kann man nicht einfach sagen, dass ein Cyberkrieg in der Zukunft nicht möglich wäre. Im Lichte von aktuellen Entwicklungen ist außerdem zu vertreten, dass die Staaten nun geradezu „den kalten Cyberkrieg" erleben.[229]

4- Die Frage über die Zurechenbarkeit ist eigentlich ein technisches Problem, denn die Technologie erlaubt, dass die Staaten ihre Identität verstecken können. Solange dies nicht gelöst ist, sind die vorhandenen Regeln des Völkerrechts nicht anwendbar.[230] Selbstverteidigung kann auch nicht Gebrauch gemacht werden, solange Zweifel daran bestehen.

Abwehrmaßnahmen gegen die Cyberangriffe, die auf kritische Infrastrukturen abzielen, zu ergreifen ist wichtig und vorrangig. Verstärkung von Sicherheitssystemen ist allerdings jetzt die einzige Lösung der Staaten im Rahmen des heutigen Völkerrechts.

Wegen des Bedrohungspotenzials müssen die Staaten, die insbesondere im Bereich der Informatik Hochtechnologie haben, taugliche Methoden finden, um die internationale Sicherheit zu gewährleisten. Es ist nicht zu vergessen, dass sich der klassische Krieg von der greifbaren Realität in die virtuelle Realität wandelt, und die virtuelle Gewalt sucht ihren Platz für sich in der Zukunft der Staatengemeinschaft.

5- Wie schon festgestellt, es geht um ein Defizit im Völkerrecht in Bezug auf Cyberangriffe. In der Literatur vertreten manche Autoren die Auffassung, dass die geltenden Völkerrechtsregelungen für die Cyberangriffe ausreichend seien.[231] Hingegen weisen andere Autoren auf die Notwendigkeit der neuen Regelungen hin und plädieren für einen Vertrags über Cyberangriffe.[232]

Wenn die Staaten die erste Ansicht vertreten wollten, sollten sie das anwendbare Völkerrecht klären. In diesem Fall ist eine Revision zum Schutz gegen Cyberangriffe denkbar, soweit die Vorschriften dafür nicht genügen. Nach dieser Auffassung werden das Selbstverteidigungsrecht oder die anderen Institutionen des Völkerrechts für anwendbar erklärt, da die Cyberangriffe wie die anderen bekannten Waffen physische Schäden zufügen könnten. Es ist auch zu diskutieren,

---

[229] Cyberangriffe auf Infrastruktur: Mit einem Hack ist alles weg, 07.12.2017, Spiegel Online, abrufbar unter: http://www.spiegel.de/forum/netzwelt/cyberangriffe-auf-infrastruktur-mit-einem-hack-ist-alles-weg-thread-686918-1.html (10.07.2018); Kalter Krieg im Netz, 30.11.2016, Süddeutsche Zeitung, abrufbar unter: https://www.sueddeutsche.de/wirtschaft/sicherheit-kalter-krieg-im-netz-1.3273614 (10.07.2018).

[230] *Johnigk/Nothdurft*, Attributierung von Cyberangriffen- Das Problem und seine Folgen, W&F, Dossier 79, 3/2015, S. 11.

[231] *Heintschel von Heinegg* (Fn. 13), S. 173; *Schaller* (Fn. 44), S. 7.

[232] Vgl. *Plate* (Fn. 35), S. 202.

ob die zweite Meinung verfolgt werden sollte. Aber im Völkerrecht neue Regelungen zu schaffen, wäre ein schwieriger und langer Weg.

6- Die Cyberangriffe können nicht vom Völkerrecht außer Acht gelassen werden. Denn sie sind die internationalen Beziehungen bestimmender Faktor geworden. Der Vorwurf, dass Russland während der USA-Präsidentenwahl 2016 durch Cyberangriffe und computergestützte Programme die Wahl manipuliert habe, wäre ein aktuelles und gutes Beispiel.

Die staatliche Kontrolle und der eingeschränkte Zugang im Internet sind keine gute Lösung. Es wäre nur eine alte Idee und bedeutete den Verzicht auf Staatenverantwortungen. Wie leben heute in einer globalen Welt, und die Meinungs- und Informationsfreiheit ist als ein Grundrecht anerkannt. Die Staaten müssen dieses Grundrecht für ihre Bevölkerung garantieren.

