StrafR Aufsatz

Luca Alexander Petersen*

Cyberangriffe – Definition, Regulierung, Pönalisierung

Cyberangriffe stellen ein viel genutztes Mittel der modernen Kriegsführung dar. Dabei wird die Nutzung vielfach heruntergespielt und auf vermeintlich bestehende Rechtslücken verwiesen. Der Beitrag setzt sich daher mit der Definition, Regulierung und Pönalisierung solcher Angriffe auseinander.

A. Einleitung

Medienberichten zufolge schossen iranische Streitkräfte am 20. 6. 2019 eine amerikanische Drohne vom Himmel, da sich diese im iranischen Luftraum befunden habe.[1] Der Gegenschlag der USA ließ nicht lange auf sich warten. Es sei jedoch kein traditioneller Gegenschlag mit kinetischer, also durch mechanische Übertragung wirkender,[2] Waffengewalt gewesen. Vielmehr wurden die Wirtschaftssanktionen weiter verschärft und eine Cyberoperation durchgeführt.[3] Der US-Präsident *Trump* rechtfertigte dieses Vorgehen damit, dass ein hypothetischer traditioneller militärischer Gegenschlag 150 Todesopfer hätte erwarten lassen, was im Vergleich zum Abschuss einer Drohne als unverhältnismäßig anzusehen sei.[4] Diese Stellungnahme vermag zunächst zu überzeugen. Sie birgt jedoch durch das häufige Einsetzen von vermeintlich minder schweren Cyberoperationen und das dadurch steigende Potenzial schwererer Gegenmaßnahmen die Gefahr einer Gewalteskalation in sich.[5] Cyberangriffe sind verdeckt. Einzig die sich daraus ergebenden Folgen sind sichtbar und können im Einzelfall der Wirkung traditioneller militärischer Angriffe mit Objekt- oder Personenschäden gleichkommen.[6] Sie sind zudem nur schwierig zurückzuverfolgen, was den Beweis einer Rechtsverletzung erheblich erschwert.[7] Durch die derzeitigen Cyberoperationen wird ein solches Vorgehen normalisiert und gleichermaßen in seiner Bedeutung heruntergespielt.[8] Viele Beispiele zeigen, dass Cyberangriffe mittlerweile zu einem gängigen, in der Nutzung exponentiell ansteigenden[9] Instrument innerhalb internationaler Konflikte geworden sind. 2007 wurde Estland durch mehrere *denial-of-services-attacks* über einen Zeitraum von drei Wochen nahezu vom gesamten internationalen Informationsfluss abgeschottet.[10] 2010 zerstörten die USA in Zusammenarbeit mit Israel mittels eines Wurmes (»Stuxnet«)[11] massenhaft zur Urananreicherung genutzte Zentrifugen des Iran.[12] Besondere Bedeutung weist der jüngste Angriff der USA auf eine iranische Computerdatenbank auf, die zur Planung von Angriffen auf Öltanker verwendet wurde.[13] Er zeitigte keinerlei physische, sondern nur Datenschäden, die die Funktionsfähigkeit der Militärbasis beeinträchtigten. Dass der Angriff gerade als Reaktion auf Militärschläge auf amerikanische Öltanker im Golf von Oman erfolgte, zeigt, dass diese neuartige Waffentechnologie längst mit traditionellen Waffen in Verbindung gebracht wird.[14] Ihr Gebrauch wirft rechtliche Fragen auf. So zeigt sich, dass die Operationen im Cyberraum vielfältig und häufig mit kinetischen Angriffen nur bedingt vergleichbar sind.[15] Im Vordergrund sollen aufgrund der Aktualität staatlich veranlasste militärische Cyberangriffe stehen, die nur auf Beschädigung oder Zerstörung von Daten abzielen und keine physischen Schäden zeitigen. Dies stellt den bestehenden Rechtsrahmen im humanitären Völkerrecht (huVR) und im

* Dipl.-Jur. *Luca Alexander Petersen* ist wissenschaftliche Hilfskraft am Lehrstuhl für Straf- und Strafprozessrecht, Rechtsvergleichung, internationales Strafrecht und Völkerrecht, Doktorand bei Prof. Dr. Dr. h. c. *Kai Ambos* und wissenschaftlicher Mitarbeiter bei Hogan Lovells International LLP in Hamburg. Der Beitrag ist eine verkürzte und aktualisierte Form der Studienarbeit, die im Seminar »Waffen- und Waffensysteme im (Humanitären) Völker(straf)recht« im WiSe 2019/2020 bei Prof. Dr. Dr. h. c. *Kai Ambos* geschrieben wurde.

1 *Al Jazeera News,* US-Iran standoff: A timeline of key events, 25. 9. 2019, https://www.aljazeera.com/news/2019/06/iran-standoff-timeline-key-events-190622063937627.html, zuletzt aufgerufen am 8. 6. 2020.

2 Vgl. *Neuneck,* Neue Waffentechniken und Rüstungskontrolle – Strahlen- und kinetische Waffen, Physik in unserer Zeit, 2001, 10 (10).

3 Vgl. *Tagesschau,* USA starteten Cyberangriffe auf den Iran, 23. 6. 2019, https://www.tagesschau.de/ausland/usa-iran-151.html, zuletzt aufgerufen am 13. 3. 2020.

4 *Trump* (@realDonaldTrump), Twitter, Tweet vom 21. 6. 2019, https://twitter.com/realDonaldTrump/status/1142055392488374272, zuletzt aufgerufen am 13. 3. 2020.

5 *Dornbusch,* Das Kampfführungsrecht im internationalen Cyberkrieg (2018), S. 102; einen Vergleich zum Kalten Krieg zieht *Akoto,* Les Cyberattaques etatiques constituent-elles des actes d'agression en vertu du droit international public: Deuxieme partie, OttawaLRev 2014, 199 (199, 230).

6 *Dornbusch* (Fn. 5), S. 100 ff.

7 *Schulze,* Cyber-»War« – Testfall der Staatenverantwortlichkeit (2015), S. 134.

8 *Rötzer,* USA–Iran: Sollen Cyberangriffe Kriege vermeiden?, heise.online, 2. 10. 2019, https://www.heise.de/tp/features/USA-Iran-Sollen-Cyberangriffe-Kriege-vermeiden-4544258.html, zuletzt aufgerufen am 13. 3. 2020.

9 *Moore,* Cyber Attacks and the Beginnings of an International Cyber Treaty, NCJIntL&ComReg 2013, 223 (229 f.).

10 Vgl. *Dornbusch* (Fn. 5), S. 31 f., *denial-of-services-attacks* bezeichnen eine Manipulation durch eine Vielzahl von Anfragen, die eine Überbelastung des Systems herbeiführen (31); *Radziwill,* Cyber-Attacks and the Exploitable Imperfections of International Law (2015), S. IX.

11 Ein Wurm stellt eine sich selbstständig über Computernetzwerke verbreitende *malware* dar, vgl. *Woltag,* Cyber Warfare: Military Cross-Border Computer Network Operations under International Law (2014), S. 47.

12 *Woltag* (Fn. 11), S. 47; *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (226).

13 *Nakashima,* Washington Post, Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers, 22. 6. 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?noredirect=on, zuletzt aufgerufen am 13. 3. 2020.

14 *Weisbord,* Judging Aggression, ColumJTransnatlL 2011, 82 (152).

15 *Dornbusch* (Fn. 5), S. 29.

Völkerstrafrecht (VStR) vor enorme Unsicherheiten. Eben diese Unsicherheiten werden vielfach ausgenutzt.[16] Teilweise wird eine ganz eigene Regulierung von Cyberoperationen gefordert.[17] Dieser Beitrag zeigt jedoch, dass sich ein einheitlicher Begriff des Cyberangriffs bestimmen lässt (dazu B.). Auch die Regelungen des *ius ad bellum* (C. II. 3.) und *ius in bello* (C. III. 4.) lassen sich auf diese Art von Angriffen anwenden.[18] So können Cyberangriffe auch ohne physischen Schaden eine Gewaltanwendung oder einen bewaffneten Angriff darstellen. Einer erweiterten Pönalisierung im VStRs bedarf es daher nicht (C. V.).

B. Der Begriff des Cyberangriffs

Der Begriff »Cyberangriff« ist stark umstritten.[19] Verkürzt ist dabei zunächst zu differenzieren, ob »Cyber« das Instrument zur Durchführung des Angriffs darstellt oder vielmehr das Objekt; also ob sich der Cyberangriff durch die »Waffe«[20] oder durch das Ziel definiert.[21] Will man sich ernsthaft mit den Besonderheiten des Cyberangriffs auseinandersetzen, ist der Blick auf das Instrument zu richten.[22] Dies zeigt nicht zuletzt ein Vergleich mit Chemiewaffen. Das Ziel, die Schädigung von Personen, ist das gleiche wie bei einem konventionellen Militärschlag. Die Folgen treten dagegen häufig nur mittelbar ein, was die Besonderheit des Einsatzmittels aufzeigt.[23] Es ist daher nicht darauf abzustellen, ob durch den Angriff ein Computernetzwerk betroffen ist, sondern vielmehr, ob der Cyberraum für den Angriff genutzt wird.[24] Davon ausgehend ist jedoch weiterhin unklar, wann ein Cyber*angriff* tatsächlich als solcher zu bezeichnen ist.[25] So werden recht uneinheitlich für scheinbar gleiche Maßnahmen die Begriffe »cyberstrikes«, »cyber-attack«, »computer network attack« verwendet.[26] Das Bundesinnenministerium (BMI) differenziert zwischen Cyber-Angriff, Sabotage, Ausspähung und Spionage.[27] Aus allen Begrifflichkeiten lässt sich zunächst entnehmen, dass der Begriff »Cyberoperationen« als Oberbegriff verwendet werden kann.[28] Es überzeugt, darunter zwischen »Cyberangriffen« und sonstiger »Cyberausnutzung« zu differenzieren.[29] Unter eine Ausnutzung sind vor allem Cyberspionage und Cybermanipulationen zu fassen.[30] Ein Cyber*angriff* zeichnet sich durch grds. schwerwiegendere Schädigungen von Objekten oder Personen aus.[31] *Schmitt et al.* konkretisieren die Definition wie folgt:[32] »Ein Cyberangriff ist eine offensive oder defensive Cyberoperation, die mit hoher Wahrscheinlichkeit Verletzungen oder den Tod von Personen oder Beschädigung oder die Zerstörung von Objekten verursachen wird.«[33] Diese Definition ist offensichtlich an die allgemeine Definition des »Angriffs« i. S. d. Art. 49 I des Zusatzprotokolls I zu den Genfer Konventionen (GK ZP I) angelehnt, sodass die Kritik von *McGhee,* diese Definition sei nur die des »Angriffs« mit dem Zusatz »Cyber«, als berechtigt anzusehen ist.[34] Dies ist jedoch mit Blick darauf, dass sie eine gewisse Schwere des Angriffs hervorhebt und dadurch Cyberspionage und psychologische Cyberoperationen, nicht aber nicht-physische Schäden *per se,* ausschließt, durchaus sachgerecht.[35] Bei der Kritik, die Definition sei zu wenig konkret,[36] muss zudem berücksichtigt werden, dass diese in der Kommentierung

16 *Djabatey,* Reassessing U. S. Cyber Operations Against Iran and the Use of Force, 17. 10. 2019, https://www.justsecurity.org/66628/reassessing-u-s-cyber-operations-against-iran-and-the-use-of-force, zuletzt aufgerufen am 13. 3. 2020.

