Androhung und Anwendung von *Gewalt* und *bewaffneter Angriff* – zwei Typusbegriffe der völkerrechtlichen Friedenssicherung vor den Herausforderungen des Cyberwars

Burkhard Schöbener

Abstract Deutsch

Die Einordnung der einzelnen Erscheinungsformen des Cyberwars in das System des völkerrechtlichen Friedenssicherungsrechts ist mit einer Vielzahl komplexer Rechtsfragen verbunden. Erörtert wird im vorliegenden Beitrag ein neuer methodologischer Ansatz zur Qualifizierung von Cyberangriffen als Anwendung von *Gewalt* i. S. d. Art. 2 Nr. 4 UN-Ch. und als *bewaffneter Angriff* nach Art. 51 S. 1 UN-Ch. In einem ersten Schritt werden zunächst die in diesem Zusammenhang bisher diskutierten Ansätze anhand ihrer wesentlichen inhaltlichen Maßgaben kurz dargestellt, jedoch letztlich nur als Ausgangspunkt für eine weitergehende methodische Differenzierung verstanden.

Nach der hier vertretenen Auffassung kann der Vielgestaltigkeit potenzieller Angriffe im Cyberwar nur ein Begriffsverständnis gerecht werden, das eine Gesamtwürdigung aller wesentlichen Einzelaspekte zulässt. Aus diesem Grund wird vorgeschlagen, die Begriffe *Gewalt* und *bewaffneter Angriff* methodologisch als Typusbegriffe zu verstehen – als konkret-allgemeine Begriffe, die keine tatbestandlich zwingenden Anforderungen stellen, sondern die Einordnung einer Maßnahme auf einer Skala zwischen zwei sich idealtypisch gegenüberstehenden Polen erlauben und somit die Möglichkeit einer Abstufung eröffnen. Ein solches Verständnis ermöglicht ein flexibles Reagieren auf neue Bedrohungsszenarien, ohne dass es neuer rechtlicher Regelungen bedarf.

Abstract English

The classification of different manifestations of cyberwar under the existing system of international peace and security law entails a variety of complex legal questions. This article discusses a new methodological approach to the qualification of cyber attacks as a *use of force* within the meaning of Art. 2 No. 4 UN-Ch. and as an *armed attack* according to Art. 51 S. 1 UN-Ch. In a first step, the approaches currently under discussion in this context will be presented briefly by reference to their essential substantive requirements, yet they will ultimately only be understood as a starting point for a more extensive methodological differentiation.

According to the view expressed here, only a conceptual understanding, allowing for an overall assessment of all essential individual aspects, can do justice to the multifaceted nature of potential attacks in cyberwar. It is therefore proposed to understand the concepts of *use of force* and *armed attack* methodologically as type concepts ("Typusbegriffe") – as concrete-general concepts that do not impose any mandatory requirements, but allow for a gradual classification of a measure on a scale between two ideally opposed poles. Such an understanding enables a flexible reaction to new threat scenarios without the need for new legal regulations.

1. Einleitung

Neue technologische Entwicklungen erweisen sich immer wieder als fundamentale Herausforderungen an bereits bestehende Rechtsordnungen, basieren letztere doch auf den Erfahrungen aus der Vergangenheit, während die technischen Neuerungen in höchst innovativer Weise zukunftsgerichtet sind. Die neuen Techniken und Methoden gewinnen dadurch immer wieder Vorsprung gegenüber den zur inhaltlichen Erstarrung neigenden rechtlichen Regelungen. Mehr noch als im innerstaatlichen Recht gilt diese Feststellung für die Völkerrechtsordnung, ist letztere angesichts ihrer generellen konsensualen Ausrichtung in ihrer substanziellen Anpassungsfähigkeit an sich höchst dynamisch wandelnde Regelungsgegenstände doch mit besonderen Hürden versehen.

Der vorliegende Beitrag widmet sich einem Themenbereich, der wie kaum ein zweiter in den letzten Jahrzehnten zentrale Fragen des völkerrechtlichen Friedenssicherungssystems aufwirft: dem Cyberwar. Durch die mit diesem neuen Begriff veranschaulichten massiven Änderungen der Kriegsführung werden aber nicht nur die völkerrechtlichen Regeln des *ius in bello* in Frage gestellt;[1] auch das grundsätzliche völkerrechtliche Verbot des *ius ad bellum*[2] sieht sich im Zeitalter der digitalen Revolution mit einer gänzlich neuen technologischen Situation konfrontiert. Die sich daraus ergebenden normativen Unsicherheiten darzustellen, zugleich aber auch neue Ansätze für interpretatorische Lösungen anhand der zentralen Begriffe der „Gewalt“ (Art. 2 Nr. 4 UN-Ch.) und des „bewaffneten Angriffs“ (Art. 51 S. 1 UN-Ch.) aufzuzeigen, ist der zentrale Zweck dieses Festschriftbeitrages zu Ehren meines lieben Freundes und Kollegen *Gilbert H. Gornig*. Durch das Verständnis von *Gewaltanwendung/-androhung* sowie *bewaffnetem Angriff* als sog. Typusbegriffe soll ein neuer methodischer Zugang zu deren inhaltlicher Erschließung aufgezeigt werden.

2. Insbesondere: der Cyberangriff (Computer Network Attack, CNA)

Gerade vor dem Hintergrund einer Analyse des Cyberwars am Maßstab des völkerrechtlichen Friedenssicherungsrechts kommt dem *Cyberangriff* eine ganz besondere Rolle zu, geht es bei ihm doch um die Handlung, die angesichts ihrer konkreten Auswirkungen mit den konventionellen Kriegsergebnissen die meisten

1 S. dazu etwa *Michael N. Schmitt*, Cyber Operations and the Jus in Bello: Key Issues, in: Raul (Pete) Pedrozo/Daria P. Wollschlaeger (Hrsg.), International Law and the Changing Character of War, International Law Studies 87 (2011), 89 ff.

2 Teilweise nach wie vor als *ius ad bellum* bezeichnet (ohne vorangestelltes *Verbot*). Angesichts des heute geltenden universellen Gewaltverbots dürfte dies kaum noch haltbar sein; s. dazu die unterschiedlichen Positionen von *Theodor Schweisfurth*, Völkerrecht, Tübingen: Mohr Siebeck 2006, 479 (Rn. 5) (*ius contra bellum*); *Thomas Bruha*, Ein Recht zum Krieg gibt es nicht mehr, in: Dieter S. Lutz/Hans J. Gießmann (Hrsg.), Stärke des Rechts gegen Recht des Stärkeren, Baden-Baden: Nomos 2003, 289 ff.

Überschneidungsbereiche aufweist. Die *Joint Chiefs of Staff* definieren die CNAs mit "*Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves*"[3].

Allerdings beschränkt sich ein solcher Angriff oftmals nicht auf die Einschränkungen und Beeinträchtigung (Hervorrufung von Störungen oder sogar Zerstörung) der Informationen eines Computernetzwerkes, sondern kann auch weitere Schäden und Funktionsbeeinträchtigungen außerhalb des Netzwerkes hervorrufen (z. B. den Absturz eines Flugzeuges herbeiführen, das Entgleisen eines Zuges verursachen). Aufgeworfen ist damit eine der wichtigsten Fragen im vorliegenden Kontext: Stellt bereits die Einschränkung oder Beeinträchtigung der Informationen des Zielnetzwerkes eine Anwendung von *Gewalt* und/oder einen *bewaffneten Angriff* dar, oder bedarf es dafür auch der Verursachung weiterer Schäden an Leib und Leben von Menschen sowie von Sachschäden?

3. Grundpfeiler des UN-Systems: Verbot der „Androhung oder Anwendung von Gewalt"

In Art. 2 Nr. 4 UN-Ch., dem *corner stone of peace in the charter*[4], ist zwar ganz allgemein von *Gewalt* (*force*) die Rede, doch werden zugleich zwei Handlungsvarianten unterschieden: die *Androhung* und die *Anwendung* (*threat* or *use* of …). Allgemein anerkannt ist heute, dass die Vorschrift im Wesentlichen inhaltlich deckungsgleich ist mit der entsprechenden Vorschrift des Völkergewohnheitsrechts[5] und insoweit auch zum *ius cogens* gehört[6]. Zugleich steht sie in einem Verhältnis der normativen Ergänzung und Vervollständigung zu Art. 51 UN-Ch. (Selbstverteidigungsrecht), für dessen inhaltliches Verständnis das universelle Gewaltverbot von maßgeblicher Bedeutung ist.

3.1. Militärische Gewalt bzw. Waffengewalt als Kerninhalt des universellen Gewaltverbotes

Trotz – vielleicht auch gerade wegen – seiner zentralen Bedeutung für das durch die Vereinten Nationen 1945 geschaffene Friedenssicherungssystem ist der Wortlaut des Art. 2 Nr. 4 UN-Ch. im Hinblick auf den dort verwendeten Gewaltbegriff nur bedingt aussagekräftig. Abgesehen von den drei Zweckklauseln (dazu sogleich

3 Joint Chiefs of Staff, Joint Publication 3–13, Department Of Defense Dictionary of Military and Associated Terms (31 January 2011), 92.