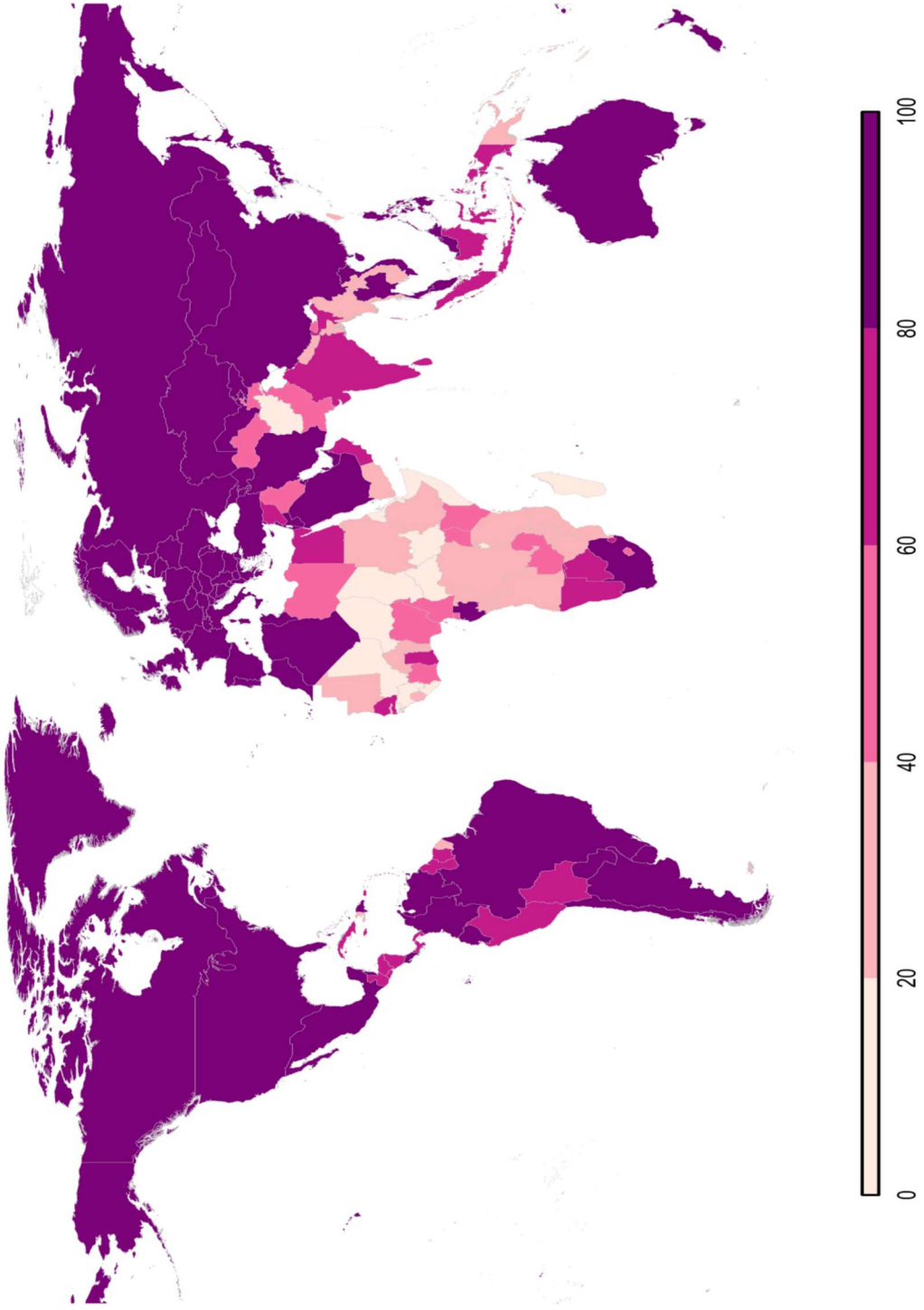
7- Schließlich darf nicht vergessen werden, dass ein massiver Angriff auf einem Staat auch andere Staaten betrifft. Die Welt ist wie ein globales Dorf. Es existieren schon die Grenzen zwischen den Staaten; aber eigentlich leben wir ohne Grenzen und universell zusammen. Beispielsweise kann das ökonomische System eines Staates zu zerfallen mit sich negative Konsequenzen für andere Staaten bringen oder die Umweltverschmutzung hat die Wirkung auf alle Menschen. Deshalb ist eine globale Zusammenarbeit der internationalen Gemeinschaft notwendig.

Es ist zu beobachten, dass der Lauf in die Richtung des *ius contra bellum*, also das Recht auf Verhinderung eines Kriegs, geht.[233] Niemand will einen neuen Krieg, egal ob konventionell oder virtuell, erklären. Jede Art des Kriegs zerstört das Leben und es wirft die Menschlichkeit um viele Jahre zurück.