17 *Arimatsu,* A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, in: *Czosseck et al.* (Hrsg.), 4th International Conference on Cyber Conflict: Proceedings, NATO CCD COE Publications, Tallinn, 2012, https://ccdcoe.org/uploads/2019/03/CyCon_book_2012.pdf, zuletzt aufgerufen am 10. 12. 2019, S. 91.

18 *Ius ad bellum* bezeichnet das Recht auf/zum Krieg, *ius in bello* dagegen das im bewaffneten Konflikt anwendbare Völkerrecht, *von Heinegg,* in: Epping/v. Heinegg (Hrsg.), Völkerrecht – Ein Studienbuch, 7. Auflage (2018), § 50 Rn. 1 ff., § 60 Rn. 1 ff.

19 *Radziwill* (Fn. 10), S. 11 f.

20 Zum Begriff des Cyberinstruments als Waffe: *Boothby,* Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors (2014), S. 176 ff.

21 *Nguyen,* Navigating *Jus Ad Bellum* in the Age of Cyber Warfare, CaliLRev 2013, 1079 (1086).

22 *Nguyen* (Fn. 21) CaliLRev 2013, 1079 (1083 f.).

23 *McGhee,* Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy, JLCyberWarfare 2013, 64 (91).

24 *Nguyen* (Fn. 21) CaliLRev 2013, 1079 (1088); a. A.: *Hathaway et al.,* The Law of Cyber-Attack, CaliLRev 2012, 817 (826), die jedoch von ihre Defintion von der überholten Definition des *U. S. Department of Defense* abhängig zu machen scheint; vgl. auch *Dornbusch* (Fn. 5), S. 33 f.

25 Vgl. *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (232).

26 *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (232); *Nguyen* (Fn. 21) CaliLRev 2013, 1079 (1085); *Radziwill* (Fn. 10), S. 11 f.

27 *BMI,* Cyber-Sicherheitsstrategie für Deutschland 2011, https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Cyber_Sicherheitsstrategie2011.pdf?__blob=publicationFile, zuletzt aufgerufen am 13. 3. 2020, S. 14 f.

28 *Kittichaisaree,* Public International Law of Cyberspace (2017), S. 154; *Schmitt et al.,* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2. Auflage (2017), S. 564.

29 »Cyber attacks and cyber exploitations«, *Roscini,* Cyber Operations and the Use of Force in International Law (2014), S. 16; *Gervais,* Cyber Attacks and the Laws of War, JLCyberWarfare 2012, 19 ff.

30 Dazu *Buchan,* Cyber Espionage and International Law (2018) S. 13 ff. So ist insbes. Spionage nach internationalem Recht nicht verboten und gehört vielmehr zur allgemeinen Staatenpraxis, vgl. dazu *McGhee,* Hack, Attack or Whack; The Politics of Imprecision in Cyber Law, JLCyberWarfare 2014, 13 (17 f.); Eine Veränderung in diesem Bereich erkennt *Buchan* (S. 66 ff.).

31 Vgl. *McGhee* (Fn. 30), JLCyberWarfare 3 (2014), 13 (14); *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (232).

32 Eine *allgemeine* Definition des Cyberangriffs wird häufig in verschiedenen Bereichen des Konfliktvölkerrechts behandelt und daher ist teilw. eine Verbindung zu der Definition eines »Angriffs« insbes. i. S. v. Art. 51 UN-Ch und Art. 49 I GK ZP I zu berücksichtigen. Durch die vielfältige Verwendung und Verweisung scheint es so, als seien in der Literatur Fragen der Definition mit solchen der Subsumtion vermengt worden; dies erkennt im Ansatz auch *Focarelli,* Self-Defence in Cyberspace, in: Tsagourias/Buchan (Hrsg.), Research Handbook on International Law in Cyberspace (2015), S. 255, 283.

33 »A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.«, *Schmitt et al.* (Fn. 28), S. 415, Rule 92 (Übersetzung durch den Verf.).

34 *McGhee* (Fn. 23) JLCyberWarfare 2013, 64 (90 f.).

35 *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (233).

36 *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (233).

näher konkretisiert wird[37]. Mit Blick in die Zukunft bedarf es letztlich allerdings einer konkreten Definition, die den Cyberangriff hinsichtlich der Intensität von anderen Cyberoperationen abgrenzt sowie die Besonderheiten der Vielfältigkeit der Angriffe umfasst.[38] Nach alledem ist ein Cyberangriff als *eine defensive oder offensive Operation* zu verstehen, *die mittels eines Computernetzwerkes durchgeführt wird, um unmittelbar oder mittelbar einen physischen Schaden an einem Objekt oder den Tod oder Verletzungen von Personen zu verursachen, oder um durch eine Datenbeschädigung oder -zerstörung die Funktionsfähigkeit eines Computernetzwerkes in erheblicher Weise zu beeinträchtigen.*[39]

C. Regulierung

Es stellt sich die Frage, ob Cyberangriffe einer Regulierung im internationalen Recht bedürfen und – bejahendenfalls –, ob sie durch das bestehende System bereits erfasst werden.

I. Regulierungsbedürftigkeit

Völkerrechtliche Regulierung meint die freiwillige kollektive Bindung mittels eines völkerrechtlichen Vertrages zwischen Staaten und/oder internationalen staatlichen Organisationen, um bestimmte Verhaltensweisen, basierend auf dem Konsensprinzip, durch Rechte und Pflichten verbindlich zu regeln.[40] Die Regulierung ist dabei stark politisch geprägt.[41] Sie folgt regelmäßig einer Funktion, wie im vorliegenden Fall der *Sicherung des Friedens und der internationalen Sicherheit.*[42] In diesem Bereich gibt es bereits eine Vielzahl von Regulierungen.[43] Insofern fragt sich, ob überhaupt ein Regelungsbedürfnis besteht.[44] Ein solches liegt regelmäßig vor, wenn sich unter Betrachtung der völkerrechtlichen Regelungen eine erhebliche Lücke aufzeigt, die nicht durch Auslegung zu schließen ist, und sich ein Konsens hinsichtlich der Notwendigkeit einer Normierung durch die Staaten bildet.[45] Regulierungen, insbes. im Völkerrecht, entstehen i. d. R. retroaktiv.[46] Dies liegt darin begründet, dass die Regulierungsbedürftigkeit erst festgestellt wird, wenn Situationen auftreten, die diese offenbaren.[47] Dagegen sind jedoch die bestehenden Regelungen häufig so weit gefasst, dass sie durch eine dynamische Auslegung auf aktuelle Veränderungen reagieren können.[48] Sowohl die UN-Charta als auch das huVR sind weit gefasst und sollen nicht nur die Fälle umfassen, die bei der Ausarbeitung der Verträge bereits erkennbar waren.[49] Nach dem oben Aufgeführten scheinen die kontrovers diskutierten Regulierungsansätze ein Regelungsbedürfnis grds. anzuzeigen. Möglicherweise fehlt es jedoch bereits an einer Regelungslücke und es besteht eine ausreichende Regulierung.

II. Cyberspace als nicht-eigenständiger Raum

Zunächst ist dafür zu untersuchen, ob die bestehenden Regelungen des *ius ad bellum* und *ius in bello* auf den Cyberraum und damit auch auf Cyberangriffe Anwendung finden können. Dies wäre dann nicht der Fall, wenn man den Cyberraum neben dem Land-, Luft-, See- und Weltraum[50] als eigenständigen Raum im völkerrechtlichen Sinne betrachten würde, weil ihm dann ein eigener rechtlicher Status zukäme.[51] Dies ist jedoch dahingehend abzulehnen, als dass der Cyberraum kein vergleichbarer souveränitätsfreier Raum, d. h. ein solcher ohne nationalstaatliche oder übergeordnete Hoheitsgewalt, ist.[52] Er ist nicht von der »realen Welt« losgelöst,[53] sondern stellt einen durch physische Konstruktionen geschaffenen Raum dar, der seine Verbindung zu diesen nicht verloren hat und einem Souverän zugeordnet werden kann.[54] Durch die Verbindung zwischen virtuellem Cyberraum und physischen Netzwerkkomponenten (Hardware) erstreckt sich die territoriale Hoheitsgewalt darauf.[55] Dies muss auch für die Daten gelten, die für den Austausch auf dieser physischen Ebene, also für die Funktionsfähigkeit, notwendig sind.[56] Aufgrund des Zieles des Grundsatzes der Souveränität, dem Staat die volle Kontrolle über den Zugang zu seinem Hoheitsgebiet und die Tätigkeiten in diesem zu gewähren,[57] muss dies auch für die Zerstörung oder Beschädigung gelten, die die Funktionsfähigkeit beeinträchtigt[58]. Durch einen solchen Angriff wird daher in die staatliche Souveränität in Form der territorialen Integrität eingegriffen.

III. Ius ad bellum

Cyberangriffe unterfallen damit grds. auch dem internationalen Recht. Dieser Rechtsrahmen ist unvollständig (bzw. unvollständig erforscht),[59] was die Gefahr der Ausnutzung von (vermeintlichen) Rechtslücken birgt.[60] Ob eine Rechtslücke tatsächlich besteht und es einer eigenständigen Regulierung bedarf, wird nachstehend untersucht.

---

37 Vgl. *Schmitt et al.* (Fn. 28), S. 415, Rule 92, Rn. 1–21.

38 Vgl. *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (232 ff.); *Roscini* (Fn. 29), S. 16 ff; *Hathaway et al.* (Fn. 24), CaliLRev 2012, 817 (822); *Nguyen* (Fn. 21) CaliLRev 2013, 1079 (1085 ff.).

39 Einen vergleichbaren Ansatz wählt *Roscini* (Fn. 29), S. 17. Vertiefend sei in diesem Zusammenhang zudem auf die Diskussion unter C. III. 1. und die Anmerkung in Fn. 93 verwiesen.

40 Vgl. *Ipsen* (Fn. 18), § 3 Rn. 3 ff., 14, 21.

41 *Herdegen,* Völkerrecht, 8. Auflage (2019), § 4 Rn. 1 ff.

42 *Ipsen* (Fn. 18), § 3 Rn. 14.

43 Allgemein zum Konfliktvölkerrecht, *Dornbusch* (Fn. 5), S. 60 ff.

44 Dazu *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (230).

45 *Moore* (Fn. 9), NCJIntL&ComReg 2013, 223 (250 ff.).

46 *Dornbusch* (Fn. 5), S. 60.

47 *Dornbusch* (Fn. 5), S. 60.

48 *v. Heinegg* (Fn. 18), § 15 Rn. 21.

49 *v. Heinegg* (Fn. 18), § 15 Rn. 21, § 55 Rn. 18 ff.

50 Dazu *Herdegen* (Fn. 41), § 31 und § 32.

51 *Dornbusch* (Fn. 5), S. 26.

52 *Radziwill* (Fn. 10), S. 88.