4 *Humphrey Waldock*, The Regulation of the Use of Force by Individual States in International Law, RdC 81 (1952/II), 451 (492).

5 *Burkhard Schöbener*, Gewaltverbot, universelles, in: Burkhard Schöbener (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg: C.F. Müller 2014, 126 (127).

6 IGH, *Nicaragua Case (Nicaragua v. United States of America)*, Urteil v. 27.6.1986, ICJ Reports 1986, 14 (Rn. 190); zuvor bereits die ILC in ILCYB 1966 Vol. II, 248 (Abschn. (3) zu Art. 50 des Entwurfs über das Recht der Verträge).

noch unter 3.1.1. enthält die Vorschrift folgende Regelung: „Alle Mitglieder [der Vereinten Nationen] unterlassen in ihren zwischenstaatlichen Beziehungen jede […] Androhung oder Anwendung von Gewalt." Weitere Erläuterungen zum Gewaltbegriff sind in der UN-Charta nicht vorgesehen, was schon immer zu Diskussionen über den möglichen Begriffsinhalt geführt hat, insbesondere in Ermangelung einer ausdrücklichen Beschränkung auf Waffengewalt (3.1.2.). Letztlich ist die Vorschrift deshalb offen für ein inhaltlich dynamisches Verständnis zugunsten eines modernen Begriffs der militärischen bzw. bewaffneten Gewalt (3.1.3.).

3.1.1. Frühe Diskussionen über den Gewaltbegriff in Art. 2 Nr. 4 UN-Ch.

In den ersten Jahrzehnten des Bestehens der neuen Friedensorganisation waren einzelne Staaten – zumal aus dem sozialistischen Interessenblock und im Gesamtkontext des Kalten Krieges – noch sehr daran interessiert, den Gewaltbegriff der Charta umfassend zu interpretieren. *Gewalt* war danach ein Synonym für jede Art von Zwangsmaßnahme in den zwischenstaatlichen Beziehungen, insbesondere also (auch) die Anwendung politischer und wirtschaftlicher Zwangsmaßnahmen. Doch war bereits während der San Francisco-Konferenz der Antrag Brasiliens abgelehnt worden, dass auch „die Drohung oder der Gebrauch wirtschaftlicher Maßnahmen" vom Gewaltverbot der Charta erfasst sein sollte.[7] Hinter dem Antrag stand – über die politisch-strategischen Überlegungen hinaus – die dogmatische Konzeption, dass der Gewaltbegriff sich nach dem Erfolg bzw. Resultat der staatlichen Einwirkung bemessen sollte, nicht hingegen nach dem dazu verwendeten konkreten Mittel bzw. Instrument. Die Anhänger eines weiten Gewaltbegriffs beriefen sich zum einen auf das Argument der Waffengleichheit, da üblicherweise ökonomisch starke Staaten Wirtschaftssanktionen nur gegenüber insoweit schwächeren Staaten verwendeten, sowie auf das Argument der identischen Gefährdungslage, da Wirtschaftssanktionen in ihren Auswirkungen auf die betroffenen Staaten einer militärischen Intervention entsprechen könnten. Die große Mehrheit der Staaten wie auch der Völkerrechtswissenschaft lehnte diese Sichtweise – nicht zuletzt auch unter Bezugnahme auf den seinerzeit verworfenen Antrag Brasiliens – jedoch ab.[8] Maßgeblich sollte das eingesetzte (Gewalt-)Mittel sein, das man ausschließlich im Gebrauch von militärischer Gewalt bzw. Waffengewalt verortete.[9] Darauf ist

7 Ausführlich dazu *Albrecht Randelzhofer/Oliver Dörr*, in: Bruno Simma (Hrsg.), The Charter of the United Nations, 3. Aufl., Oxford: Oxford University Press 2012, Art. 2 (4), Rn. 17 ff., insb. Rn. 18.

8 S. nur *Randelzhofer/Dörr* (Fn. 7), Art. 2 (4), Rn. 17 f., m. w. N.; *Torsten Stein/Christian v. Buttlar/Markus Kotzur*, Völkerrecht, 14. Aufl., München: Vahlen 2017, Rn. 775; zur Diskussion um den Gewaltbegriff s. auch *Ian Brownlie*, International Law and the Use of Force by States, Oxford: Oxford University Press 1963, 362.

9 *Burkhard Schöbener/Jochen Herbst/Markus Perkams*, Internationales Wirtschaftsrecht, Heidelberg: C.F. Müller 2010, Kap. 2 Rn. 107 f. m. w. N.; s. auch *Wolff Heintschel von Heinegg*, Informationskrieg und Völkerrecht, in: Volker Epping/Horst Fischer/Wolff Heintschel von Heinegg (Hrsg.), FS für Knut Ipsen zum 65. Geburtstag, Etschberg: Kuselit 2000, 129 (138).

im Zusammenhang mit den Maßnahmen der digitalen Kriegsführung zurückzukommen.

Irrelevant für die Feststellung eines Verstoßes gegen das universelle Gewaltverbot sind die in Art. 2 Nr. 4 UN-Ch. genannten – auf den ersten Blick als Restriktionen des Normtatbestandes erscheinenden – Zwecksetzungen, wonach die Gewaltandrohung oder -anwendung „gegen die territoriale Unversehrtheit oder die politische Unabhängigkeit" des angegriffenen Staates gerichtet sein muss oder „sonst mit den Zielen der Vereinten Nationen unvereinbar" ist.[10] Die Entstehungsgeschichte der Zweckklausel offenbart, dass mit ihrer Einfügung eine Einschränkung des Normtatbestandes gerade nicht beabsichtigt war: Vor allem kleinere Staaten drängten – zur Vermeidung einer argumentativen Umgehung des Gewaltverbotes durch militärisch mächtige Staaten – darauf, die Zweckklausel mit ihren drei Alternativen in den Wortlaut der Vorschrift zu implementieren[11], um auf diese Weise besonders intensive Formen der verbotenen Gewaltanwendung hervorzuheben,[12] ohne zugleich den Normtatbestand einengen zu wollen.[13] Gleichwohl ist die Zweckklausel für das Gesamtverständnis der Vorschrift auch heute durchaus noch von Bedeutung, drückt sie doch in ihren beiden ersten Alternativen (Verletzung der territorialen Unversehrtheit oder Verletzung der politischen Unabhängigkeit) – sofern mit militärischer Gewalt vorgenommen – das traditionelle Kriegsverständnis aus, das auch heute noch – insoweit unbestritten – den Kerninhalt des universellen Gewaltverbotes bildet.

3.1.2. Fehlende adjektivische Präzisierung der Gewalt

Wenn heute ganz überwiegend die Auffassung vertreten wird, der in Art. 2 Nr. 4 UN-Ch. ohne jegliche adjektivische Präzisierung verwendete Rechtsbegriff „Gewalt" sei ausschließlich als *militärische* Gewalt bzw. *Waffen*gewalt zu verstehen, dann findet dies jedenfalls keine direkte Grundlage im Normtext des universellen Gewaltverbotes[14]. Auch aus einer rein sprachwissenschaftlichen Sicht ist der Begriff der *Gewalt* durchaus einem weiten Verständnis zugänglich.[15] Mehr noch: Gerade die explizit formulierte Abhängigkeit einer rechtmäßigen Selbstverteidigung (Art. 51 UN-Ch.) von einem „bewaffneten Angriff" (*armed attack*) belegt,

10 Zu einer aus dem Wortlaut abgeleiteten *These von der tatbestandlichen Restriktion des universellen Gewaltverbotes* vgl. ablehnend bereits *Burkhard Schöbener*, Schutz der Menschenrechte mit militärischer Gewalt: die humanitäre Intervention zwischen Völkerrecht und internationaler Politik, Zeitschrift für Politik 47 (2000), 293 (299 ff.), m. N. auch zu den Vertretern des vorgenannten Argumentationsansatzes.

11 Zusammenfassend *Schöbener*, Menschenrechte (Fn. 10), 301, m. w. N.

12 *Schöbener*, Gewaltverbot (Fn. 5), 132.

13 *Brownlie* (Fn. 8), 267; *Falko Dittmar*, Angriffe auf Computernetzwerke, Berlin: Duncker & Humblot 2005, 65; *Schöbener*, Menschenrechte (Fn. 10), 301.

14 Zur Diskussion vgl. *Russell Buchan*, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, Journal of Conflict and Security Law 17 (2012), 211 (215).