[233] Vgl. *Hobe/Fuhrmann*, Vom ius in bello zum ius contra bellum: Der Beitrag der Zweiten Haager Friedenskonferenz zur Entwicklung des modernen Völkerrechts, Die Friedens – Warte 82 (2007), S. 97 ff.

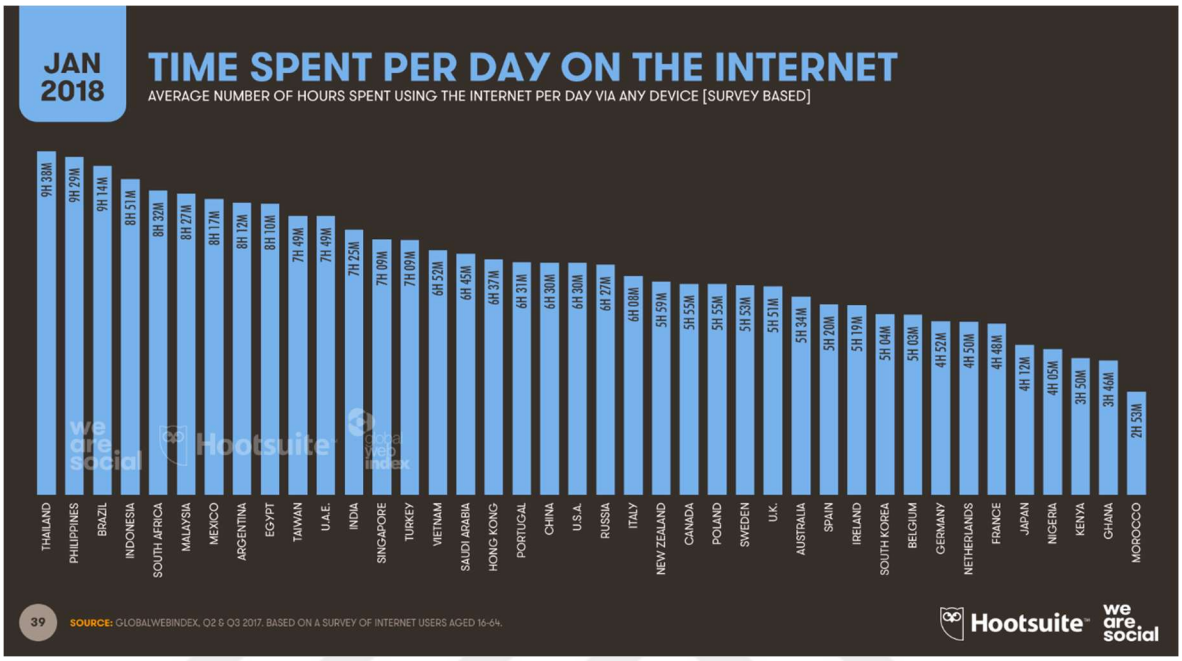
Anhänge:

1: „Proportion of youth (15-24) using the Internet, 2017*", abrufbar unter: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (02.05.2018).