53 *Dinniss,* Cyber Warfare and the Laws of War (2012), S. 28; *Dornbusch* (Fn. 5), S. 26.

54 *Dinniss* (Fn. 53), S. 28; *Schulze* (Fn. 7), S. 112.

55 *Schmitt et al.* (Fn. 28), S. 12, Rule 1, Rn. 4.

56 *Schmitt et al.* (Fn. 28), S. 12, Rule 1, Rn. 4; Vgl. auch UN-Generalversammlung, Developments, 24. 6. 2013, UN Doc. A/68/98, Ziff. 20.

57 Vgl. *Schmitt et al.* (Fn. 28), S. 19 (Rule 4), Rn. 14.

58 *v. Heinegg,* Legal Implications of Territorial Sovereignty in Cyber-Space, in: (Fn. 17), S. 7, 14; *Schmitt et al.* (Fn. 28), S. 20, Rule 4, Rn. 13.

59 *Radziwill* (Fn. 10), S. 4 f.

60 *Radziwill* (Fn. 10), S. 5.

1. Cyberangriff als Gewaltanwendung i. S. v. Art. 2 IV UN-Ch

Damit ein Cyberangriff eine *Gewaltanwendung* (»use of force«) darstellen kann, müsste er als Gewalt i. S. d. Art. 2 IV UN-Ch zu begreifen sein. Das Gewaltverbot, das zum Gewohnheitsrecht geworden ist und nach ganz herrschender Meinung auch zum zwingenden Völkerrecht *(ius cogens)* gehört,[61] umfasst die Anwendung bewaffneter oder militärischer Gewalt, die einem Staat zurechenbar ist.[62] Dies entspricht der gewöhnlichen und im Zusammenhang stehenden Bedeutung im engeren Sinne, vgl. Art. 31 I WÜRV.[63] Darüber hinaus können, insbes. in Abgrenzung zu Art. 51 UN-Ch (»armed attack«) und Art. 44 UN-Ch (»armed forces«), auch indirekte Gewalt[64] und in Grenzen auch – zumindest im traditionellen Sinne – nicht als militärisch erachtete physische Gewalt unter das Verbot fallen.[65] Nach ganz h. M. meint dies jedoch wiederum Waffengewalt und nicht wirtschaftlichen oder politischen Zwang, der vielmehr unter das Interventionsverbot fällt.[66] Was genau dagegen unter der *Gewalt* zu verstehen ist, ist weiterhin stark umstritten.[67] In der Konsequenz ist die Einordnung von Cyberangriffen mit nur mittelbaren Schäden oder reinen Datenschäden als Gewalt schwierig.[68] Ausgangspunkt der Überlegung muss dabei das Ziel der UN-Charta sein, beständigen Frieden zu schaffen und vor Gewalttätigkeiten zu schützen.[69] Zum einen darf dabei der Begriff der Gewalt nicht zu eng verstanden werden, um ein möglichst breites Verbot und damit einen größtmöglichen Schutz zu gewährleisten. Zum anderen darf der Begriff nicht zu weit verstanden werden, da damit ggf. auch das Recht zur Selbstverteidigung gem. Art. 51 UN-Ch einhergeht.[70] In der Literatur haben sich mehrere Ansätze entwickelt, um diesen Zwiespalt zu lösen: Im Mittelpunkt steht dabei die Frage, unter welchen Anforderungen ein Cyberangriff, obwohl er keine traditionelle »bewaffnete« Gewalt darstellt, als Gewaltanwendung angesehen werden kann.[71] Dabei ist zu differenzieren: Mittlerweile recht unumstritten fallen Cyberangriffe, die zu (mittelbaren) physischen Schäden führen, unter das Gewaltverbot.[72] Bei dem jüngsten militärischen Angriff der USA auf die iranische Computerdatenbank handelt es sich jedoch weder um eine bloß psychische noch um eine rein wirtschaftliche oder politische Zwangsmaßnahme.[73] Zudem enthält Art. 2 IV UN-Ch selbst nicht den Zusatz der »bewaffneten« Gewalt.[74] Maßgeblich kommt es darauf an, woran für die Gewaltanwendung angeknüpft wird.

a) Instrument-based-Ansatz

Nach dem *instrument-based*-Ansatz ist für diese Frage das Mittel, das für die Schädigungshandlung oder Zwangsausübung eingesetzt wird, selbst ausschlaggebend.[75] Zwar scheint dieser Ansatz mit Blick auf die betreffende Frage zunächst konsequent, da es gerade um die Art der »Waffe« geht. Ein zweiter Blick belegt jedoch, dass dieser nur bedingt praktikabel ist. Der Ansatz ist extrem weit gefasst und geht nicht auf die technischen Besonderheiten einer Waffe ein.[76] Innerhalb dieses Ansatzes schwanken die genauen Voraussetzungen. Nach einer engen Ansicht wird ein physischer Zwang gefordert.[77] Dieser tritt im Falle eines Cyberangriffs jedoch nicht unmittelbar ein.[78] Dem ist wiederum entgegenzuhalten, dass die Gewaltanwendung im Falle des Einsatzes toxischer Chemikalien zweifellos zu bejahen ist und damit ein entsprechender Fall bereits anerkannt ist.[79] Doch auch an einem weiteren Verständnis, das keinen physischen Zwang voraussetzt, bestehen erhebliche Zweifel. Bei neuartigen Waffen müsste immer der entsprechende Einzelfall geprüft werden. Zudem ist mit Blick auf das huVR entscheidend, welche Folgen durch den Einsatz von Waffen entstehen. Es zielt gerade auf die Eingrenzung von Gewalt und deren Auswirkungen im Rahmen militärischer Notwendigkeiten ab.[80] Dies zeigt sich insbes. daran, dass das huVR gerade generelle Verbote ausspricht, die Einzelfälle umfassen.[81] Im Ergebnis ist dem IGH zuzustimmen, dass es bei der Anwendung von Gewalt nicht auf die Art der Waffe ankommt.[82]

b) Target-based-Ansatz

Der *target-based*-Ansatz stellt dagegen auf das Ziel des Cyberangriffs ab.[83] Handelt es sich bei den Zielen um be-

---

61 *Herdegen* (Fn. 41), § 34 Rn. 16.

62 *Herdegen* (Fn. 41), § 34 Rn. 15.

63 Dazu *Benatar,* The Use of Cyber Force: Need for Legal Justification?, GoJIL 2009, 375 (381).

64 *Simma et al./Randelzhofer/Dörr,* UN-Ch, 3. Auflage (2012), Art. 2(4) Rn. 23 ff.

65 *Simma et al./Randelzhofer/Dörr* (Fn. 64), Art. 2(4) Rn. 21 f.

66 Diese Ansicht könnte, gerade im Hinblick auf die derzeitigen Sanktionsmaßnahmen der USA, erheblich ins Wanken geraten; vgl. dazu *Dittmar,* Angriffe auf Computernetzwerke – Ius ad bellum und ius in bello (2005), S. 70 ff. m. w. N. Aufgrund des Fokus dieses Beitrags wird jedoch auf eine Vertiefung verzichtet.

67 *Radziwill* (Fn. 10), S. 131; *Simma et al./Randelzhofer/Dörr* (Fn. 64), Art. 2(4) Rn. 16.

68 *Schulze* (Fn. 7), S. 98, der diese Fälle als »Grauzone« bezeichnet.

69 *v. Heinegg* (Fn. 18), § 55 Rn. 16; vgl. Art. 1 Abs. 1 UN-Ch und Art. 103 UN-Ch, woraus sich der Vorrang der UN-Ch ergibt.

70 *Weisbord* (Fn. 14) ColumJTransnatlL 2011, 82 (151).

71 *Radziwill* (Fn. 10), S. 132.

72 *Dornbusch* (Fn. 5), S. 115 f.

73 Vgl. *v. Heinegg* (Fn. 18), § 55 Rn. 18.

74 Vgl. insofern Art. 51 UN-Ch. wodurch ein qualitativer Unterschied deutlich wird; dazu auch *Schulze* (Fn. 7), S. 98.

75 *Kanuck,* Information Warfare: New Challenges for Public International Law, HarvIntLJ 1996, 272 (289).

76 *Miller,* Cyberattacks, the Laws of War, and the Crime of Aggression, ILSAQuart 2013, 21 (22).

77 *Hollis,* Why States Need an International Law for Information Operations, Lewis&ClarkLRev 2007, 1023 (1041).

78 *Dornbusch* (Fn. 5), S. 71.

79 *Schmitt,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, ColumJTransnatlL 1999, 885 (913); *Woltag,* Cyber Warfare, MPEPIL 2015, Rn. 2.

80 *Dornbusch* (Fn. 5), S. 72.

81 Ebenda.

82 IGH, Advisory Opinion, Legality of the Threat or Use of Nuclear Weapons, 8. 6. 1996, 1996 ICJRep 226, para. 39.

83 *Sharp,* Cyberspace and the Use of Force (1999), S. 129 f.; *Jensen,* Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, StanJIntL 2002, 207 (226 ff.).

sonders bedeutsame bzw. anfällige Teile der Infrastruktur des betroffenen Staates, soll schon allein deshalb eine Gewaltanwendung vorliegen.[84] Als solche sind insbes. auch die Militär- und Staatsverwaltung anzusehen.[85] Der Vorteil dieses Ansatzes liegt darin, dass er eine weitergehende Differenzierung hinsichtlich der Intensität vereinfacht. Dies ist jedoch auch zugleich die größte Schwäche. So beinhaltet dieser Ansatz einen erheblichen Spielraum hinsichtlich der Frage, welche Ziele als kritisch zu betrachten sind, und verlagert damit lediglich die Definitionsfrage.[86] Zudem sind schon geringfügigste Störungen umfasst, sobald ein entsprechendes Ziel betroffen ist.[87] Auch scheint dieser Ansatz letztlich doch auf den Effekt des Angriffs abzustellen und dabei die kritische Infrastruktur als maßgebliches Kriterium heranzuziehen.

c) Effect-based-Ansatz

All dies zeigt, dass es vielmehr auf die Auswirkungen ankommt, worauf der *effect-based-Ansatz* entscheidend abstellt. Innerhalb dieses Ansatzes gibt es eine Vielzahl an Ansätzen, unter welchen Voraussetzungen ein Effekt für die Annahme einer Gewaltanwendung ausreichen soll. So vertritt *Sharp,* dass bereits jeder *computer network attack* (CNA), der zerstörerischen Effekt auf die territoriale Integrität oder die politische Unabhängigkeit eines Staates hat, eine unrechtmäßige Gewaltanwendung darstellt.[88] Dieser sehr weitgehende Ansatz ist zweifelsohne näher zu spezifizieren. *Schmitt* hat dazu ein System von mittlerweile acht Faktoren entwickelt.[89] Dieser Ansatz sieht sich indes dem Einwand ausgesetzt, dass sich daran die weitere Frage der Zuordnung der einzelnen Faktoren in ihrer Bedeutung anschließt. Letztlich scheint dabei nur das Kriterium der *Schwere* des Angriffs wirklich bedeutsam.[90] Die Ungenauigkeit, die sich durch die Vielzahl von Faktoren ergibt, verdeutlicht *Silver,* indem er die beabsichtigten Auswirkungen verändert und dabei aufzeigt, dass es letztlich nur entscheidend sei, ob die Zerstörung von Sachwerten oder Verletzung von Leib und Leben die vorhersehbare Folge seien.[91] Die Kriterien erscheinen in ihrer Gänze für die Lösung des Problems wenig praktikabel. Dennoch vermag der *effect-based*-Ansatz seinem Grunde nach zu überzeugen. So sind unter einer *Gewaltanwendung* nicht nur ein direkter bewaffneter Angriff zu verstehen, sondern eben auch solche Maßnahmen, die einen ähnlichen Wirkungsgehalt in sich tragen.[92]