15 *Marco Benatar*, The Use of Cyber Force: Need for Legal Justification?, Goettingen Journal of International Law 1 (2009), 375 (381), um dies dann jedoch nach Maßgabe der völkerrechtlichen Auslegungsmaßgaben deutlich einzuschränken (382 ff.).

dass man bei der Schaffung der UN-Charta durchaus den inhaltlichen Mehrwert adjektivischer Präzisierungen kannte und sinnvoll zu verwenden wusste.[16] Gleichwohl bedeutet das keineswegs, dass der Gewaltbegriff damit – im Rahmen eines vor-rechtlichen, linguistischen Verständnisses – einer generellen Determinierung durch die jeweils betroffenen Staaten zugänglich werden sollte. Zumindest eine gewisse inhaltliche Entwicklungsoffenheit des Gewaltbegriffs war damit aber fraglos konzediert.

In der Staatenpraxis sind die beiden Handlungsalternativen (Androhung, Anwendung) von unterschiedlicher Relevanz. Im Mittelpunkt steht üblicherweise die Anwendung von Gewalt, ist diese doch bei konventionellen Waffen (z. B. Artilleriesysteme, Kampfpanzer und -hubschrauber) ohne weiteres objektiv identifizierbar. Überdies ist die generelle und konkrete Eignung solcher „Waffen" zur Herbeiführung massiver Verletzungen der körperlichen Unversehrtheit und des Lebens einer Vielzahl von Menschen sowie von Sachschäden (allg.: Folgeschäden) klar ersichtlich, ohne dass es auf die tatsächliche Verursachung solcher Folgeschäden aber letztlich ankommt. Denn auch der Einmarsch mit Panzern etc. in einen fremden Staat gegen dessen Willen ist schon für sich genommen ein Einsatz von (Waffen-)Gewalt, ohne dass auch nur ein einziger Schuss abgegeben worden sein muss. Selbst wenn man darin keine Anwendung von Gewalt sehen will, so ist doch jedenfalls ihre Androhung offensichtlich.

Für das heute vorherrschende einschränkende Verständnis dürfte vor allem die historisch-waffentechnische Situation am Ende des Zweiten Weltkrieges als reale Vorlage gedient haben, ein Verständnis, das auch in den Jahrzehnten danach angesichts der weithin gleichbleibenden Funktionsweisen der Waffentechnik – abgesehen von ABC-Waffen – keiner grundsätzlichen Revision bedurfte. Und der Waffen-Charakter von ABC-Waffen stand angesichts ihrer konkreten Einsatzszenarien und ihres spezifischen Schädigungspotentials niemals in Zweifel. Gleichwohl wird eine andere Dimension erreicht, wenn man – eher unreflektiert – auch die generelle Verwendung von Viren, Würmern etc. im Cyberraum als solche bereits dem Begriff der (Androhung oder Anwendung von) Gewalt zuordnen wollte. Insoweit bedarf es einer weiteren Aufklärung des Begriffs der militärischen Gewalt bzw. Waffengewalt.

3.1.3. Dynamisches Begriffsverständnis von militärischer/bewaffneter Gewalt

Während der klassische Waffenbegriff allerdings durch das Kriterium der Freisetzung kinetischer Energie[17] gekennzeichnet ist, knüpft der moderne Begriff – wie schon bei der Einbeziehung von biologischen und chemischen Waffen[18] – vor al-

16 S. auch *Matthew C. Waxman*, Cyber Attacks as "Force" under UN Charter Article 2 (4), International Law Studies 87 (2011), 43 (46), dass eine gewollte Beschränkung des Art. 2 Nr. 4 UN-Ch. auf die Verwendung von Waffengewalt im Text auch ihren Ausdruck gefunden hätte.

17 Vgl. *Dittmar* (Fn. 13), 203.

18 *Torsten Stein/Thilo Marauhn*, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 60 (2000), 1 (6); *Heintschel von Heinegg* (Fn. 9), 138: „Der Grund dafür ist so

lem an die Auswirkungen des Einsatzes des Instrumentes (Mittels) an, insbesondere dessen generelle Fähigkeit zur Herbeiführung von massiven physischen Schäden, sei es an der körperlichen Unversehrtheit und dem Leben von Menschen als auch durch die Verursachung bedeutsamer Sachschäden, ggf. – aber nicht notwendig[19] – einschließlich deren Zerstörung.

Auch der IGH[20] hat 1996 in seinem Gutachten zu Nuklearwaffen ausdrücklich betont, dass der Begriff der „Waffe" keinen instrumentenspezifischen Beschränkungen unterliegt:

> "These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons."

Was seinerzeit noch ohne weiteres für ABC-Waffen umfassende Geltung beanspruchen konnte, ist durch die technologische Entwicklung der letzten 30 Jahre jedoch mit neuen Fragezeichen versehen worden: Heute geht es darum, ob es – wiederum gemessen an der Gemeinsamkeit der bisher als Waffen bekannten Instrumente – eines „physischen Elementes" zur Erfüllung der Waffeneigenschaft (Art. 51 UN-Ch.) bedarf, oder ob auch „rein elektronische oder virtuelle Waffen" erfasst werden.[21] Angesichts der Aussage des IGH im Nuklearwaffen-Gutachten und vor dem Hintergrund der Einbettung der einschlägigen Vorschriften (Art. 2 Nr. 4, Art. 51 UN-Ch., Artt. 39, 41, 42 UN-Ch.) in ein normatives Gesamtkonzept zur Erhaltung des Weltfriedens gebietet eine an Ziel und Zweck orientierte Auslegung (Art. 31 Abs. 1 WVK) die chartabasierte dynamische Weiterentwicklung dieser Konzeption.[22] Der offene Wortlaut der genannten Vorschriften erlaubt eine solche systemimmanente Weiterentwicklung nicht nur, sondern gebietet sie sogar. Denn nur auf diese Weise lässt sich der waffentechnologischen Weiterentwicklung auf hinreichend rechtssicherem Grund begegnen.

---

einfach wie offensichtlich: Der Einsatz von biologischen und chemischen Waffen hat unmittelbar Gesundheitsbeeinträchtigungen oder gar den Tod zur Folge. Ist er einem Staat zurechenbar und gegen einen anderen Staat gerichtet, handelt es sich daher um verbotene Gewaltanwendung i.S. der Charta der Vereinten Nationen."

19 Zur Maßgeblichkeit der Auswirkung des Instrumenteneinsatzes: *Stein/Marauhn* (Fn. 18), 6.

20 IGH, *Gutachten über die Legalität von Nuklearwaffen*, Gutachten v. 8.7.1996, ICJ Reports 1996, 226 (Rn. 39). Die Aussage bezieht sich auf Art. 2 Nr. 4, Art. 39 und Art. 51 UN-Ch.

21 So *Stephan Hobe*, Das Selbstverteidigungsrecht im Cyberspace (Vortrag auf einer Akademietagung für Offiziere der Bundeswehr am 16./17.11.2021 in Bensberg, Manuskript), 14 (B.II.1.), der aber eine analoge Anwendung des Art. 51 UN-Ch. befürwortet, „da die Anwendung des naturgegebenen Selbstverteidigungsrechts nicht davon abhängen kann, wie ein möglicher Angriff verursacht bzw. ein entstandener Schaden vermittelt wurde." Eine Betonung des physischen Zwanges findet sich vor allem im Schrifttum der 1950er Jahre; s. nur *Waldock* (Fn. 4), 492.

22 Im Ergebnis ebenso *Yoram Dinstein*, Computer Network Attacks and Self-Defense, International Law Studies 76 (2002), 99 (103); *Albrecht Randelzhofer/Georg Nolte*, in: Simma (Fn. 7), Art. 51, Rn. 43, m. w. N.

3.1.4. Zwischenergebnis

Festzuhalten bleibt somit, dass der nach wie vor aktuelle Gewaltbegriff grundsätzlich auf das verwendete Mittel (Instrument) rekurriert, das traditionell an die Inanspruchnahme kinetischer Energie anknüpft, um dann – im Hinblick auf die Besonderheiten neuartiger Waffentechnik – auch die nicht kinetisch betriebenen Instrumente im Hinblick auf ihr enormes Schädigungspotential erfassen zu können. Dies gibt bereits einen ersten Hinweis darauf, dass ein moderner Gewaltbegriff vor dem Hintergrund der technischen Entwicklungen der letzten Jahrzehnte nicht mehr bei der Qualifizierung des Mittels als „Waffe" bzw. als Einsatz von „Waffengewalt" stehen bleiben kann, sondern auch die (potentiellen) Folgen zu berücksichtigen hat. Erforderlich ist mithin eine *Gesamtbetrachtung*,[23] wie sie bislang typischerweise bei der Frage nach der *Androhung* von (Waffen-)Gewalt[24] von Interesse ist, angesichts der zunehmenden *Komplexität* der *Handlungs-Wirkungs-Zusammenhänge* aber auch bei der Frage nach der *Anwendung* von Gewalt zunehmend in den Fokus tritt. Hier wie dort bedarf es einer Gesamtbetrachtung bzw. Gesamtbewertung (dazu unter 5.–7.).