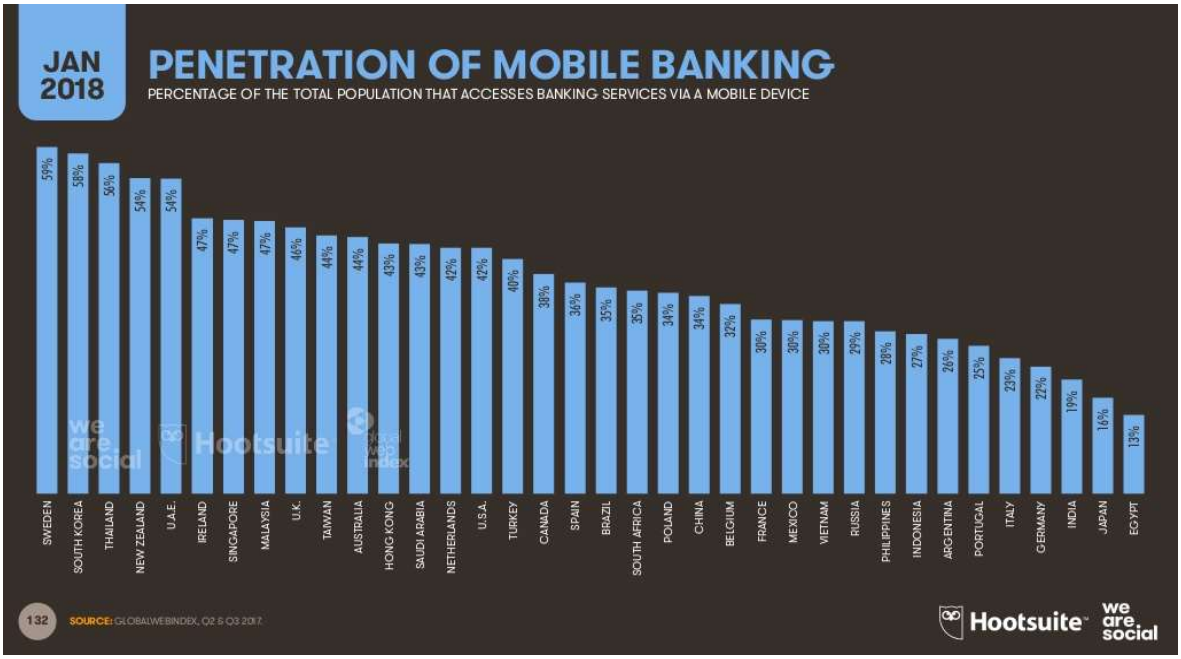
Die Ressource: ITU

2: „ Time spent per day on the Internet, 2018", abrufbar unter: https://wearesocial.com/de/blog/2018/01/global-digital-report-2018 (20.04.2018).



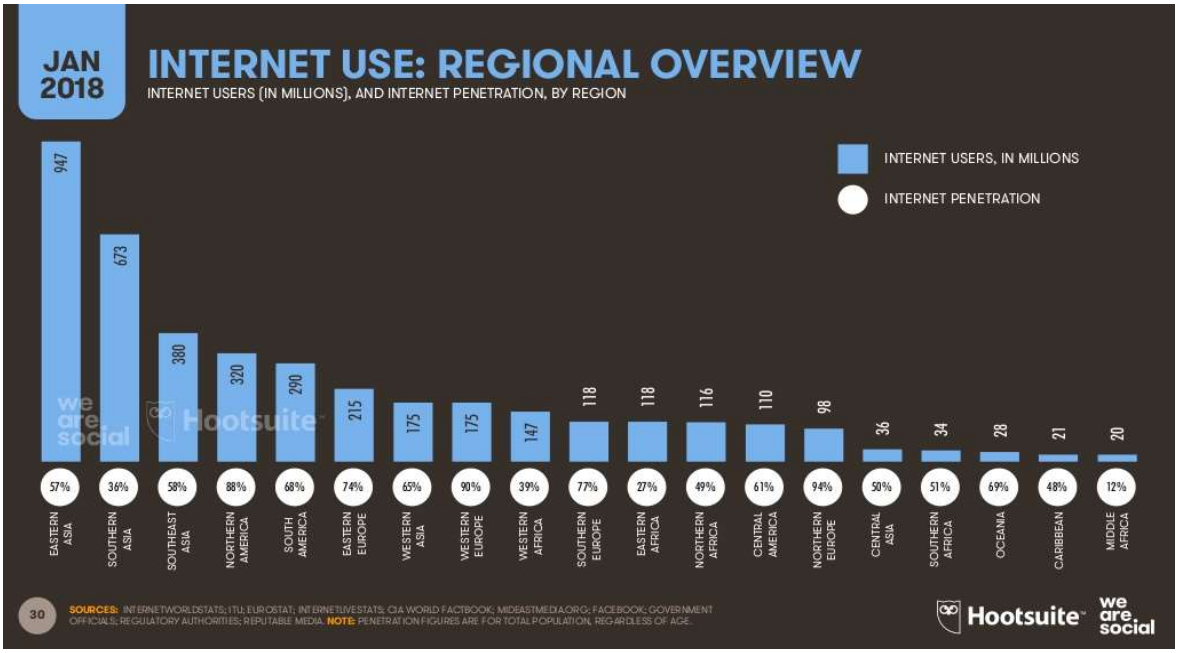
3: „Penetration of mobile banking, 2018", abrufbar unter:

https://wearesocial.com/de/blog/2018/01/global-digital-report-2018 (20.04.2018).