Gegenstand erheblicher Diskussion ist dabei wiederum die Frage, ob auch Angriffe, die lediglich die Funktionen beeinträchtigen, in ihrer Intensität physischen Objektbeschädigungen gleichgestellt werden können.[93] So lässt sich dem *Tallinn Manual* entnehmen, dass mehrheitlich befürwortet wird, dass die Beeinträchtigung der Funktionalität nur dann als Beschädigung des Objekts zu verstehen sei, wenn das betroffene Objekt oder Teile davon auch tatsächlich ausgetauscht werden müssen.[94] Dieses Verständnis begegnet Zweifeln.[95] Es scheint recht willkürlich, die Notwendigkeit einer physischen Reparatur zu fordern, wenn doch die Folgen durch den Funktionsausfall in gleicher Weise eintreten, obwohl sie durch eine technische Wiederherstellung beseitigt werden können.[96] Insbes. zeigt sich dies dadurch, dass die Cyberangriffe als Alternative zu einem traditionellen militärischen Angriff genutzt werden.[97] Der militärische Vorteil, also die Funktionslosigkeit der betroffenen militärischen Einheit, besteht in beiden Fällen gleichermaßen.[98] Es kann damit nicht darauf ankommen, ob die Wiederherstellung der Funktionsfähigkeit eines physischen oder technischen Wiederaufbaus bedarf.[99] Die zeitliche Begrenzung des Schadens aufgrund der Wiederherstellbarkeit stellt gerade eine Besonderheit von Cyberangriffen dar.[100] Begrenzend muss eine Funktionsbeeinträchtigung gefordert werden, die bei einem entsprechenden

84 *Jensen* (Fn. 83), StanJIntL 2002, 207 (226 f.); vgl. *Nguyen* (Fn. 21) CaliLRev 2013, 1079 (1119), *Radziwill* (Fn. 10), S. 138; Allg. zu kritischen Infrastrukturen: *Roscini* (Fn. 29), S. 55 ff.

85 Des Weiteren: »Wasser- und Lebensmittelversorgung, Gesundheit, Gefahrstoffanlagen, Energieversorgung, Transportwesen, Kommunikation, Finanz- und Bankenwesen«, *Dornbusch* (Fn. 5), S. 99; *Focarelli* (Fn. 32), S. 268 f.

86 *Handler,* The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, StanJIntL 48 (2012), 209 (228).

87 Ebenda.

88 *Sharp* (Fn. 83), 90 f.

89 »Severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy«, *Schmitt* (Fn. 79), ColumJTransnatlL 1999, 885 (914 f.); »responsibility«, *Schmitt,* Computer Network Attack: The Normative Software, YbIntHumL 2001, 53 (65), wurde in »military character« und »state involvement« aufgesplittet, sowie »presumptive legitimacy« durch »presumptive legality« ersetzt, *Schmitt et al.* (Fn. 28), S. 334, Rule 69, Rn. 9.

90 Silver, Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, ILS 2002, 73 (89, 91).

91 *Silver* (Fn. 90), ILS 2002, 73 (91).

92 So entschied der IGH, dass das Bewaffnen und Trainieren von Rebellen schon eine Gewaltanwendung i. S. v. Art. 2 Abs. 4 UN-Ch darstellen könne, IGH, Judgement, *Military and Paramilitary Activities in and against Nicaragua,* Merits, 27. 6. 1986, ICJRep 1986, 14, para. 228; Generell zum Problem der indirekten Gewaltanwendung vgl. *Simma et al./Randelzhofer/Dörr* (Fn. 64), Art. 2(4) Rn. 23–8.

93 Anm.: Dieser Abschnitt befand sich in der urspr. Arbeit i. R. d. Diskussion über die Definition und ist zum Zwecke der Anschaulichkeit hier angepasst worden.

94 *Schmitt et al.* (Fn. 28), S. 415, Rule 92, Rn. 10.

95 Dies zeigt sich auch im Vergleich der beiden Auflagen des *Tallinn Manuals,* dem sich ein Meinungswandel entnehmen lässt. War 2013 noch davon die Rede, dass ein *paar* Experten soweit gingen, vgl. *Schmitt et al.,* Tallinn Manual on the International Law Applicable to Cyber Operations (2013), S. 109, Rule 30, Rn. 11, sind es 2017 bereits *einige* Experten innerhalb der oben bezeichneten Mehrheit – und damit mehr als 2013 –, die eine Ausweitung auf eine technische Wiederherstellung befürworten, vgl. *Schmitt et al.* (Fn. 28), S. 415, Rule 92, Rn. 11.

96 *Barkham,* Information Warfare and International Law on the Use of Force, NYUJIntL&P 2001, 57 (92).

97 Vgl. Aussagen von US-Präsident *Donald Trump* (Fn. 4) mit zugehörigem Haupttext.

98 Vgl. *Radziwill* (Fn. 10), S. 63–66.

99 Vgl. *Dornbusch* (Fn. 5), S. 97 f.

100 *Nguyen* (Fn. 21) CaliLRev 2013, 1079 (1103).

kinetischen Angriff eine physische Reparatur notwendig machen würde und damit als erheblich zu bezeichnen ist.[101]

d) Effect-on-target-based-Ansatz

Die Ungenauigkeiten des *effect-based*-Ansatzes könnten durch eine Verbindung zu einem *effect-on-target-based*-Ansatz beseitigt werden und dadurch einheitlich physische Schäden sowie Funktionsbeeinträchtigungen erfassen. Letztlich sind beide darin enthaltenen Kriterien maßgeblich und längst in der Literatur vermengt.[102] So wird mehrheitlich entweder ein Angriff, der vergleichbar intensive Schäden verursacht, oder ein auf eine kritische Infrastruktur gerichteter, der kumulativ von einer gewissen Intensität ist, als Gewaltanwendung angesehen.[103] Durch das Zusammenspiel beider Ansätze mit den Kriterien der kritischen Infrastruktur *(target)* und der Schwere *(effect)* könnten insofern sowohl unmittelbare und mittelbare physische Schäden als auch nur auf die Funktionsunfähigkeit gerichtete Angriffe einheitlich bestimmt werden und dadurch der bestehenden Rechtsunsicherheit im Falle von Cyberangriffen begegnet werden.[104] Dieses Verständnis geht damit einher, dass Angriffe, die die staatliche Souveränität und insbes. solche Strukturen betreffen, die vom staatlichen Militär genutzt werden, auch bei geringerer Intensität eher als Gewaltanwendung im traditionellen Sinne angesehen werden.[105] Die Beschädigung oder Zerstörung von Daten und damit auch Computernetzwerksystemen stellt danach immer dann eine Gewaltanwendung i. S. d. Art. 2 IV UN-Charta dar, wenn sie sich gegen eine kritische Infrastruktur richtet und in ihrer Wirkung auf die Funktion als erheblich anzusehen ist.[106]

2. Cyberangriff als bewaffneter Angriff i. S. v. Art. 51 UN-Ch

Gem. Art. 51 UN-Ch besteht das Recht zur Selbstverteidigung unter der Voraussetzung, dass ein *bewaffneter Angriff* (»armed attack«) vorliegt. Die Anforderungen daran sind ungleich höher als i. R. v. Art. 2 IV UN-Ch.[107] Dabei ist zunächst festzustellen, dass es für die Voraussetzung des *bewaffneten* Angriffs nicht zwingend auf die Bestimmung der »Cyberwaffe« als Waffe im herkömmlichen Sinne ankommt, sondern vielmehr auf eine Vergleichbarkeit der Wirkungen.[108] So bedarf es einer massiveren und koordinierteren Gewaltanwendung gegen einen anderen Staat,[109] wobei auch eine Vielzahl kleinerer Angriffe einen bewaffneten Angriff darstellen können.[110] Ein Cyberangriff kann das Recht auf Selbstverteidigung auslösen, soweit dieser, nach *Ausmaß und Auswirkungen,* einen bewaffneten Angriff darstellt.[111] Dabei kommt es wiederum nicht auf die Waffe selbst an.[112] Im Mittelpunkt steht daher die Frage, ob ein Angriff ohne physische Schäden diese Schwelle überschreiten kann.[113] Das bloße Zerstören oder Beschädigen von Daten, das nur die Funktionsfähigkeit des Computersystems beeinträchtigt, solle dafür nicht reichen.[114] Dies vermag nach dem oben Gesagten nicht zu überzeugen. Datenbeschädigungen, die – wie im Fall *Stuxnet* –[115] physische Schäden hervorrufen, stellen bei entsprechendem Ausmaß einen bewaffneten Angriff dar, da sie mit Mitteln der Kriegsführung begangen werden und über einen bloßen Grenzzwischenfall hinausgehen.[116] Versteht man diese Voraussetzung als »Mehr« gegenüber der Gewaltanwendung, kann es wiederum keinen Unterschied machen, ob die Funktionsfähigkeit durch physische oder virtuelle Schäden erheblich eingeschränkt wird.[117] Beim jüngsten Angriff gegen den Iran war dies wohl nicht gegeben. Anders jedoch, wenn unter Umständen die gesamte Staatsverwaltung, Sicherheitssysteme oder die Elektrizitätsnetze betroffen sind und durch die Funktionsbeeinträchtigungen dieser Infrastrukturen zwar keine unmittelbaren Schäden, aber bspw. notstandsähnliche Zustände in der Zivilbevölkerung eintreten,[118] sodass auch diese als schwerwiegendste Gewaltanwendungen[119] bezeichnet werden können.[120] Unter Berücksichtigung dessen, dass einem angegriffenen Staat ein Selbstverteidigungsrecht gerade dann zustehen muss, wenn dieser im Rahmen seiner kritischen

---

101 Vgl. *Schmitt et al.* (Fn. 28), S. 415, Rule 92, Rn. 11.

102 *Focarelli* (Fn. 32), S. 269; *Dornbusch* (Fn. 5), S. 99 ff.

103 Vgl. *Dornbusch* (Fn. 5), S. 112, die innerhalb des *targeted-based*-Ansatzes eine Intensitätsschwelle fordert, wofür letztlich die Folgen heranzuziehen sind.

104 Vgl. *Roscini,* Cyberoperations and the Use of force (Fn. 32), S. 233, 245 ff.

105 *Dornbusch* (Fn. 5), S. 100.

106 So auch *Dornbusch* (Fn. 5), S. 111 f., 233; *Ziolkowski,* Stuxnet – Legal Considerations, HuV-I 2008, 202 (209); Ablehnend dagegen *Schulze* (Fn. 7), S. 95 f.