3.2. Anwendungsszenarien des Cyberwars – Konkrete Folgenbetrachtung am Beispiel kritischer Infrastrukturen

Für den Instrumentenkasten des Cyberwars hat dies zur Folge, dass sich die völkerrechtlich zutreffende Erfassung der unterschiedlichen Mittel digitaler Kriegsführung nicht nach formalen Kriterien (z. B. die technischen Begriffe „Waffe" oder „militärische Gewalt") bestimmt, sondern insoweit vor allem auf die spezifische Wirkungsweise jedes einzelnen Instrumentes abzustellen ist (3.2.1.). Hinzu kommen weitere Überlegungen zu etwaigen physischen Folgeschäden (3.2.2.) und zur Intensität der Einwirkung (3.2.3.). Verdeutlicht wird dies nachfolgend am Beispiel der Einwirkung auf kritische Infrastrukturen.

3.2.1. (Drohende) Einwirkung auf Systeme kritischer Infrastruktur

Die Einordnung einer Cyberattacke als Verstoß gegen das universelle Gewaltverbot (Art. 2 Nr. 4 UN-Ch.) – dasselbe gilt auch für den *bewaffneten Angriff* gem. Art. 51 Abs. 1 S. 1 UN-Ch. – ist jedenfalls dann ohne größere Schwierigkeiten zu leisten, wenn die vorgenannten Folgen (Verletzung von Leib und Leben und/oder Herbeiführung erheblicher Sachschäden) *unmittelbar* (direkt) verursacht werden.[25] In diesen Fällen erweist sich das eingesetzte Mittel schon allein angesichts

23 S. die Zusammenstellung einzelner Beispiele bei *Dinstein*, Computer Network Attacks (Fn. 22), 105; außerdem *Heather Harrison Dinniss*, Cyber Warfare and the Laws of War, Cambridge: Cambridge University Press 2012, 80.

24 Zur Gesamtbewertung im Hinblick auf die Androhung von Gewalt s. IGH, *Gutachten über die Legalität von Nuklearwaffen* (Fn. 20), Rn. 47: Ob eine Androhung von Gewalt vorliege, "depends upon various factors".

25 *Dittmar* (Fn. 13), 90 f.; *Christopher C. Joyner/Catherine Lotrionte*, Information Warfare as International Coercion, EJIL 12 (2001), 825 (849 f.); *Stein/Marauhn* (Fn. 18), 7.

der von ihm bewirkten Folgen, soweit sie denen einer klassischen militärischen Maßnahme nicht nachstehen, als Anwendung von (militärischer bzw. Waffen-) Gewalt.

Nichts anderes gilt auch für die Einwirkung auf Systeme kritischer Infrastrukturen. Dahinter steht die Überlegung, dass es zur Aufrechterhaltung eines ordnungsgemäßen und effizienten Staatswesens besonderer, auf moderner Technik basierender Systeme bedarf. Werden diese Systeme und Einrichtungen ganz oder teilweise zerstört oder auf andere Weise um ihre Funktionsfähigkeit gebracht, dann kann dies – u. a. in Abhängigkeit von dem Grad der Funktionsbeeinträchtigung – durchaus als „Gewalt" im Sinne des völkerrechtlichen Friedenssicherungsrechts zu qualifizieren sein. Derartige Systeme und Einrichtungen lassen sich aber nicht abschließend aufführen; sie sind in ihrer Art und Gewichtung geprägt vom jeweiligen Entwicklungsstand von Staat, Verwaltung, Ökonomie und Gesellschaft. Soweit es vorliegend um Eingriffe im Zusammenhang mit dem universellen Gewaltverbot geht, erscheint eine generelle Charakterisierung des Eingriffsobjektes deshalb nicht zielführend. Vielmehr ist die kritische Infrastruktur inhaltlich in einer Weise zu präzisieren, dass der zentrale Zweck des universellen Gewaltverbotes dabei seine (auch begrenzende) Funktion zur Geltung bringen kann.

Die Qualifizierung von Cyberangriffen ist – über die rechtlichen Schwierigkeiten bei der inhaltlichen Präzisierung der einschlägigen völkerrechtlichen Begriffe hinaus – vor allem auch deshalb mit besonderen Unsicherheiten behaftet, weil solche Angriffe höchst unterschiedliche Auswirkungen mit sich bringen können: von bloßen „Infektionen" des gegnerischen Netzwerks und dessen Ausspähung, über Ärgernisse angesichts der Schädigung von Sachen (z. B. Gebäuden, Infrastruktureinrichtungen und -systemen) bis hin zur Vernichtung einer mehr oder weniger großen Anzahl von Menschenleben, ggf. aber auch „nur" der Verletzung der Gesundheit.[26] So wird im Kontext der Gesamtheit kritischer Infrastrukturen teilweise dahingehend differenziert, Angriffe auf Banken- und Finanzsysteme sowie auf Telekommunikationssysteme stellten keine bewaffneten Angriffe (Art. 51 UN-Ch.) dar;[27] verbunden ist diese Feststellung jedoch mit einer Reihe von Vorannahmen, die in der Lebenswirklichkeit allenfalls zu einer generellen, graduell abstufbaren Systematisierung führen, nicht aber zu abschließenden Feststellungen kategorialer Art.[28]

Zu den im vorliegenden Zusammenhang relevanten Systemen kritischer Infrastruktur gehören vor allem militärische und militärisch genutzte Anlagen und Einrichtungen, aber auch die typischen Versorgungsnetzwerke (insb. Strom, Öl, Gas, Wasser), die Verkehrswege und das Transportwesen, das Gesundheitswesen usw. Irrelevant ist insoweit, ob diese Aufgaben vom Staat und seinen Organisations-

26 S. dazu nur *Michael N. Schmitt*, Computer Network Attack and the Use of Force in International Law, Colum. J. Transnat'l L. 37 (1999), 885 (912); *Dittmar* (Fn. 13), 151.

27 So *Dittmar* (Fn. 13), 156.

28 Zutreffend *Dittmar* (Fn. 13), 156, indem er seine Auffassung mit der zutreffenden Einschränkung verbindet, dass sich „ ‚Grauzonen' nicht vermeiden lassen und daß u. U. nur kleine Veränderungen zu einer anderen rechtlichen Bewertung führen"; *Dinstein*, Computer Network Attacks (Fn. 22), 105, mit differenzierten Beispielen.

einheiten selbst oder von Privaten (aus der Mitte der Gesellschaft) wahrgenommen werden. Maßgeblich ist allein, dass sie aufgrund des Eingriffs von außen nicht mehr ihre zentrale Aufgabe erfüllen können.

3.2.2. Erforderlichkeit der Verursachung physischer Folgeschäden?

Ob es insoweit auch zwingend der zusätzlichen Herbeiführung physischer Folgeschäden bedarf, um eine Qualifizierung als militärische Gewalt i.S.d. Art. 2 Nr. 4 UN-Ch. zu erlauben, ist äußerst umstritten.[29] Zur Abgrenzung gewaltsamer und gewaltfreier Maßnahmen greift ein Teil der Literatur erkenntnisleitend auf die Abgrenzung von Art. 41 und Art. 42 UN-Ch. zurück.[30]

Vor diesem Hintergrund stellt eine Meinungsgruppe[31] (*consequentiality approach*)[32] darauf ab, dass es – wie im Regelfall beim Einsatz kinetischer Waffen und von ABC-Waffen – zu entsprechenden Schäden an Leib und Leben von Menschen sowie zu Sachschäden größeren Ausmaßes kommen müsse. Das führt in der Konsequenz dazu, dass z. B. bei einer Cyberattacke danach differenziert wird, ob es sich um einen Angriff auf ein Telekommunikationssystem oder auf Banken- und Finanzsysteme handelt, die beide allein schon mangels Zerstörung größerer Sachwerte oder einer gewissen Anzahl der Verletzung von Leib und Leben nicht als Anwendung von (Waffen-)Gewalt zu qualifizieren sind.[33] In diesen Bereichen kritischer Infrastruktur ist auch nicht ohne weiteres ersichtlich, unter welchen konkreten Umständen solche Virenangriffe zur Vorbereitung von Militärschlägen dienen können. Anders ist dies zweifellos bei sicherheitsrelevanten Systemen (z. B. militärischen oder polizeilichen Anlagen und Einrichtungen). Ein auf solche Systeme gerichteter Virenangriff wird häufig der gezielten Vorbereitung militärisch relevanter Operationen dienen, ohne dass aber zum konkreten Zeitpunkt solche bereits objektiv ersichtlich sind. Auch Vertreter der Ansicht, die grundsätzlich den Eintritt entsprechender Schadensfolgen verlangen, machen durchaus Zugeständnisse insoweit, dass sie bereits diese Vorbereitungshandlung als Angriffsbeginn qualifizieren.[34]

Idealtypisch gegenübergestellt ist diesem auf die Wirkung abstellenden Interpretationsansatz derjenige Ansatz, der beim Mittel bzw. Instrument der militärischen Operation ansetzt (*instrumentality approach*)[35]. Vor dem Hintergrund des funktionsbezogenen Waffenbegriffs, von dem auch der IGH ausgeht (s. o.), wird die *Cyberwaffe* dann so weit präzisiert, dass jedes diese Definition erfüllende In-

29 S. *Katharina Ziolkowski*, Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen, HuV-I 21 (2008), 202 (208 f.).

30 So etwa *Schmitt* (Fn. 26), 912 f., 924.

31 Grundlegend bereits *Brownlie* (Fn. 8), 362; vgl. auch *Dinstein*, Computer Network Attacks (Fn. 22), 103; *Stein/Marauhn* (Fn. 18), 7: Verursachung „vergleichbarer Schäden"; bestätigend und zusammenfassend: *Dittmar* (Fn. 13), 155 ff.