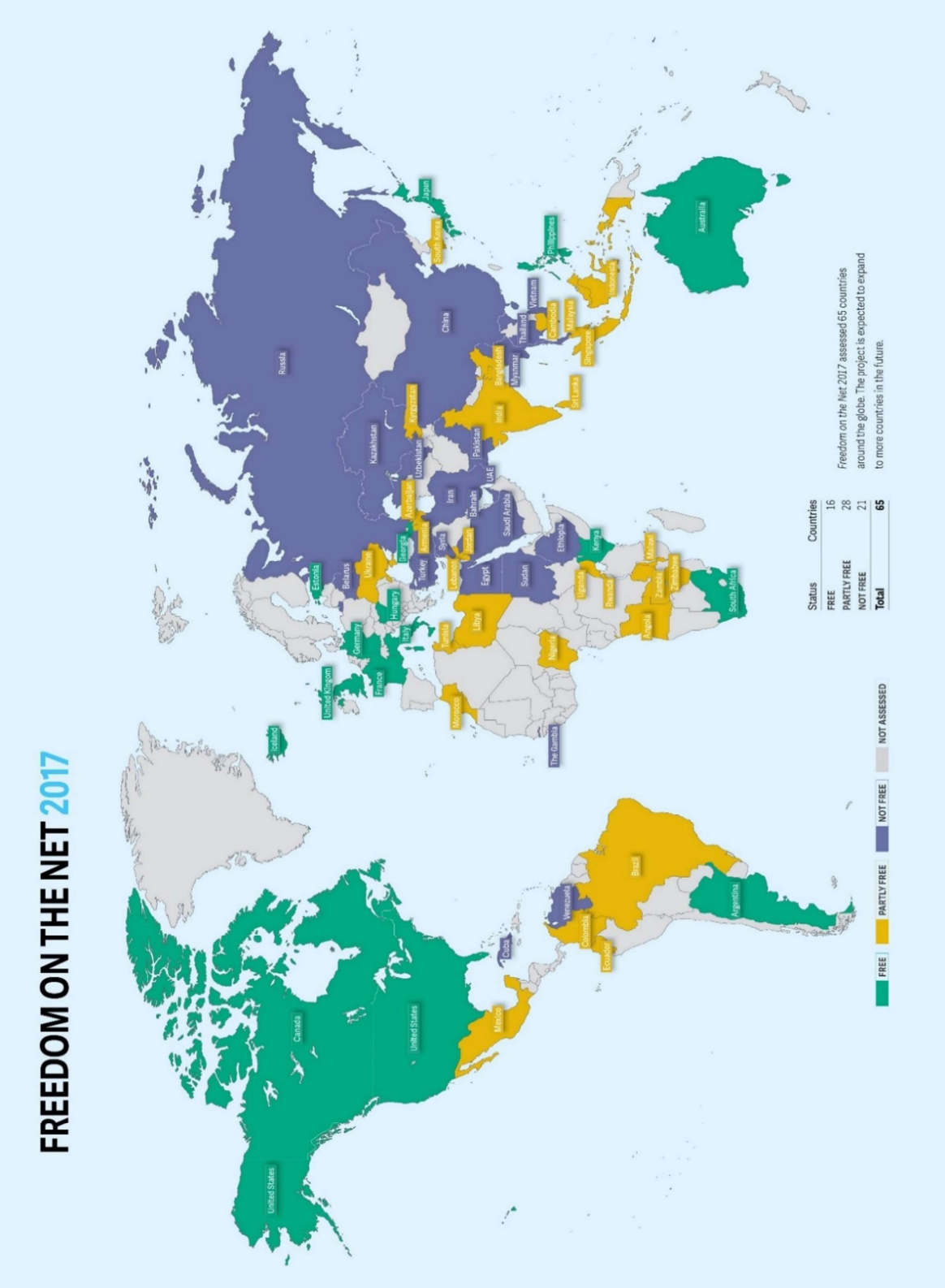


4: „Internet use: regional Overview, 2018”, Abrufbar unter dem Link:

https://wearesocial.com/de/blog/2018/01/global-digital-report-2018 (20.04.2018).



5: „Freedom on the Internet 2017”, Abrufbar unter: https://freedomhouse.org/report/freedom-net/freedom-net-2017 (21.04.2018).



Die Ressource: Freedom House

Literaturverzeichnis

Arnauld, Andreas von Völkerrecht, 3. Auflage, Heidelberg, 2016.

Bens, Jonas Cyberwar und völkerrechtliches Selbstverteidigungsrecht, BRJ 2 (2011), S. 149 – 155.

Bothe, Michael Stellungnahme zu Rechtsfragen des Cyberwars für den Verteidigungsausschuss des Deutschen Bundestages, Ausschussdrucksache 18 (12) 633, 17.2.2016.

BMI Cyber-Sicherheitsstrategie für Deutschland, 2016, abrufbar unter:https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (01.07.2018).

Clausewitz, Carl von Vom Kriege, Hamburg, 1987.

Dietz, Andreas Der Krieg der Zukunft und das Völkerrecht der Vergangenheit?, DÖV 12 (2011), S. 465 – 472.

Dittmar, Falko Angriffe auf Computernetzwerke- Ius ad bellum und ius in bello, Berlin, 2005.