107 *Simma et al./Randelzhofer/Dörr* (Fn. 64), Art. 51 Rn. 6, 20 ff.; *Radziwill* (Fn. 10), S. 132; eine Gleichstellung der Begriffe, die aufgrund des unterschiedlichen Wortlauts kaum haltbar scheint, befürwortet dagegen *Ziolkowski, Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force, in: (Fn. 17), S. 299.

108 *v. Heinegg* (Fn. 18), § 56 Rn. 11; *Schmitt et al.* (Fn. 28), S. 340, Rule 71, Rn. 5; In dem hier behandelten Kontext wird die Verwendung der Cyber*mittel* jedoch regelmäßig als Cyber*waffe* zu verstehen sein (S. 452, Rule 103, Rn. 2); zur Frage, ob es sich um Waffen handelt, vgl. *Koloßa,* Is There Really a Need for a New "Digital Geneva Convention"?, HuV 2019, 37 (44 f.).

109 *Herdegen* (Fn. 41), § 34 Rn. 22.

110 *Simma et al./Randelzhofer/Dörr* (Fn. 64), UN-Ch, Art. 51 Rn. 21.

111 *Schmitt et al.* (Fn. 28), Rule 71, S. 339, mit Bezug auf *»scale and effect«,* IGH, *Nicaragua* (Fn. 92), para. 195.

112 IGH, *Nuclear weapons* (Fn. 82), para. 39.

113 *Focarelli* (Fn. 32), S. 256.

114 *Schmitt,* Cyber Operations and the Jud Ad Bellum Revisited, VillLRev 2011, 569 (589).

115 Dazu *Schmitt et al.* (Fn. 28), S. 342, Rule 71, Rn. 10.

116 *Schmitt et al.* (Fn. 28), S. 339, Rule 71, Rn. 11; *v. Heinegg* (Fn. 18), § 56 Rn. 7 f., 12.

117 Uneinig zeigt sich, wie auch im Falle der Gewaltanwendung, die Expertenkommission, *Schmitt et al.* (Fn. 28), S. 343, Rule 71, Rn. 13.

118 So auch *Bring,* The Use of Force under the UN-Charter – Modification and Reform through Practice or Consensus, in: Ebbesson et al. (Hrsg.), International Law and Changing Perceptions of Security – Liber Amicorum Said Mahmoudi (2014), S. 12; *Dittmar* (Fn. 66), S. 157 f.; *Dinstein,* Computer Network Attacks and Self Defense ILS 2002, 99 (105). Einen dahingehenden Ausblick in die Staatenpraxis wagt *Schmitt,* Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum, HarvNatlSecJ 2017, 239; kritisch: *Kittichaisaree* (Fn. 28), S. 171 f.

119 IGH, *Nicaragua* (Fn. 92), paras. 191 (»most grave forms of the use of force«).

120 Kritisch dagegen *Schmitt* (Fn. 118) HarvNatlSecJ 2017, 239 (266 f.).

Infrastrukturen angegriffen wird,[121] ist für einen *effect-on-target-based*-Ansatz zu plädieren, der das Ausmaß und die Auswirkungen berücksichtigt, aber auch die besonders sensiblen Infrastrukturen.[122] Dabei ist jedoch festzuhalten, dass es sich um einen Extremfall handeln muss, damit das Selbstverteidigungsrecht ausgelöst wird.[123]

3. Staatenverantwortlichkeit

Der Staat muss darüber hinaus für das begangene Unrecht verantwortlich sein, damit der angegriffene Staat gegen diesen sein Selbstverteidigungsrecht ausüben darf.[124] Verantwortlich ist ein Staat grds. nur für das Handeln eigener *de-facto-* oder *de-jure*-Staatsorgane.[125] Cyberangriffe werden jedoch häufig durch nichtstaatliche Akteure durchgeführt.[126] Gem. Art. 8 ILC-Artikel und Völkergewohnheitsrecht[127] ist das Verhalten von nicht-staatlichen Einheiten einem Staat ausnahmsweise zuzurechnen, wenn dieser eine *effektive Kontrolle* (»effective control«) über die Akteure ausübt.[128] Danach muss der Staat über jede spezifische Verletzungshandlung des nichtstaatlichen Akteurs die effektive Kontrolle ausüben.[129] Für einen solch engen Zurechnungsmaßstab spricht, dass der Staat grds. nur für sein Handeln verantwortlich sein soll.[130] Nach einem weitergehenden Ansatz des ICTY genügt dagegen bereits eine generelle *Gesamtkontrolle* (»overall control«) über die Koordinierung oder Planung eines militärischen Einsatzes einer nichtstaatlichen Gruppierung.[131] Dafür spricht, dass bei einer zu engen Zurechnungsschwelle in vielfältiger Weise eine Umgehungsmöglichkeit bestünde, die eine erhebliche Durchsetzungslücke durch fehlende Staatenverantwortlichkeit begründen würde.[132] Angesichts der steigenden Anzahl an Cyberangriffen scheint der *overall-control*-Ansatz zunächst vorzugswürdig, da die ohnehin schwierige Staatenverantwortung unter geringeren Anforderungen begründet werden kann.[133] Dieser Ansatz wird jedoch vielfach als zu weitgehend abgelehnt.[134] Folge wäre auch, dass Staaten deutlich einfacher und möglicherweise zu Unrecht verantwortlich gemacht werden können.[135] Mit Blick auf das sich auslösende Selbstverteidigungsrecht des angegriffenen Staates ist dies mit besonderer Skepsis zu betrachten.[136] Eine allgemeine Anerkennung der *Gesamtkontrolle* als Zurechnungsregel ist daher nicht sachgerecht.[137] Betrachtet man jedoch die aktuellen Entwicklungen neuartiger Kriegsführung, ist es zumindest *de lege ferenda* notwendig, dass die Zurechnungskriterien in realistischer Weise angepasst werden.[138] Einen Kompromiss könnte dabei eine Beweislastumkehr durch die Begründung einer *Gesamtkontrolle* hinsichtlich einer *effektiven Kontrolle* bieten.[139] Es bedarf folglich weiterhin der *effektiven Kontrolle.* Darüber hinaus kommt auch ein Selbstverteidigungsrecht gegenüber nichtstaatlichen Akteuren in Betracht, sofern diese eine gewisse Organisationsstruktur besitzen.[140]

IV. Ius in bello

Des Weiteren werden im Folgenden Cyberangriffe unter den Regelungen des *ius in bello* betrachtet, namentlich der Regelungen der Genfer Abkommen von 1949.[141]

1. Cyberangriff i. R. v. bewaffneten Konflikten (huVR)

Vorliegend wird aufgrund des Schwerpunkts des Aufsatzes und mit Blick darauf, dass bewaffnete Gruppen regelmäßig die nötigen Ressourcen nicht besitzen und mangels entsprechenden Wissens nicht staatlichen Militärstrukturen vergleichbar agieren,[142] nur der internationale bewaffnete Konflikt zwischen Staaten betrachtet.[143] Nach umstrittener Definition liegt ein bewaffneter Konflikt i. S. d. gemeinsamen Art. 2 der GK vor, wenn es einen Einsatz von Waffengewalt zwischen Staaten oder anhaltende bewaffnete Gewalt zwischen Regierungsbehörden und organisierten bewaffneten Gruppen oder zwischen solchen Gruppen innerhalb eines Staates gibt.[144]

---

121 *Kittichaisaree* (Fn. 28), S. 153, 166 ff.

122 Vgl. *Focarelli* (Fn. 32), S. 268 f.

123 Vgl. *Schmitt et al.* (Fn. 28), S. 341 ff., Rule 71, Rn. 7 ff.

124 *Herdegen* (Fn. 41), § 58 Rn. 1.

125 Art. 4 und 5 ILC-Artikel; *Dörr* (Fn. 18), § 30 Rn. 7 ff., 11 f.

126 *Schulze* (Fn. 7), S. 142.

127 *Schulze* (Fn. 7), S. 59.

128 *Herdegen* (Fn. 41), § 58 Rn. 6; IGH, *Bosnia and Herzegovina v. Serbia and Montenegro,* Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Merits, 2007 ICJRep, S. 43, para. 388 ff.; *Nicaragua* (Fn. 92), para. 115.

129 *Herdegen* (Fn. 41), § 58 Rn. 6; *Dörr* (Fn. 18), § 30 Rn. 19 f.; Nicht ausreichend insofern die Kontrolle der DRK über die Rebellentruppen, IGH, *Dem. Rep. Congo v. Uganda,* Armed Activities on the Territory of the Congo, 2005 ICJRep, S. 168; Ein leicht anderes Verständnis vertritt *Schulze* (Fn. 7), S. 61.

130 *Schulze* (Fn. 7), S. 139.

131 ICTY, *Prosecutor v. Tadić,* Appeals Chamber, Judgment, ICTY-94-1-A, 15. 7. 1999, paras. 117, 137.

132 *Dornbusch* (Fn. 5), S. 127.

133 *Shackelford,* State Responsibilty for Cyber Attacks: Competing Standards for a Growing Problem, in: Czosseck/Podins (Hrsg.), Conference on CyberConflict: Proceedings, CCD COE Publications, Tallinn, 2010, https://ccdcoe.org/uploads/2018/10/Shackelford-State-Responsibility-for-Cyber-Attacks-Competing-Standards-for-a-Growing-Problem.pdf, zuletzt aufgerufen am 13. 3. 2020, S. 197, 203 f.

134 IGH, *Genocide* (Fn. 128), para. 400.

135 *Schulze* (Fn. 7), S. 139.

136 Vgl. *Schulze* (Fn. 7), S. 150.

137 *Schmitt et al.* (Fn. 28), S. 96, Rule 17, Rn. 5 f.; *Schulze* (Fn. 7), S. 139 ff., der hervorhebt, dass auch bei der Entscheidung des ICTY nicht einzelne Privatpersonen zugerechnet wurden. A. A. *Dornbusch* (Fn. 5), S. 127 f.

138 Vgl. *Dornbusch* (Fn. 5), S. 127.

139 *Herdegen* (Fn. 41), § 58 Rn. 6; Ablehnend *Schulze* (Fn. 7), S. 151, der darüber hinaus eine Übertragung der »*safe-haven*«-Doktrin erwägt.

140 *Focarelli* (Fn. 32), S. 276 ff.; ausführlich dazu *Szabó,* Anticipatory Action in Self-Defence: Essence and Limits under International Law (2011), S. 203 ff.

141 Vgl. *v. Heinegg* (Fn. 18), § 60 Rn. 21 ff.

142 *Gill,* International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of 'Attack' under the Humanitarian Law of Armed Conflict, in: Tsagourias/Buchan (Fn. 32), S. 366, 371.

143 Es ist grds. zwischen einem internationalen – zwischen zwei Staaten – ausgeübten und einem nicht internationalen Konflikt zwischen Staat und nichtstaatlichen oder zwischen ausschließlich nichtstaatlichen organisierten bewaffneten Gruppen zu differenzieren, *v. Heinegg* (Fn. 18), § 61 Rn. 1.