32 So die Bezeichnung durch *Benatar* (Fn. 15), 389.

33 Überzeugend *Dittmar* (Fn. 13), 156, m.w.N.

34 So *Dittmar* (Fn. 13), 156 f., m.w.N.

35 So die Bezeichnung durch *Benatar* (Fn. 15), 389.

strument, sofern tatsächlich betätigt, als Anwendung von (Waffen-)Gewalt gilt: "Any capability, device, or combination of capabilities and techniques, which if used for its intended purpoose, is likely to impair the integrity or availability of data, a program, or information located on a computer or information processing system."[36]

Diese Beispiele ließen sich in vielfältiger Ausdifferenzierung weiter fortführen.[37] Aber schon so ist erkennbar, dass es keine stringente und konsequente Anwendungslinie gibt – und geben kann. Legt man nämlich den *consequentiality approach* zugrunde, dann ist es schlicht inkonsequent, den Beginn eines Angriffs auf ein sicherheitsrelevantes System bereits in der Einnistung oder sogar der Beeinträchtigung des Computernetzwerks zu verorten, während für alle anderen Fälle die massive Verletzung von Leib und Leben sowie Hervorrufung von Sachschäden verlangt wird. Der *instrumentality approach* kommt völlig ohne jegliche tatsächliche Schadenszufügung aus und stellt vielmehr – allein oder zusammen mit anderen Kriterien – auf die generelle Fähigkeit und konkrete Wahrscheinlichkeit der Schadenszufügung ab. Eine Qualifizierung als (Waffen-)Gewalt allein aufgrund dieses Kriteriums würde den Begriff der Gewalt in Art. 2 Nr. 4 UN-Ch. der Grenzenlosigkeit anheimgeben.

3.2.3. Art und Intensität der Einwirkung?

Welcher Art die Einwirkung sein muss und ob es insoweit einer bestimmten Intensität bedarf, ist ebenfalls umstritten. Gefordert wird teilweise ein „massives Stören" solcher Infrastruktursysteme;[38] andere Stimmen verlangen, dass über die Störung hinaus auch physische Folgeschäden außerhalb des Systems eintreten müssen[39]; wiederum andere begnügen sich hingegen – zur Gewährleistung einer Vergleichbarkeit mit kinetisch betriebenen Waffen – damit, dass die massive Störung „eine ähnliche Wirkung der Friedensstörung bzw. der Störung des öffentlichen Lebens haben kann wie ein Bombardement"[40]. Der IGH hat sich bisher mit dieser Frage noch nicht befassen müssen, gleichwohl aber in seinem Nicaragua-Urteil (1986) die Gelegenheit genutzt, den Gewaltbegriff des Art. 2 Nr. 4 UN-Ch. abzugrenzen vom Begriff des „bewaffneten Angriffs" (Art. 51 S. 1 UN-Ch.). Deshalb wird die Frage nach Art und Intensität der Einwirkung nachfolgend im Kontext des Selbstverteidigungsrechts erörtert. Es sei aber bereits vorweggenommen, dass der Gerichtshof im Rahmen des universellen Gewaltverbotes bislang keine besonderen Anforderungen an Art und Intensität des grenzüberschreitenden Einsatzes von (Waffen-)Gewalt stellt, die Hürden hinsichtlich der Intensität der Gewaltanwendung bei einem „bewaffneten Angriff" hingegen deutlich höher gelegt hat.

36 *Graham H. Todd*, Armed Attack in Cyberspace: Deterring Assymetric Warfare with an Asymmetric Definition, Air Force Law Review 64 (2009), 65 (83).
37 S. nur *Ziolkowski* (Fn. 29), 207 ff.
38 S. *Ziolkowski* (Fn. 29), 208 f.
39 So *Schmitt* (Fn. 26), 912 f., 924, unter Hinweis auf die Abgrenzung von Art. 41 und Art. 42 UN-Ch.
40 *Ziolkowski* (Fn. 29), 208; ebenso *Stein/Marauhn* (Fn. 18), 7.

4. Selbstverteidigungsrecht, Art. 51 UN-Ch.

Neben dem System kollektiver Sicherheit (VII. Kapitel, Art. 39 ff. UN-Ch.) bildet das Selbstverteidigungsrecht (Art. 51 UN-Ch.) die zweite in der Charta ausdrücklich aufgeführte Ausnahmeregelung zum universellen Gewaltverbot.[41] Gegenmaßnahmen des von einem Cyberangriff betroffenen Staates sind mit der Frage konfrontiert, ob sie als Selbstverteidigungsmaßnahme gegen einen „bewaffneten Angriff" auch die Anwendung militärischer Gewalt einschließen dürfen und welche Maßnahmen ggf. davon umfasst sind.

4.1. Systematische Einordnung des Selbstverteidigungsrechts

Unter systematischen Gesichtspunkten ist beachtenswert, dass das Selbstverteidigungsrecht in Art. 51 UN-Ch. geregelt wurde – und damit im Kapitel über das System kollektiver Sicherheit (VII. Kapitel; Art. 39–51 UN-Ch.). Ging man ursprünglich noch davon aus, dass das Selbstverteidigungsrecht gar keiner expliziten Regelung in der Gründungsurkunde der Vereinten Nationen bedurfte, so war Art. 51 UN-Ch. nun allein schon durch diese Einordnung – zumindest im äußeren Erscheinungsbild – auf den rechtlichen Wirkungszusammenhang der kollektiven Sicherheit beschränkt. Sinn macht dies fraglos angesichts der in Art. 51 S. 1 UN-Ch. eingefügten sog. Subsidiaritätsklausel („bis der Sicherheitsrat […] die erforderlichen Maßnahmen getroffen hat"; in Art. 51 S. 2 UN-Ch. finden sich Maßgaben für die weitere Ausgestaltung und Präzisierung der Rechtsstellung des Sicherheitsrates). Zugleich betont die Vorschrift aber auch die besondere Herkunft („das naturgegebene Recht"/"the inherent right") und die aktuelle Ausprägung (neben der individuellen auch die „kollektive Selbstverteidigung"/"collective self-defence")[42] dieses Rechtes. In der Konsequenz bedeutet das zwar, dass – nach Auffassung des IGH[43] – jedenfalls 1945 neben der neu geschaffenen Norm des Vertragsrechts auch eine solche des Gewohnheitsrechts bestand. Inhaltliche Unter-

41 Eine dritte Ausnahme, die Vorschriften über die sog. Feindstaatenklauseln (Art. 107 i. V. m. Art. 53 UN-Ch.), wird bereits seit Jahrzehnten als obsolet angesehen; vgl. *Schöbener* (Fn. 5), 132.

42 Im Völkergewohnheitsrecht war das kollektive Selbstverteidigungsrechts zu diesem Zeitpunkt noch sehr umstritten; vgl. *Nico Krisch*, Selbstverteidigung und kollektive Sicherheit, Berlin: Springer 2001, 235.

43 In seiner Nicaragua-Entscheidung hat der IGH dann 1986 ausdrücklich hervorgehoben (IGH, *Nicaragua Case* [Fn. 6], Rn. 176): "The court therefore finds that Art. 51 of the charter is only meaningful on the basis that there is a 'natural' or 'inherent' right of self-defence, and it is hard to see that this can be other than of a customary nature, even if its present content has been confirmed and influenced by the charter." Weiter heißt es: "It cannot […] be held that Article 51 is a provision which 'subsumes and supervenes' customary international law. It rather demonstrates that in the field in question, the importance of which for the present dispute need hardly be stressed, customary international law continues to exist alongside treaty law. The areas governed by the two sources of law thus do not overlap exactly, and the rules do not have the same content. This could also be demonstrated for other subjects, in particular for the principle of non-intervention."

schiede beider Normen waren damit seinerzeit nicht ausgeschlossen, dürften sich angesichts der generellen Ausrichtung an Art. 51 UN-Ch. in den letzten Jahrzehnten aber weithin egalisiert haben.