Dörr, Oliver Gewalt und Gewaltverbot im modernen Völkerrecht, APuZ B 43 (2004), S.14 – 20.

EU KOM (2004) 702 „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung", abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33259 (20.04.2018).

EU Green Paper, 17.11.2005, Doc. COM (2005), 576 final, abrufbar unter:https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52005DC0576&from=EN (20.04.2018).

EU Schlussfolgerungen des Europäisches Rates zu den Themen Migration, Sicherheit und Verteidigung, Arbeitsplätze, Wachstum und Wettbewerbsfähigkeit, Innovation und Digitales sowie zu weiteren Themen, 28. Juni 2018, abrufbar unter: http://www.consilium.europa.eu/de/press/press-releases/2018/06/29/20180628-euco-conclusions-final/ (25.07.2018).

Fink, Udo Recht im virtuellen Raum: Die Rechtsordnung des Cyberspace, in: Odendahl, Kerstin und Giegerich, Thomas (Hrsg.), 2014, Berlin, S. 53 – 70.

Funke, Andreas Erga omnes – Pflichten, in: Schöbener, Burkhard (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, Heidelberg, 2014, S. 248 – 251.

Funke, Andreas Ius cogens – Normen, in: Schöbener, Burkhard (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, Heidelberg, 2014, S. 248 – 251.

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

Glenny, *Misha* Das Ende der Nettigkeiten, IP 6 (2012), S. 80 – 84.

Hegel, Georg Wilhelm F. Grundlinien der Philosophie des Rechts, Frankfurt am Main, 1986.

Heintschel von Heinegg Wolff Cyber-Bedrohungen aus dem Netz, IZPB 326 (2015), S. 23 – 27.

Heintschel von Heinegg, *Wolff* Cyberspace-Ein völkerrechtliches Niemandsland?, in: Schmidt -Radefeldt, Roman und Meissler, Christine (Hrsg.) Automatisierung und Digitalisierung des Krieges, 2012, Baden-Baden, S. 159 – 174.

Heintschel von Heinegg, *Wolff* § 52 Ausnahmen vom Gewaltverbot, in: Ipsen, Knut (Hrsg.), Völkerrecht, 6. Auflage, München, 2014, S. 1077 – 1099.

Heintschel von Heinegg, *Wolff* Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung, in: Epping, Volker/ Fischer, Horst/ Heintschel von Heinegg, Wolff (Hrsg.), Brücken bauen und begehen. FS für Knut Ipsen zum 65. Geburtstag, München, 2000, S. 129 – 156.

Heintschel von Heinegg, Wolff Völkerrecht im Cyberraum- Das Tallinn-Handbuch und der Tallinn-2- Prozess, W&F, Dossier 79, 3/2015, S. 5 – 7.

Heintschel von Heinegg, Wolff — Casebook Völkerrecht, München, 2005.

Heintschel von Heinegg, Wolff — § 53 Wahrung und Wiederherstellung des Weltfriedens und der internationalen Sicherheit durch Systeme kollektiver Sicherheit, in: Ipsen, Völkerrecht, 6. Auflage, München, 2014, S. 1100 – 1117.

Herdegen, Matthias — Völkerrecht, 16. Auflage, München, 2017.

Hobe, Stephan — Einführung in das Völkerrecht, 10. Auflage, Tübingen, 2014.

Hobe, Stephan/Fuhrmann, Johannes — Vom ius in bello zum ius contra bellum: Der Beitrag der Zweiten Haager Friedenskonferenz zur Entwicklung des modernen Völkerrechts, Die Friedens – Warte 82 (2007), S. 97 – 117.

Hoeren, Thomas/ Bensinger, Viola (Hrsg.) — Haftung im Internet, Berlin, 2014.

Ipsen, Knut — § 59 Anwendungsbereiche und Grundstruktur des Rechts des bewaffneten Konflikts, in: ders. (Hrsg.), Völkerrecht, 6. Auflage, München, 2014, S. 1196 – 1204.

Jellinek, Georg — Allgemeine Staatslehre, 3. Auflage, 6. Neudruck, Darmstadt, 1959.

Johnigk, Sylvia/ Nothdurft, Kai — Attributierung von Cyberangriffen- Das Problem und seine Folgen, W&F, Dossier 79, 3/2015, S. 7 – 12.

Keber, Tobias O./Roguski, P. Nick Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis, AVR 49 (2011), S. 399 – 434.

Kreß, Claus/Schiffbauer, Björn Erst versenkt, dann zu Völkerrecht erhoben, JA 2009, S. 611 – 616.

Krieger, *Heike* Krieg gegen Anonymus, AVR 50 (2012), S. 1 – 20.