144 *Dinniss* (Fn. 53), S. 118 ff.; vgl. dazu ICTY, *Prosecutor v. Tadić,* Appeals

a) Begründung eines internationalen bewaffneten Konflikts

Zu untersuchen ist zunächst, ob ein Cyberangriff überhaupt einen internationalen bewaffneten Konflikt begründen kann. Problematisch ist dies wiederum dahingehend, dass *bewaffnete Gewalt* gefordert ist.[145] Dies könnte deshalb zu verneinen sein, weil der Cyberangriff zumeist keine unmittelbaren physischen Schäden hervorrufen wird und damit mit traditionellen Mitteln der Kriegsführung nur bedingt vergleichbar ist.[146] Wie bereits dargelegt, kann ein solcher Angriff allerdings ähnlich schwere Schäden hervorrufen. Ein Konsens scheint mittlerweile insoweit zu bestehen, als dass ein Cyberangriff einen bewaffneten Konflikt auslösen kann, wenn er kinetische Wirkungen entfaltet, die den Auswirkungen des Einsatzes traditioneller Waffengewalt gleichkommen.[147] Gemeint ist damit i. d. R. ein physischer Schaden, der eine Reparatur notwendig macht.[148] Dabei wird insbes. darauf verwiesen, dass es nicht darauf ankommen könne, ob ein traditionelles oder nicht traditionelles Mittel eingesetzt werde, wenn es letztlich die gleichen bzw. vergleichbare Konsequenzen hat.[149] In der Folge wären bloße, die Funktionsfähigkeit beeinträchtigende Datenbeschädigungen nicht umfasst.[150] Stellt man, wie oben dargestellt, konsequent auf die Wirkungen ab, kann es nicht entscheidend sein, ob auch eine bloß »virtuelle Reparatur« möglich ist, der Angriff aber nicht weniger intensiv ist.[151] Dafür spricht, dass es gerade Sinn und Zweck des huVRs ist, einen umfassenden Schutz der Zivilbevölkerung vor den Folgen bewaffneter Konflikte zu gewährleisten.[152] Dies erklärt auch das Fehlen einer expliziten Gewaltschwelle für das Bestehen eines internationalen bewaffneten Konflikts, um eine etwaige Schutzlücke zu vermeiden.[153] So scheinen auch die jüngsten Aktivitäten zu bestätigen, dass es Ziel der attackierenden Staaten ist, Ungewissheiten auszunutzen, um kritische Infrastrukturen anzugreifen, ohne dadurch einen eindeutigen bewaffneten Konflikt zu begründen.[154] Es überzeugt daher, eine bloße Funktionsstörung grds. ausreichen zu lassen.[155] Diese muss jedoch von gewisser Intensität hinsichtlich der Dauer und des Ausmaßes und damit im Ergebnis mit traditioneller bewaffneter Gewalt vergleichbar sein.[156] Mit Blick auf die derzeitigen Aktivitäten ist diese Intensität indes eher fernliegend, da Cyberangriffe vielmehr vereinzelt und in Kombination mit traditionellen Waffen angewendet werden.

b) Angriff i. S. v. Art. 49 I GK ZP I

Relevant wird dies beispielsweise im Falle von Angriffen i. S. v. Art. 49 I GK ZP I. Nach der dortigen Legaldefinition ist eine offensive oder defensive Gewaltanwendung gegen den Gegner als Angriff zu verstehen. Fraglich ist daher wiederum, wie eine Gewaltanwendung zu definieren ist und ob Cyberangriffe darunterfallen können.[157] Insofern kann zunächst festgehalten werden, dass die Gewaltanwendung, die zur Begründung eines bewaffneten Konflikts führt, auch einen Angriff i. S. d. Art. 49 I GK ZP I darstellt.[158] Dagegen können die Begriffe nicht grds. gleichgestellt werden.[159] Eine Gewaltanwendung, die zugleich als Angriff innerhalb eines bewaffneten Konflikts anzusehen ist, muss nach dem dargelegten Verständnis eine Intensitätsschwelle überschreiten, die aber notwendigerweise geringere Anforderungen als der bewaffnete Konflikt selbst hat, um den Schutz der Zivilbevölkerung gewährleisten zu können.[160] Auch ein Angriff, der das anvisierte Objekt physisch nicht verletzt, aber in der Funktionalität zumindest vorübergehend beeinträchtigt, kann einen militärisch relevanten Angriff darstellen.[161] Dementsprechend muss eine solche Operation in diesem Falle erst recht als Gewaltanwendung und damit als Angriff i. S. v. Art. 49 I ZP I GK zu betrachten sein.[162]

c) Konfliktparteien

Im bewaffneten Konflikt ist es weitgehend anerkannt, dass für die Zurechnung eines Akteurs zu einem Staat bzw. einer bewaffneten Gruppe der Nachweis einer *Gesamtkontrolle* genügt.[163] Die Zurechnung wird daher deutlich weniger problematisch sein.[164]

2. Prinzipien des humanitären Völkerrechts

Innerhalb des bewaffneten Konflikts sind darüber hinaus gewisse Grundprinzipien des huVRs zu berücksichtigen,

Chamber Decision, ICTY-94-1-AR, 2.10.1995, para. 70; ICC, Prosecutor v. Lubanga, PTC I Decision, ICC-01/04-01/06, 29. Jan. 2007, para. 209; *Herdegen* (Fn. 41), § 56 Rn. 5.

145 *Droege,* Get off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, IRRC 2012, 533 (545).

146 *Dornbusch* (Fn. 5), S. 88 ff.

147 *IKRK,* Commentary GC I, 2016, Art. 2 Rn. 255; *Schmitt et al.* (Fn. 28), S. 381, Rule 82, Rn. 4.

148 Vgl. *Dornbusch* (Fn. 5), S. 97.

149 *IKRK* (Fn. 147), Art. 2 Rn. 255; *v. Heinegg* (Fn. 18), § 61 Rn. 8.

150 Anders wäre dies nur, wenn man mit *Todd,* Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, AFLRev 2009, 65 (81 ff.), und *Barkham* (Fn. 96), NYUJIntL&P 2001, 88, Daten als Objekte betrachten würde. Dies überzeugt mit Blick auf den oben vertretenen *effect-based*-Ansatz nicht. Es erscheint sachgerecht, die Verschiedenheit der Daten zu physischen Objekten zu begreifen und auf eine Vergleichbarkeit der Konsequenzen zu verweisen; vgl. *Dornbusch* (Fn. 5), S. 94 ff. Offengelassen *IKRK* (Fn. 147), Art. 2 Rn. 256.

151 *Schmitt et al.* (Fn. 28), S. 417, Rule 92, Rn. 10.

152 Vgl. *v. Heinegg* (Fn. 18), § 60 Rn. 2; *Droege* (Fn. 145), IRRC 2012, 533 (547).

153 *Droege* (Fn. 145), IRRC 2012, 533 (547).

154 Vgl. *Droege* (Fn. 145), IRRC 2012, 533 (547).

155 *Dornbusch* (Fn. 5), S. 111 f.

156 *Chaumette,* International Criminal Responsibility of Individuals in Case of Cyberattacks, ICLRev 2018, 1 (13 f.).

157 Vgl. *Dornbusch* (Fn. 5), S. 139.

158 *Dornbusch* (Fn. 5), S. 140 f.

159 *Dornbusch* (Fn. 5), S. 140 m. w. N. in Fn. 548.

160 *Lubell,* Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?, ILS 2013, 252 (271 f.).

161 Vgl. *Droege* (Fn. 145), IRRC 2012, 533 (559).

162 *Droege* (Fn. 145), IRRC 2012, 533 (559); *Dornbusch* (Fn. 5), S. 141; vgl. *Gill* (Fn. 142), in: (Fn. 32), S. 375 f., der einen Vergleich zu Chemiewaffen zieht; kritisch dagegen *Schmitt et al.* (Fn. 28), S. 415, Rule 92, Rn. 11, vgl. auch oben unter »B«.

163 *Schmitt et al.* (Fn. 28), S. 380, Rule 82, Rn. 2 ff.

164 Dazu s. o. S. 12 f.

die sich im Hinblick auf Cyberangriffe als besonders problematisch herausstellen. Ausgewählte werden im Folgenden kurz beleuchtet.

a) Unterscheidungsgrundsatz

Gemäß dem in Art. 48 I GK ZP I niedergeschriebenen[165] Unterscheidungsgrundsatz sind die Konfliktparteien verpflichtet, »jederzeit zwischen der Zivilbevölkerung und Kombattanten sowie zwischen zivilen Objekten und militärischen Zielen« zu unterscheiden.[166] Die Verbindung zwischen militärisch und zivil genutzten Computernetzwerken (»dual-use«) im Falle von Cyberangriffen begründet insoweit die erste Problematik.[167] Auch hier lässt sich wiederum auf den zu Beginn genannten Beispielsfall *Stuxnet* verweisen. Der Wurm traf nach seiner Setzung nicht nur die staatlichen Computersysteme des Atomprojekts, sondern verteilte sich auch auf zivile.[168] Dabei blieb der Wurm jedoch unerkannt und auch ohne Wirkung, da die Wirkung nur bei den entsprechenden staatlichen Systemen eintreten konnte.[169] Umstritten ist nun, ob ein Angriff, der auf ein militärisches Netzwerk gerichtet ist und nur als Nebeneffekt auch ein ziviles trifft, als Verstoß gegen den Unterscheidungsgrundsatz anzusehen ist.[170] Die Ansicht, dass immer automatisch ein Verstoß vorliegt[171], ist mit Blick auf die daraus entstehende fast grundsätzliche Verletzung des huVRs schwer haltbar. Andererseits könnte eine zu weite Auslegung dazu führen, dass der gesamte zivile Cyberraum zu einem rechtmäßigen militärischen Ziel würde.[172] Dies ist jedoch nur bedingt vorstellbar. Vielmehr wird sich ein Angriff regelmäßig gegen ein Computernetzwerk richten können, das nur Teil des Gesamtsystems ist und daher einzeln betrachtet werden kann.[173] Insofern ist dem *Tallinn Manual* zuzustimmen, dass es zur Erfüllung des Grundsatzes nur darauf ankommen kann, ob ein militärisches Ziel getroffen werden soll.[174] Eine Berücksichtigung der möglicherweise auch betroffenen zivilen Objekte findet dann i. R. d. Prüfung der Verhältnismäßigkeit statt.[175] Daran anschließend stellt sich die Frage, ob virtuelle Daten auch als zivile Objekte[176] verstanden werden können. Mit Blick auf den Wortsinn ist eine solche Gleichstellung mit physischen Objekten abzulehnen.[177] Vielmehr ist konsequenterweise auf den Funktionsverlust und die Vergleichbarkeit mit einem Objektschaden abzustellen.[178] Die hier betrachteten Angriffe müssen sich daher am Unterscheidungsgrundsatz messen lassen.

b) Verhältnismäßigkeitsgrundsatz

Zunächst ist festzuhalten, dass der Verhältnismäßigkeitsgrundsatz an die erwarteten kollateralen zivilen Opfer, Verletzungen, Schäden und Zerstörungen anknüpft.[179] Insofern wird bestätigt, dass Cyberoperationen, die keinen physischen Effekt erwarten lassen, diesem Grundsatz nicht unterfallen.[180] Bei der Gleichstellung hinsichtlich der Funktionsfähigkeit ist jedoch auf den Effekt am Objekt abzustellen.[181] Die Verhältnismäßigkeit aufgrund der Spezialität des Angriffs und der damit zusammenhängenden geringeren Gefahr von Kollateralschäden wird dahingehend jedoch i. d. R. eingehalten werden.[182] Überdies ist dem Ansatz zuzustimmen, der die Reversibilität im Falle der Datenbeschädigungen positiv berücksichtigt.[183]