4.2. Wortlaut: „bewaffneter Angriff"

Diese inhaltliche Angleichung des Selbstverteidigungsrechts im Vertrags- und Gewohnheitsrecht erfasst nicht zuletzt auch die maßgebliche Voraussetzung für das Selbstverteidigungsrecht, dass sich nämlich ein „bewaffneter Angriff" ("armed attack") ereignet ("occurs"). Bedeutsam ist das vor allem deshalb, weil in den ersten Jahren nach Gründung der Vereinten Nationen teilweise die Ansicht vertreten wurde, das gewohnheitsrechtliche und das chartabasierte Selbstverteidigungsrecht stünden mehr oder weniger isoliert nebeneinander, und die gewohnheitsrechtliche Norm setze keineswegs notwendig einen „bewaffneten Angriff" voraus, sondern könne auch eingreifen im Falle gewaltsamer Angriffe auf wichtige Interessen des Staates im Ausland, z. B. von Leib und Leben der sich außerhalb des eigenen Staatsgebietes aufhaltenden eigenen Staatsangehörigen.[44] Mittlerweile dürfte die inhaltliche Identität des Selbstverteidigungsrechts nach Maßgabe beider Rechtsquellen aber nicht mehr in Zweifel stehen.

4.2.1. Abgrenzung zum Gewaltbegriff aus Art. 2 Nr. 4 UN-Ch.: Spürbarkeitskriterium (IGH)

Auch wenn das Adjektiv „bewaffnet" im Vergleich zum Begriff der Gewalt dem erforderlichen „Angriff" ein – vergleichsweise – konkretes Anforderungsprofil verleiht, so ist die damit verbundene inhaltliche Präzisierung doch nicht mehr als eine erste Annäherung: Denn – wie gesehen – setzt auch der Begriff der Gewalt den Einsatz von Waffen voraus, hat sich insoweit aber auch – dynamisch und entwicklungsoffen – den modernen Waffenbegriff (s. o.) zu Eigen gemacht.

Dennoch hat der IGH in seiner Nicaragua-Entscheidung daraus nicht die – eigentlich naheliegende – Konsequenz gezogen, der Anwendung der Rechtsbegriffe „(Waffen-)Gewalt" (Art. 2 Nr. 4 UN-Ch.) und „bewaffneter Angriff" (Art. 51 S. 1 UN-Ch.) ein identisches Verständnis zuzusprechen. Vielmehr differenziert er beide Begriffe danach aus, dass der „bewaffnete Angriff" der engere Begriff sei, während der Gewaltbegriff darüber hinausgehe und zusätzlich auch solche weiteren Handlungen erfasse, die ebenfalls mit Waffengewalt ausgeführt werden, aber einen gewissen Schweregrad nicht überschreiten:

> "[The Court] has primarily to consider whether a State has a right to respond to intervention with intervention going so far as to justify a use of force in reaction to measures which do not constitute an armed attack but may nevertheless involve a use of force."[45]

44 So etwa *Derek William Bowett*, Self-Defence in International Law, Manchester: Manchester University Press 1958, 184 ff.; s. auch *Julius Stone*, Aggression and World Order, Berkeley: University of California Press 1958, 97 ff.

45 IGH, *Nicaragua Case* (Fn. 6), Rn. 210.

Zur Abgrenzung stellt der Gerichtshof[46] darauf ab. dass es notwendig sei, "to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms." Als Abgrenzungsmaßgaben verweist der IGH in diesem Zusammenhang auf die *Friendly Relations*-Deklaration der UN-Generalversammlung (1970), die er als Ausdruck der Rechtsüberzeugung (*opinio iuris*) der Staatengemeinschaft im Hinblick auf die einschlägigen Normen des Völkergewohnheitsrechts begreift; für das vertragliche Selbstverteidigungsrecht dürfte nichts anderes gelten.

Maßgeblich ist für den Gerichtshof[47] zunächst abstrakt, ob eine solche Operation aufgrund ihres Umfangs und ihrer Auswirkungen (*because of its scale and effects*) als bewaffneter Angriff eingestuft worden wäre, nicht nur als bloßer Grenzvorfall (*a mere frontier incident*). Dass solche Grenzscharmützel unter Einsatz militärischer Gewalt vorgenommen werden, führt nach seiner Auffassung zwar zu einer Qualifizierung als Gewalt i. S. d. einschlägigen Gewohnheitsrechts sowie des Art. 2 Nr. 4 UN-Ch.; gleichwohl stellten solche punktuellen und vorübergehenden Grenzkonflikte aber (noch) keinen bewaffneten Angriff i. S. d. gewohnheitsrechtlichen sowie des vertragsbasierten Selbstverteidigungsrechts dar. Als Reaktionsmöglichkeit bleiben dem davon betroffenen Staat dann allein solche Maßnahmen, wie sie auch bei anderweitigen Verstößen gegen das Interventionsverbot erlaubt sind. Im Nicaragua-Fall qualifizierte der IGH die US-Lieferung von Waffen und Logistik an die Contras zwar als illegale Gewaltanwendung, setzte diese Gewaltanwendung jedoch nicht mit einem bewaffneten Angriff gleich.[48] Im Jahr 2003 legte der Gerichtshof die rechtlichen Maßgaben der Nicaragua-Rechtsprechung dann auch dem Oil Platforms-Fall[49] zugrunde und kam zu dem Ergebnis, dass die dortige konkrete Konstellation nicht dem Nicaragua-Standard entsprach, wonach nur die „schwersten/schwerwiegendsten" (*most grave*) Formen der Gewalt einen bewaffneten Angriff darstellen.

Gleichwohl ist der Nicaragua-Standard keineswegs allgemein akzeptiert. Im Schrifttum[50] wird teilweise jeglicher grenzüberschreitenden Anwendung von militärischer Gewalt die Qualität eines bewaffneten Angriffs zugesprochen: "An armed attack means any use of armed force, and does not need to cross some treshold of intensity." Verbunden ist damit aber auch der Hinweis auf die inhaltlichen Ausdifferenzierungen des Art. 51 UN-Ch., d. h. dass – neben dem Grundsatz der Verhältnismäßigkeit – mit einer Geringfügigkeit der Gewaltanwendung auch ein Anscheinsbeweis (*prima facie evidence*) verbunden sein könne für einen Irrtum oder für die fehlende Absicht zu einer Angriffshandlung. Ein zunehmender Teil der Li-

46 IGH, *Nicaragua Case* (Fn. 6), Rn. 191.
47 IGH, *Nicaragua Case* (Fn. 6), Rn. 195.
48 IGH, *Nicaragua Case* (Fn. 6), Rn. 195.
49 IGH, *Oil Platforms Case (Islamic Republic of Iran v. United States of America)*, Urteil v. 6.11.2003, ICJ Reports 2003, 161 (Rn. 51; 63 f.; 72).
50 *Elizabeth Wilmshurst*, Principles of International Law on the Use of Force by States in Self-Defence, Chatham House, International Law Programme WP 05/01 (2005), 1 (6).

teratur[51] vertritt diese Ansicht ebenfalls und spricht sich damit für eine einheitliche Handhabung der (Waffen-)*Gewalt* und des *bewaffneten Angriffs* aus.

Die h. M.[52] folgt hingegen dem IGH, indem sie den „bewaffneten Angriff" bereits mit einer *Spürbarkeitsschwelle* (*de minimis*-Schwelle) ausstattet, die es – je nach Gewichtung der einzelnen Kriterien – erlaubt, das tatsächliche Geschehen im Rahmen einer Gesamtbetrachtung zu bewerten. Erfasst werden dann nur die *schwersten/schwerwiegendsten* (*most grave*) Formen der Gewaltanwendung. Letztlich kann es sich dabei immer nur um eine Frage der *Intensität* der *Gewaltanwendung* handeln.

4.2.2. Tallin-Manual (2013)

Aufgegriffen wurde die Abgrenzungsformel des IGH, in der es darum geht, die "most grave forms of the use of force (those constituting an armed attack)" zu unterscheiden "from other less grave forms" (s. o.) im Jahr 2013 vom *Tallinn Manual on the International Law Applicable to Cyber Warfare* (nachfolgend: Tallin-Handbuch)[53]. Bei dem Handbuch handelt es sich um eine Darstellung der völkerrechtlichen Regeln für den Bereich des Cyberwars, die von einer internationalen Expertengruppe ausgearbeitet wurden.[54] Die dort getroffenen Festlegungen sind rechtlich nicht verbindlich, vermögen aber dennoch wichtige Hinweise zum aktuellen Stand aktueller Völkerrechtsfragen zu geben. Dem Abschnitt über die Selbstverteidigung (Rule 13) wird ein Leitsatz vorangestellt, der die wesentlichen Erkenntnisse unter Rückgriff auf die *scale-and-effects*-Klausel folgendermaßen zusammenfasst:

---

51 *Bernhard Kempen/Christian Hillgruber/Christoph Grabenwarter*, Völkerrecht, 3. Aufl., München: Vahlen 2021, § 38 Rn. 102; *Christian Hillgruber*, Interventions- und Gewaltverbot, Kriegsrecht, in: Jörg Menzel/Tobias Pierlings/Jeannine Hoffmann (Hrsg.), Völkerrechtsprechung, Tübingen: Mohr Siebeck 2005, 812 (818); kritisch auch *Yoram Dinstein*, War, Aggression and Self-Defence, 6. Aufl., Cambridge: Cambridge University Press 2017, 209: "The assumption that 'a mere frontier incident' can have no 'scale and effects' is quite bothersome"; allgemein zur Diskussion: *Randelzhofer/Nolte* (Fn. 22), Art. 51, Rn. 6 ff., m. w. N.