Lacho, Irving und Richardson, Courtney Terrosit Use of the Internet The Real Story, JFQ 45, 2 (2007), S. 100 – 103.

Mayer, Franz C. Recht und Cyberspace, NJW, 1996, S. 1782 – 1792.

NATO Warsaw Summit Communiqué, 09. Juli 2016, abrufbar unter: https://www.nato.int/cps/en/natohq/official_texts_133169.htm, Ziff. 70 (01.07.2018).

NATO Cyber Security Strategy Documents, abrufbar unter: https://ccdcoe.org/cyber-security-strategy-documents.html (29.07.2018).

NATO Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Adopted by Heads of State and Government in Lisbon, 19/20.11.2010, abrufbar unter: https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (27.07.2018).

NATO Cyber defense, abrufbar unter: https://www.nato.int/cps/en/natohq/topics_78170.htm (27.07.2018).

Neuneck, Götz/ Reinhold, Thomas Die Militarisierung des Cyberspace, W&F, Dossier 79, 3 (2015), S. 3 – 4.

Oellers-Frahm, Karin Der IGH und die Lücke zwischen Gewaltverbot und Selbstverteidigungsrecht- Neues im Fall „Kongo gegen Uganda?“, ZEuS 1 (2007), S. 71 – 92.

Pichler, Rufus Internationale Zuständigkeit im Zeitalter globaler Vernetzung, München, 2008.

Plate, Tobias Völkerrechtliche Fragen bei Gefahrenabwehrmaßnahmen gegen Cyber-Angriffe, ZRP (2011), S. 200 – 202.

Randelzhofer, Albrecht Art. 2 Ziff.4, in: Simma, Bruno (Hrsg.), Charta der Vereinten Nationen, München, 1991, S. 67 – 90.

Sartorius II Internationale Verträge Europarecht Textsammlung, Lieferung 58, März 2016.

Schaller, *Christian* Internationale Sicherheit und Völkerrecht im Cyberspace SWP-Studie, Berlin, 2014.

Schmahl, Stefanie Cybersecurity, in: Dethloff, Nina/ Nolte, Georg/ Reinisch, August (Hrsg.), Freiheit und Regulierung in der Cyberwelt-Rechtsidentifikation zwischen Quelle und Gericht, BDGVR (47), 2016, S. 159 – 190.

Schmahl, Stefanie Zwischenstaatliche Kompetenzabgrenzung im Cyberspace AVR 47 (2009), S. 284 – 327.

Schmitt, *Michael N. (Hrsg.)/ Internationale Expertengruppe* Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013 (zitiert nach: Tallinn Manual).

Schmitt, *Michael N. (Hrsg.)/ Internationale Expertengruppe* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017 (zitiert nach: Tallinn Manual 2.0).

Schmitt, Michael N. Angriffe im Computernetz und das ius ad bellum, NZWehrr 5 (1999), S. 177 – 195.

Schöbener, *Burkhard* Verantwortlichkeit, völkerrechtliche, in: ders. (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, Heidelberg, 2014, S. 483 – 490.

Schöbener, Burkhard Gewaltverbot, universelles, in: ders. (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, Heidelberg, 2014, S. 126 – 133.

Schöbener, Burkhard Uniting for Peace-Resolution (1950), in: ders. (Hrsg.), Völkerrecht-Lexikon zentraler Begriffe und Themen, 2014, S. 481 – 483.

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

Stadlmeier, Sigmar/ Unger, Walter J. Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht, Schmalenbach, Kirsten (Hrsg.) in: Aktuelle Herausforderungen des Völkerrechts: Beiträge zum 36. Österreichischen Völkerrechtstag 2011, S. 63 – 80.

Stein, Torsten/ Buttlar, Christian von/ Kotzur, Markus Völkerrecht, 14. Auflage, München, 2017.

Stein, Torsten/ Marauhn, Thilo Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), S. 1 – 40.

Todd, Graham H. Armed Attack in Cyberpace: Deterring Asymmetric Warfare with an Asymmetric Definiton, Air Force Law Review 64 (2009), S. 65 – 102.

UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN-Doc. A/68/98, 24.06.2013, abrufbar unter: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf (01.07.2018).

UN UN-GA „Developments in the field of information and telecommunications in the context of international security", 04.12.1998, UN Doc. A/RES/53/70, abrufbar unter: https://www.un.org/disarmament/topics/informationsecurity/ (20.07.2018).

UN GA Res. 3314 (XXIX) „Definition der Aggression“ vom 14.12.1974, Sartorius II Nr. 6.