V. Zwischenfazit

Die Ausführungen zeigen auf, dass eine völkerrechtliche Regulierung schon aus Gründen der Rechtsklarheit zu begrüßen wäre.[184] Die Entwicklungen in der Literatur und teilweise in der Staatenpraxis lassen jedoch erahnen, dass eine solche nicht zwingend notwendig ist.[185] Die Ansätze, die versuchen Cyberangriffe unter bestehende Regulierungen zu fassen, scheinen sich dahingehend immer mehr zu konkretisieren und können durch Verhaltensregeln (»soft law«) weitergehend entsprechend gesteuert werden.[186]

D. Pönalisierung

Abschließend ist zu klären, ob das Durchführen von Cyberangriffen völkerstrafrechtlich zu pönalisieren ist. Im VStR kommt es zu einer Kombination aus strafrechtlicher, individueller Verantwortlichkeit und Grundsätzen des Völkerrechts.[187] In diesem Zusammenhang umfasst die Pönalisierung auch die Sanktionierung der Verletzung von Völkerrechtsgütern in individueller Form.[188] Bei der Legitimation der Pönalisierung, und damit auch hinsichtlich

165 Der Unterscheidungsgrundsatz gilt darüber hinaus auch gewohnheitsrechtlich im nichtinternationalen Konflikt, vgl. *Rowe,* Distinctive Ethical Challenges of Cyberweapons, in: Tsagourias/Buchan (Fn. 32), S. 310.

166 *v. Heinegg* (Fn. 18), § 62 Rn. 8.

167 *Chaumette* (Fn. 156), ICLRev 2018, 1 (15 f.).

168 *Gill* (Fn. 142), S. 376 f.

169 *Gill* (Fn. 142), S. 376 f.

170 *Chaumette* (Fn. 156), ICLRev 2018, 1 (15 f.).

171 *IKRK,* Report 31IC/11/5.1.2, 2011, https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf, zuletzt abgerufen am 13. 3. 2020, S. 36 f.

172 *Geiß/Lahmann,* Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space, IsrLRev 2012, 381 (385 f.); *Droege* (Fn. 145), IRRC 2012, 533 (565).

173 *Schmitt et al.* (Fn. 28), S. 446, Rule 101, Rn. 6.

174 *Schmitt et al.* (Fn. 28), S. 445, Rule 101, Rn. 1 ff.

175 Vgl. *Droege* (Fn. 145), IRRC 2012, 533 (571).

176 Vgl. Art. 52 IStGH-Statut.

177 *Dornbusch* (Fn. 5), S. 95. Für eine Gleichstellung dagegen *Ambos,* International Criminal Responsibility in Cyberspace, in: Tsagourias/Buchan (Fn. 32), S. 118, 131.

178 *Dornbusch* (Fn. 5), S. 96 ff; s. a. oben S. 9 f.

179 *Gill* (Fn. 142), S. 375.

180 *Gill* (Fn. 142), S. 375.

181 So auch *Dornbusch* (Fn. 5), S. 180.

182 Vgl. *Gill* (Fn. 142), S. 377.

183 Vgl. *Dornbusch* (Fn. 5), S. 180 f.

184 So zeigt bereits die Resolution 53/70 der UN-Generalversammlung, dass die Gefahr durchaus früh erkannt wurde. Von einer Kodifikation ist man dagegen noch weit entfernt.

185 So auch *Koloßa* (Fn. 108), HuV 2019, 37 (51 ff.); *Schulze* (Fn. 7), S. 190, der i. E. jedoch eine Kodifizierung befürwortet.

186 Zur Wirkung *Dörr* (Fn. 18), § 21 Rn. 9.

187 *Frau* (Fn. 18), § 35 Rn. 2; *Ambos,* Internationales Strafrecht, 5. Auflage (2018), § 5 Rn. 1.

188 *Ambos,* Treatise on International Criminal Law, Vol. 1 (2013), S. 65 f.

der Frage der Strafwürdigkeit,[189] kommt es maßgeblich auf die Strafzwecke an. Neben solchen, die aus den nationalen Rechtsordnungen übernommen wurden,[190] sind dies vor allem auch die Förderung eines dauerhaften Weltfriedens, die nationale Aussöhnung oder die Schaffung einer unparteiischen und unbestrittenen Geschichtsaufzeichnung.[191] Der Präambel des IStGH-Statuts lässt sich entnehmen, dass »die schwersten Verbrechen, welche die internationale Gemeinschaft als Ganzes berühren«, verfolgt werden sollen. Es bedarf also einer »internationalen Betroffenheit« der Weltgemeinschaft.[192] Zu klären ist damit, ob Cyberangriffe diese Schwelle überschreiten. Zur Beantwortung dieser Frage kann der *gravity*-Test herangezogen werden, den der IStGH verwendet, um festzustellen, ob ein Fall zugelassen wird.[193] Maßgeblich ist dahingehend die rechtliche und relative Schwere des Einzelfalles, die auch in vielen Artikeln des IStGH-Statuts niedergelegt ist.[194] Nach den Kriterien »scale, nature, manner of commission, impact«[195] haben Cyberangriffe aufgrund ihrer Auswirkungen und damit zusammenhängenden Außenwirkung grds. das Potenzial, die notwendige Schwere für eine individuelle völkerstrafrechtliche Pönalisierung zu erreichen.[196] Auch die Straftatbestände nach dem VStR (vgl. Art. 5 IStGH-Statut) könnten Cyberangriffe bereits umfassen, sodass besonders schwere Taten bereits pönalisiert sind.

I. Verbrechen i. S. d. Völkerstrafrechts

Cyberangriffe müssten zunächst der Jurisdiktionsgewalt des IStGH unterfallen.[197] Trotz einiger Besonderheiten der Cyberangriffe erscheint durch eine erweiterte Auslegung eine Zuständigkeitslücke dahingehend nicht zu bestehen.[198] Aufgrund des betrachteten Rechtsrahmens und des Umfangs des Beitrags wird im Folgenden auf das Verbrechen der Aggression gem. Art. 8*bis* IStGH-Statut und auf Kriegsverbrechen gem. Art. 8 IStGH-Statut eingegangen.[199]

1. Kriegsverbrechen gem. Art. 8 IStGH Statut

Zunächst wird dabei die Strafbarkeit wegen Kriegsverbrechen gem. Art. 8 IStGH-Statut betrachtet. Diese liegt vor, wenn ein Verstoß gegen das huVR vorliegt, der unmittelbar eine völkerrechtliche Strafbarkeit i. S. d. Art. 8 IStGH-Statut begründet.[200] Nach dem oben Dargelegten findet das huVR auch i. R. d. Cyberkriegsführung Anwendung. Die oben aufgeführten erheblichen Komplikationen hinsichtlich des Unterscheidungsgrundsatzes zeigen auf, dass regelmäßig zumindest objektiv ein Verbrechen gem. Art. 8 II b) IStGH-Statut wegen eines Angriffs auf Zivilisten oder ziviler Objekte vorliegen könnte.[201] Dies gilt sowohl für Cyberangriffe, die einen kinetischen Schaden verursachen, als auch für solche, die nur die Funktionsfähigkeit beeinträchtigen.[202] Eine Verwirklichung von Art. 8 II a) IStGH-Statut wegen einer schweren Verletzung der GK durch Cyberangriffe ist ebenfalls im Grundsatz möglich.[203]

2. Verbrechen der Aggression gem. Art. 8bis IStGH-Statut

Das Verbrechen der Aggression liegt dann vor, wenn eine individuell verantwortliche Person i. S. d. Art. 8*bis* I IStGH-Statut eine Angriffshandlung i. S. d. Abs. 2 in der in Abs. 1 geforderten Form begeht.

a) Individuelle Verantwortlichkeit (»leadership clause«)

Zunächst ist bereits problematisch, dass der Cyberangriff regelmäßig von nichtstaatlichen Akteuren durchgeführt wird, Art. 8*bis* jedoch deren Verhalten nicht umfasst.[204] Der Akt der Aggression muss »durch eine Person, die tatsächlich in der Lage ist, das politische oder militärische Handeln eines Staates zu kontrollieren oder zu lenken,«[205] begangen werden. Entgegen dem Wortlaut kann dies auch eine Personengruppe sein, die insgesamt die Voraussetzungen erfüllt.[206] Schon nach dem Wortlaut kann daher auch ein Angriff eines nicht-staatlichen Akteurs einem Staat zugerechnet werden und zur individuellen Verantwortlichkeit einer Person führen, soweit diese Person in der Position ist, effektive Kontrolle auszuüben.[207] Richtigerweise kann die strafrechtliche Verantwortung eines Anführers nicht von seinen Kenntnissen über die technischen Abläufe abhängen.[208] Vielmehr muss es genügen, dass er den Angriff generell anordnet.[209]

189 So auch *Werkmeister,* Straftheorien im Völkerstrafrecht (2015), S. 50.
190 »Resozialisierung, Vergeltung, Sühne, Spezial- und Generalprävention«, *Frau* (Fn. 18), § 35 Rn. 4; vgl. auch *Guilfoile,* International Criminal Law (2016), S. 87; kritisch dagegen *Ambos* (Fn. 187), § 5 Rn. 4.
191 *Guilfoile* (Fn. 190), S. 87.
192 *Gierhake,* Zur Legitimation des Völkerstrafrechts, ZIS 2008, 354 (358).
193 *Roscini,* Gravity in the Statute of the International Criminal Court and Cyber Conduct that constitutes, instigates or Facilitates International, CLF 2019, 1 (2, 8); vgl. auch IStGH, Situation in the DRC, Pre-Trial Chamber I, Decision on the Prosecutor's Application for Warrants of Arrest, ICC-01/04-01/06, 10. Feb. 2006, para. 41.
194 Ebenda (2).
195 Ebenda (14, 18, 19, 21).
196 Ebenda (25).
197 Vgl. insbes. Art. 12 II a), b) und 13 b) IStGH Statut.
198 Ausführlich *Chaumette* (Fn. 156), ICLRev 2018, 1 (23).
199 Hinsichtlich des Genozidverbrechens gem. Art. 6 IStGH-Statut und des Verbrechens gegen die Menschlichkeit gem. Art. 7 IStGH-Statut sei verwiesen auf: *Chaumette* (Fn. 156), ICLRev 2018, 1 (9 f., 20 ff.); *Roscini* (Fn. 193), CLF 2019, 1 (3 ff.).
200 *Ambos* (Fn. 187), § 7 Rn. 229.
201 Vgl. *Chaumette* (Fn. 156), ICLRev 2018, 1 (15 f.); hinsichtlich der Kenntlichmachung im bewaffneten Konflikt vgl. *Schmitt et al.* (Fn. 28), S. 496 ff., Rules 124–127.
202 *Chaumette* (Fn. 156), ICLRev 2018, 1 (15 f.).
203 *Chaumette* (Fn. 156), ICLRev 2018, 1 (14); *Roscini* (Fn. 193), CLF 2019, 1 (3).
204 *Ambos,* Individual Criminal Responsibility for Cyber Aggression, JCo&SL 2016, 495 (503).
205 Art. 8*bis* Abs. 1 i. V. m. Art. 25 Abs. 3*bis* IStGH-Statut.
206 Triffterer/Ambos/*Zimmermann/Freiburg,* ICC Commentary, 3. Auflage (2016), Art. 8*bis* Rn. 35.
207 Triffterer/Ambos/*Zimmermann/Freiburg* (Fn. 206), Art. 8*bis* Rn. 92.
208 *Ambos* (Fn. 204), JCo&SL 2016, 495 (503 f.).
209 *Ambos* (Fn. 204), JCo&SL 2016, 495 (503 f.).