52 S. nur *Dieter Blumenwitz*, Das universelle Gewaltanwendungsverbot und die Bekämpfung des grenzüberschreitenden Terrorismus, BayVBl. 1986, 373 (379): „militärische Angriffshandlung, die eine gewisse Intensität erreicht"; *Jonas Bens*, Cyberwar und grenzüberschreitendes Selbstverteidigungsrecht, Bonner Rechtsjournal 2011, 149 (151); *Benatar* (Fn. 15), 393: "Figuring out when a cyber force is sufficiently severe to rise to the level of an armed attack is crucial." Zurückhaltender *Wolff Heintschel von Heinegg*, in: Knut Ipsen, Völkerrecht, 7. Aufl., München: C.H. Beck 2019, § 56 Rn. 11: De minimis-Ausnahme nur bei „minimalen Beeinträchtigungen".

53 Veröffentlicht durch Michael N. Schmitt (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2013.

54 Dem Handbuch von 2013 folgte vier Jahre später noch ein zweites Handbuch, diesmal zu den völkerrechtlichen Regeln für Cyberattacken in Friedenszeiten: Michael N. Schmitt (Hrsg.), Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2017.

> "A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."

Und unter Ziff. 3 dieses Abschnitts heißt es ergänzend:

> "The International Group of Experts unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the charter. […] For example, it is universally accepted that chemical, biological and radiological attacks of the requisite scale and effects to constitute armed attacks trigger the right of self-defence. This is so, despite their non-kinetic nature, because the ensuing consequences can include serious suffering or death. Identical reasoning would apply to cyber operations."

4.2.3. Anwendung militärischer Gewalt unterhalb des Spürbarkeitskriteriums

Nicht beantwortet hat der IGH bisher allerdings die Frage, ob auch bei einem Nichterreichen der Erheblichkeitsschwelle der angegriffene Staat – oder ein dritter Staat, ähnlich einer kollektiven Selbstverteidigung – sich dagegen seinerseits mit Gewalt wehren darf:

> "[I]f one State acts towards another State in breach of the principle of non-intervention, may a third State lawfully take such action by way of counter-measures against the first State as would otherwise constitute an intervention in its interna1 affairs? A right to act in this way in the case of intervention would be analogous to the right of collective self-defence in the case of an armed attack, but both the act which gives rise to the reaction, and that reaction itself, would in principle be less grave."[55]

Letztlich hat der Gerichtshof die Frage offengelassen, welche Gegenmaßnahmen (*countermeasures*) dem von einer solchen, unter geringer Gewaltanwendung vorgenommenen Intervention betroffenen Staat grundsätzlich zur Verfügung stehen – und der Rechtsanwendung in diesem Bereich damit Steine statt Brot geliefert. Seinen Grund dürfte dieses Vorgehen vor allem darin finden, dass die normative Interaktion von Art. 2 Nr. 4 und Art. 51 UN-Ch. unter gleichzeitiger Berücksichtigung ihrer ungeklärten völkergewohnheitsrechtlichen Ausdruckspotentiale in abstrakter Form gar nicht generell erfassbar ist. Dafür sind die insoweit vorstellbaren Konstellationen zu vielgestaltig und entwicklungsoffen. Besonders deutlich wird dies angesichts der Cyberwar-Problematik, die ein Anknüpfen an strikte Entweder-oder-Lösungen gar nicht erst zulässt. Nach allgemeinen Regeln dürfen solche Gegenmaßnahmen aber ausschließlich friedlicher (gewaltfreier) Natur sein.[56] Vor dem Hintergrund der damit aber sichtbar werdenden Regelungslücke wird in Bezug auf diese Gegenmaßnahmen von einzelnen Stimmen auch die Zulässigkeit von "*forcible countermeasures*" befürwortet[57] als einer Art *kleines Selbstverteidigungsrecht*.

55 IGH, *Nicaragua Case* (Fn. 6), Rn. 210.

56 *Andreas v. Arnauld*, Völkerrecht, 4. Aufl., Heidelberg: C.F. Müller 2019, Rn. 421, 1087.

57 So *Bruno Simma*, Sondervotum zu IGH, *Oil Platforms Case (Islamic Republic of Iran v. United States of America)*, Urteil v. 6.11.2003, ICJ Reports 2003, 324 (Rn. 12 ff.). Kritisch *Hobe* (Fn. 21), 13 (B.II.1.).

5. „Bewaffneter Angriff“ als Anwendungsfall typologischer Rechtserkenntnis

Die bisherigen Versuche zur Einordnung von Cyberangriffen in das völkerrechtliche Friedenssicherungssystem verdeutlichen, dass die potentielle Vielgestaltigkeit solcher Angriffe mit einer Vielgestaltigkeit der Lösungsansätze einhergeht. Nicht zuletzt das Tallin-Handbuch führt eine Vielzahl von Einzelkriterien an (*severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legality*)[58], die erst im Rahmen einer Gesamtbetrachtung die Frage beantworten, ob ein bewaffneter Angriff vorliegt. Methodischer Anknüpfungspunkt einer Gesamtbetrachtung ist ein Verständnis des bewaffneten Angriffs als *Typusbegriff*, wodurch ein alle wesentlichen Aspekte des Einzelfalles berücksichtigender Ansatz zur Verfügung steht, der sich von dem klassischen Entweder-oder-Ansatz von Gattungsbegriffen grundlegend unterscheidet.

5.1. Lehre vom Typusbegriff – methodischer Türöffner für ein modernes Begriffsverständnis

Im Völkerrecht generell, im Friedenssicherungsrecht im Besonderen wird bislang noch keine Unterscheidung vorgenommen zwischen abstrakt-allgemeinen Rechtsbegriffen (auch Klassen- oder Gattungsbegriffe genannt) einerseits und Typusbegriffen andererseits. Erstere sind üblicherweise einer Definition zugänglich – und ist auch nur eines der Definitionsmerkmale nicht erfüllt, dann ist der Normtatbestand zwingend nicht gegeben. Für das Denken in abstrakt-allgemeinen Begriffen gibt es deshalb nur ein Entweder-oder: Der Rechtsanwender muss stringente inhaltliche Abgrenzungen vornehmen, für die er einer Formulierung im Normtext bedarf, die jeden Einzelfall – positiv oder negativ – erfasst.

Das *typologische* Denken nimmt seinen Ausgangspunkt in der Abgrenzung zum abstrakt-allgemeinen Begriff und in der Erkenntnis, dass es weitere Rechtsbegriffe gibt, die sich inhaltlich gerade nicht durch Definition und Subsumtion erfassen lassen; sie sind deshalb nicht als abstrakt-allgemeine Begriffe zu qualifizieren, sondern als konkret-allgemeine Begriffe, auch Typusbegriffe genannt. Deren Anwendung passt nicht in das Entweder-oder-Schema; vielmehr sind sie geprägt durch ihre konkrete Funktionsbestimmung und ein damit verbundenes Mehr-oder-weniger der inhaltlichen Zuordnung.

Für den Typusbegriff ist kennzeichnend, dass er „nicht als eine Addition isoliert gedachter Merkmale“ erscheint, sondern sich „als ein Ganzes sinnvoll aufeinander bezogener ‚Momente‘ dar[stellt], die nur in dieser ihrer wechselseitigen Verbundenheit den Begriff ausmachen.“[59] Seine inhaltliche Erkenntnis ist dann aber

58 Tallin-Manual von 2013 (Fn. 53), Rule 11 Nr. 9 (49 ff.). Dazu auch *Schmitt* (Fn. 26), 914 f., der diese Kriterien zum Teil bereits vorwegnimmt.