UN GA Res. 2625 (XXV) „Friendly Relations“- Deklaration vom 24.10.1970, Sartorius II Nr. 4.

UN S/Res/1368 (2001), S/ Res/1373 (2001), S/Res/1540 (2004) und S/Res/2178 (2014), abrufbar unter: http://www.un.org/en/sc/documents/resolutions/ (20.07.2018).

UN UN- GA “Resolution adopted by the General Assembly 377 (V). Uniting for Peace”, 03.11.1950, UN Doc. A/RES/5/377, abrufbar unter: http://www.un-documents.net/a5r377.htm (20.07.2018).

US DoD Department of Defense Dictionary of Military and Associated Terms, Juni 2018, S. 59. Abrufbar unter: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (01.07.2018).

Wiegandt, Jan Internationale Rechtsordnung oder Machtordnung? (ZaöRV) 71 (2011), S. 31 – 76.

Wiegold, Thomas Cyberwar: Bundeswehr meldet „Anfangsbefähigung zum Wirken“, augengeradeaus.net, 05.06.2012.

Ziolkowski, Katharina Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen, HuV-I 21 (2008), S. 202 – 213.

Gerichtsentscheidungen

IGH, Urteil vom 13.09.1928 Case concerning the Factory at Chorzów (*Chorzów III*), PCIJ Series A No. 17.

IGH, Urteil vom 09.04.1949 The Corfu Cahnnel Case (Merits) (*Corfu Channel II*), ICJ Reports 1949, 4.

IGH, Urteil vom 05.02.1970 Case concerning the Barcelona Traction, Light and Power Company, Limited (New Application 1962) (Second Phase) (*Barcelona Traction II*), ICJ Reports 1970, 3.

IGH, Urteil vom 27.06.1986, Military and Paramilitary Activities in and against Nicaragua (Merits) (*Nicaragua II)*, ICJ Rep. 1986, 14.

IGH, Gutachten vom 08.07.1996 Legality of the Threat or Use of Nuclear Weapons (*Nuclear Weapons*), ICJ Reports 1996, 226.

IGH, Urteil vom 06.11.2003 Case concerning Oil Platforms (Merits) (*Oil Platforms II*), ICJ Reports 2003, 161.

IGH, „ *Mauer*"-Gutachten vom 09.07.2004 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ Reports 2004, 136.

IGH, Urteil vom 13.07.2009 Dispute Regarding Navigational and Related Rights (*Costa Rica v. Nicaragua*), ICJ Reports 2009, s. 213.

ICTY, *Prosecutor v. Tadic*. Case IT-94-1-T, Judgment and Opinion

Internetquellen

https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (02.05.2018).

https://de.wikipedia.org/wiki/Chronologie_des_Internets (30.03.2018).

https://de.wikipedia.org/wiki/Arpanet (30.03.2018).

https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity (12.01.2018).

https://www.welt.de/wirtschaft/webwelt/article3355416/Kreml-Jugend-bekennt-sich-zu-Attacke-auf-Estland.html (19.07.2018).

http://www.faz.net/aktuell/politik/ausland/computerwurm-israel-testete-stuxnet-in-geheimer-atomanlage-1573182.html (14.03.2018).

https://de.wikipedia.org/wiki/Edward_Snowden (29.07.2018).

https://www.sueddeutsche.de/digital/us-bundesverwaltung-millionen-us-amerikaner-von-cyber-angriff-betroffen-1.2559663 (19.07.2018).

https://wearesocial.com/de/blog/2018/01/global-digital-report-2018 (20.04.2018).

https://www.turkiye.gov.tr/bilgilendirme?konu=siteHakkinda.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (20.04.2018).

https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf, S. 12 (20.04.2018).

http://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf (20.04.2018).

https://freedomhouse.org/report/freedom-net/freedom-net-2017 (21.04.2018).

https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce2010 (24.07.2018).

https://www.unric.org/de/aufbau-der-uno/46 (20.04.2018).

http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?ref=world (10.07.2018).

http://archive.defense.gov/speeches/speech.aspx?speechid=1593 (20.05.2018)

https://www.drk-mittelhessen.de/fileadmin/Bilder_und_Videos/PDFs/Das_DRK/Materialien/Allgemein/Das_Humanitaere_Voelkerrecht__Antworten_auf_Ihre_Fragen.pdf. (25.07.2018).

http://www.spiegel.de/forum/netzwelt/cyberangriffe-auf-infrastruktur-mit-einem-hack-ist-alles-weg-thread-686918-1.html (10.07.2018).

https://www.sueddeutsche.de/wirtschaft/sicherheit-kalter-krieg-im-netz-1.3273614 (10.07.2018).