b) Schwellenklausel (»threshold clause«)

Darüber hinaus müsste die Schwellenklausel i. S. v. Art. 8*bis* I IStGH-Statut erfüllt sein, wonach die Handlung »ihrer Art, ihrer Schwere und ihrem Umfang nach, eine offenkundige Verletzung der Charta der Vereinten Nationen« darstellen muss.[210] Nach dem oben Dargestellten ist eine nach »Art, Schwere und Umfang«[211] offenkundige Verletzung der UN-Charta durch datenbeschädigende Cyberangriffe theoretisch denkbar,[212] praktisch dagegen jedoch kaum vorstellbar. Unterstrichen wird dies durch die zweite Auslegungshilfe, wonach es sich bei der Aggression um »the most serious and dangerous form of the illegal use of force« handeln muss.[213] Dass ein Cyberangriff diese Schwelle tatsächlich erreicht, ist derzeit, insbes. bei lediglich datenbeschädigenden Operationen, nicht zu erwarten.[214]

c) Handlungen i. S. v. Art. 8bis II IStGH-Statut

Ein Cyberangriff könnte als eine der in Art. 8*bis* II IStGH-Statut niedergelegten Handlungsalternativen anzusehen sein. Dafür ist zunächst festzustellen, ob die dortige Aufführung abschließend ist. Für ein solches Verständnis zeigt sich *Miller* offen. Dafür sprechen der nicht eindeutige Wortlaut und die *travaux preparatoires.*[215] Gerade die von *Miller* aufgeführten, nicht umgesetzten Erweiterungen lit. h) und i)[216] zeigen doch, dass den Vertragsstaaten eine mögliche Regelungslücke durchaus bewusst war, und ein Konsens dahingehend gerade nicht zustande kam. Und selbst wenn man davon ausginge, dass die Aufzählung in den Verhandlungen als nicht abschließend angesehen wurde, muss man bei dem derzeitigen Vertragstext festhalten, dass eine Erweiterung, ebenso wie eine Analogie,[217] mit dem Grundsatz *nullum crimen sine lege* (Art. 22 IStGH Statut) unvereinbar ist.[218] Die Auflistung ist daher als abschließend zu betrachten.[219] Dagegen könnte der Cyberangriff jedoch als »Einsatz von *Waffen* jeder Art durch einen Staat gegen das Hoheitsgebiet eines anderen Staates«[220] oder »Angriff durch die Streitkräfte eines Staates« i. S. v. lit. d) angesehen werden.[221] Art. 8*bis* II IStGH-Statut setzt jedoch zunächst wiederum Waffengewalt voraus. Dieser Begriff ist, insbes. nach den *travaux preparatoires,* von seinem Grundverständnis deutlich enger als derjenige der UN-Ch und umfasst insofern zunächst nur traditionelle, kinetische Schäden verursachende Waffen.[222] Nach dem bereits festgestellten, mittlerweile weit anerkannten Verständnis, wonach auch ein Cyberangriff einen militärischen Akt darstellen kann, kann auch eine entsprechende Auslegung nicht ausgeschlossen werden und ist mit dem Legalitätsprinzip vereinbar.[223] Ebenso verhält es sich i. R. v. lit. b) und d). Nach dem hier zugrunde gelegten Verständnis der Angriffe durch »Cyberwaffen«[224] und entsprechendem Abstellen auf die Folgen, die sich territorial sowohl hinsichtlich physischer Folgen als auch Funktionsbeeinträchtigungen auswirken, überzeugt es, Cyberangriffe auch unter Berücksichtigung der Wortlautgrenze als Waffen i. S. v. lit. b) und als Angriff i. S. v. lit. d) einzuordnen.[225] Ein Cyberangriff kann folglich ein Aggressionsverbrechen darstellen.

II. Verantwortlichkeit und Beweisbarkeit

Auch im Rahmen der strafrechtlichen Verantwortlichkeit und der entsprechenden Beweisführung ist die Anonymität des Internets eine erhebliche Herausforderung.[226] Eine Zurückverfolgung bis zum Hacker selbst oder der Begründung einer Vorgesetztenverantwortlichkeit[227] ist allerdings nicht grds. ausgeschlossen.[228] Insofern bedarf es eines Abkommens, das eine Zurückverfolgung vereinfacht und die Staaten zu einer Zusammenarbeit in diesen Fällen verpflichtet.[229]

III. Zwischenfazit

Auch hinsichtlich der Pönalisierung von Cyberangriffen greifen die bestehenden völkerstrafrechtrechtlichen Regelungen und es bedarf insofern nicht notwendigerweise einer gesonderten Strafbarkeit im IStGH-Statut.[230] Was das Verständnis des Cyberangriffs als neuartige Waffe im huVR und VStR angeht, ergibt sich ebenfalls kein besonderes, über die im IStGH-Statut geregelten Strafbarkeiten hinausgehendes Pönalisierungsbedürfnis. So zeigt auch der eingangs aufgeführte Cyberangriff der USA, dass dieser zwar als Gewaltanwendung i. S. d. Art. 2 IV UN-Ch einzuordnen ist, indes nicht die Schwere besitzt, um eine individuelle Völkerstraftat darzustellen.

---

210 *Ambos* (Fn. 187), § 7 Rn. 265.

211 *Satzger,* Internationales und europäisches Strafrecht, 8. Auflage (2018), § 16 Rn. 83.

212 Generell zum zur Befürwortung der Strafbarkeit wegen der Verletzung der UN-Ch, *Weisbord* (Fn. 14) ColumJTransnatlL 2011, 82 (155 f.).

213 Res. RC/Res.6, vom 16. 6. 2010, abgedruckt in *Ambos,* Das Verbrechen der Aggression nach Kampala, ZIS 2010, 649 (651).

214 So auch *Chaumette* (Fn. 156), ICLRev 2018, 1 (9); *Radziwill* (Fn. 10), S. 170; *Ambos* (Fn. 177), S. 141.

215 *Miller,* The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression, SCalInterdiscLJ 2014, 217 (231 f.).

216 Ebenda (231).

217 *Weisbord* (Fn. 14), ColumJTransnatlL 2011, 82 (154 f.); befürwortet wiederum von *Miller* (Fn. 215), SCalInterdiscLJ 2014, 217 (233 ff.).

218 *Ambos* (Fn. 177), S. 140.

219 *Satzger* (Fn. 211), § 16 Rn. 83; *Ambos* (Fn. 213), ZIS 2010, 649 (657); a. A. Triffterer/Ambos/*Zimmermann/Freiburg* (Fn. 206), Art. 8*bis* Rn. 158; *Miller* (Fn. 215), SCalInterdiscLJ 2014, 217 (231); Gillet, The Anatomy of an International Crime: Aggression at the International Criminal Court, ICLRev 2013, 829 (845).

220 Triffterer/Ambos/*Zimmermann/Freiburg* (Fn. 206), Art. 8*bis* Rn. 158.

221 *Ambos* (Fn. 204), JCo&SL 2016, 495 (495 f.).

222 *Gillet* (Fn. 219), ICLRev 2013, 829 (838).

223 *Ambos* (Fn. 177), S. 138 f.

224 *Boothby* (Fn. 20), S. 176 ff.; *Schmitt et al.* (Fn. 28), S. 452, Rule 103.

225 Vgl. *Chaumette,* ICLRev 18 (2018), 1 (8 f.); Triffterer/*Ambos/Zimmermann/Freiburg* (Fn. 206), Art. 8*bis* Rn. 158; *Ambos* (Fn. 177), S. 140.

226 *Chaumette* (Fn. 156), ICLRev 2018, 1 (24 ff.).

227 Dazu *Schmitt et al.* (Fn. 28), S. 396, Rule 85.

228 *Chaumette* (Fn. 156), ICLRev 2018, 1 (26).

229 Ansätze bietet *Schulze* (Fn. 7), S. 205 ff.

230 *Roscini* (Fn. 193), CLF 2019, 1 (6).

E. Fazit

Aufgrund des Bestehens erheblicher Interessenskonflikte ist nicht von einem *politischen* Konsens hinsichtlich einer die Cyberkriegsführung regelnden völkerrechtlichen Übereinkunft auszugehen. Dies kann als Ergebnis dieses Beitrags jedoch auch nicht als zwingend notwendig bewertet werden.[231] So kann bereits durch eine klare Definition und einheitliche Auslegung hinsichtlich des bestehenden internationalen Rechts eine klare Linie gefunden werden, die dazu führt, dass durch eine einheitliche Staatenpraxis[232] dem Einsatz von Cyberangriffen klare Grenzen aufgezeigt werden und insofern die von diesen ausgehende Gefahr der Ausnutzung von Rechtsunsicherheiten eingedämmt werden kann.[233] Insgesamt zeichnet sich eine klare Tendenz dahingehend ab, Operationen im Cyberraum nicht mehr als rein virtuell zu betrachten, sondern vielmehr im Zusammenhang mit ihrer physischen Herkunft und den entsprechenden Auswirkungen.[234] Dies ist für die hier betrachteten, auf mittelbare physische Schäden oder Funktionsbeeinträchtigungen gerichteten militärischen Operationen sachgerecht. Anders ließe sich dies hinsichtlich auf Informationsgewinnung oder psychologische Beeinflussung gerichtete Maßnahmen bewerten.[235] Probleme zeigen sich endlich in der Zurückverfolgung von Handlungen im Cyberraum. Hier ist wiederum ein Handlungsbedarf zu konstatieren, der sich jedoch nicht durch die Regulierung von Cyberangriffen selbst, sondern primär durch zu schaffende Regelungen, Informationspflichten oder Beweishilfe betreffend, erschöpft.[236]

231 So auch *Dinniss* (Fn. 53), S. 28.

232 *Radziwill* (Fn. 10), S. 101.

233 Vgl. *Miller* (Fn. 215), SCalInterdiscLJ 2014, 217 (257), der die Bedeutung des *Tallinn Manuals* hervorhebt.

234 *Radziwill* (Fn. 10), 101 ff.

235 *Radziwill* (Fn. 10), S. 102 ff.

236 Vgl. *Beucher/Utzerath,* Cybersicherheit – Nationale und internationale Regulierungsinitiativen Folgen für die IT-Compliance und die Haftungsmaßstäbe, MMR 2013, 362.