59 *Karl Larenz*, Methodenlehre der Rechtswissenschaft, 5. Aufl., Berlin: Springer 1983, 441. Zur berechtigten generellen Kritik an Larenz’ Typuslehre angesichts ihrer ideologischen Vorprägung s. nur *Horst Ehmann*, Vom logischen Begriff zum Typus, in:

nicht das Resultat der gedanklichen Isolierung einzelner Besonderheiten, sondern einer *Gesamtbetrachtung*: „Der Typus […] ist ein ‚Gefüge', ein sinnvoll strukturiertes Ganzes, in dem jedes ‚Moment' auf ein ‚Sinnzentrum', einen ‚geistigen Kern' bezogen und dadurch in seiner Funktion, in seiner Bedeutung vom Ganzen her bestimmt ist."[60] Bezeichnet wird der Typus deshalb im gleichen Sinn auch als „elastisches" oder „interdependentes Merkmalsgefüge".[61]

In der Rechtsanwendung zeigt sich die Besonderheit des typologischen Denkens darin, dass grundsätzlich nicht von bestimmten, abstrakt formulierten Abgrenzungskriterien ausgegangen wird, sondern von zwei sich idealtypisch gegenüberstehenden gedanklichen Polen, die für den Typusbegriff damit die Möglichkeit der Abstufbarkeit eröffnen. Zwischen den beiden entgegengesetzten Polen sind jeweils beliebig viele Zwischenstufen denkbar, so dass nicht das „Entweder-oder" klassenlogischer Begriffe zum Zug kommt, sondern ein „Mehr-oder-weniger" der Zuordnung zu den beiden Endpunkten.[62] Mit anderen Worten: „Typologische Zuordnung ist Vergleich eines Einzelfalles mit dem Typus unter bestimmten Wertgesichtspunkten mit dem Ergebnis der [...] Einordnung eines konkreten Falles in den Kreis der durch den gesetzlichen Tatbestand gemeinten Fälle aufgrund einer Gleichsetzung mit typischen unter diesen Tatbestand gehörigen Fällen."[63] Ein Typusbegriff in diesem Sinne ist z. B. der Begriff der *Bedrohung des Friedens* (Art. 39 UN-Ch.).[64]

Dass auch die Begriffe der (*Waffen-*)*Gewalt* und des *bewaffneten Angriffs* als Typusbegriffe zu begreifen sind, wird deutlich, wenn man sich im Tallin-Handbuch anschaut, wie die einzelnen der dort genannten Kriterien (s. o.) interagieren:

> "These factors are not exhaustive. Depending on the attendant circumstances, States may look to others, such as the prevailing political environment, whether the operation portends the future use of military force, the identity of the attacker, any record of cyber operations by the attacker, and the nature of the target (such as critical infrastructure). Moreover, the factors operate in concert. As an example, a highly invasive operation that causes only inconvenience such as temporary denial of service is unlikely to be classified as a use of force. By contrast, some may categorize massive cyber operations that cripple an economy as a use of force even though economic coercion is presumptively lawful."[65]

Peter Hanau (Hrsg.), FS für Klaus Adomeit, Köln: Luchterhand 2008, 131 (138 f., mit Fn. 26 ff.) m. w. N. Unabhängig davon ist der Begriff des Typus jedoch keine „Erfindung" von Larenz, sondern auch im Übrigen allgemein anerkannt. S. dazu nur die Definition des Typus bei *Ehmann*, 131 (139 f.), die mit dem hiesigen Verständnis übereinstimmt.

60 *Detlef Leenen*, Typus und Rechtsfindung, Berlin: Duncker & Humblot 1971, 46 f.

61 *Leenen* (Fn. 60), 34, 47.

62 *Leenen* (Fn. 60), 40 f.

63 *Leenen* (Fn. 60), 39 f.

64 Dazu näher *Burkhard Schöbener*, Verfassungsstaatliche Verantwortung für eine internationale Friedensordnung, in: Horst Dreier/Hans Forkel/Klaus Laubenthal (Hrsg.), Raum und Recht, FS 600 Jahre Würzburger Juristenfakultät, Berlin: Duncker & Humblot 2002, 407 (455 ff.); dort auch (457 f.) zu einzelnen faktischen und normativen Kriterien des „interdependenten Merkmalsgefüges" (Typus) der *Friedensbedrohung*.

65 Tallin-Manual von 2013 (Fn. 53), Rule 11 Nr. 10 (52).

Gerade in dieser Umschreibung wird die besondere Art der Inhaltserfassung im konkreten Fall als *elastisches* bzw. *interdependentes Merkmalsgefüge* mehr als deutlich. Maßgeblich ist eine Gesamtbetrachtung aller zur Verfügung stehenden Informationen und völkerrechtlichen Bewertungsmaßstäbe. Das bedeutet hingegen nicht, dass alle der im Tallin-Handbuch genannten Kriterien im Einzelfall tatsächlich in die holistische Analyse einzubeziehen sind.

5.2. Ansätze zu einer typologischen Rechtsanwendung: Gewährleistung des Friedens in den zwischenstaatlichen Beziehungen

Um der Gewaltanwendung und dem bewaffneten Angriff noch zusätzliche rechtliche Konturen zu verleihen, bedarf es zur näheren Bestimmung des Typus auch einer konkreteren *Funktionszuordnung*. Mittlerweile gibt es hinsichtlich der sehr unterschiedlichen Erscheinungsformen und vielgestaltigen Intensität von Cyberangriffen zwar eine Reihe von Systematisierungsversuchen, denen es darum geht, die Vielzahl der Differenzierungsargumente zu ordnen und zu strukturieren.[66] Es fehlt aber regelmäßig an einer normativen Einbindung dieser Problematik in den Gesamtkontext des völkerrechtlichen Friedenssicherungssystems. Zu diesem Zweck ist das gemeinsame *Sinnzentrum* bzw. die gemeinsame *Funktion* beider Begriffe – (Waffen-)Gewalt und bewaffneter Angriff – herauszustellen, um auf dieser Grundlage dann einzelne Merkmale dieses Typus in ihrer *Bedeutung vom Ganzen her* näher bestimmen zu können.

Die nähere Bestimmung des Gewaltbegriffs und der Voraussetzungen des Selbstverteidigungsrechts kann ohne eine inhaltliche Präzisierung des *Friedensbegriffs* – als dem interpolaren Gegenbegriff zum *bewaffneten Angriff* – nicht gelingen. Nach dem traditionellen *negativen Friedensbegriff* besteht immer dann Frieden im völkerrechtlichen Sinn, wenn es im zwischenstaatlichen Bereich zu keiner Anwendung militärischer Gewalt kommt. Mit anderen Worten: Jeder Verstoß gegen Art. 2 Nr. 4 UN-Ch. ist zugleich eine Verletzung des internationalen Friedens. Hinzu tritt nach dem *positiven Friedensbegriff* auch die Verpflichtung der Staaten zur Gewährleistung eines menschenrechtlichen Mindeststandards auf dem von ihnen beherrschten Staatsgebiet. Mit anderen Worten: Jeder Staat, der gegen diesen Mindeststandard (ius cogens, erga omnes-Wirkung) verstößt, verletzt zugleich auch seine Verpflichtung zur Gewährleistung des internationalen Friedens.[67] Zur Wiederherstellung des Friedens stehen zwei Wege offen: ein Eingreifen des UN-Sicherheitsrates (VII. Kapitel der UN-Charta) und – subsidiär – das Selbstverteidigungsrecht des angegriffenen Staates: und zwar sowohl als individuell als auch als kollektiv ausgeübtes Recht (s. o.). Für die nachfolgenden Überlegungen ist davon aus-

66 S. nur *Bens* (Fn. 52), 151 ff.: Folgentheorie, Domänentheorie, Instrumententheorie; *Benatar* (Fn. 15), 387 ff.: Instrumentality Approach, Consequentiality Approach.

67 Zur grundsätzlichen Unterscheidung des inneren und des äußeren (zwischenstaatlichen) Friedens vgl. *Schöbener*, Verfassungsstaatliche Verantwortung (Fn. 64), 408 f., 449 ff., m. w. N.; zur Differenzierung von negativem und positivem Friedensbegriff s. auch *Schöbener/Herbst/Perkams* (Fn. 9), Kap. 2 Rn. 2 ff.; *Burkhard Schöbener/Matthias Knauff*, Allgemeine Staatslehre, 4. Aufl., München: C.H. Beck 2019, § 7 Rn. 90 ff.

zugehen, dass der Sicherheitsrat seiner „Hauptverantwortung für die Wahrung des Weltfriedens und der internationalen Sicherheit“ (Art. 24 Abs. 1 UN-Ch.; s. auch Art. 39 UN-Ch.) nicht nachkommt, weil nur unter dieser Bedingung das Selbstverteidigungsrecht aktiviert werden darf (Art. 51 S. 1 UN-Ch.).

Nähert man sich vor dem Hintergrund des – hier allein maßgeblichen – negativen Friedensbegriffs der Frage nach dem konkreten Schutzzweck von Gewaltverbot und Selbstverteidigungsrecht, nach deren gemeinsamen „Sinnzentrum“, dann findet sich dieses – in einem obersten Ableitungszusammenhang – in der staatlichen Souveränität des angegriffenen Staates. Angesichts des schillernden Charakters des Souveränitätsverständnisses sind daraus – in einem zweiten Ableitungszusammenhang – dann die konkreten Ausprägungen der *territorialen Unversehrtheit* und der *politischen Unabhängigkeit* zu extrahieren, die – unabhängig von ihrer Inbezugnahme in Art. 2 Nr. 4 UN-Ch. – als prägende Kriterien sowohl der staatlichen Souveränität[68] als auch des negativen Friedensbegriffs aufzufassen sind. Die Beeinträchtigung (schon) eines der beiden im Verhältnis der Alternativität stehenden Tatbestände mit militärischer Gewalt (von einiger Intensität) kann dann sowohl als militärische Gewalt i. S. v. Art. 2 Nr. 4 UN-Ch. als auch als bewaffneter Angriff gem. Art. 51 UN-Ch. aufgefasst werden.

6. Beeinträchtigung der territorialen Unversehrtheit oder der politischen Unabhängigkeit

In einem letzten Gedankenschritt sollen nun einzelne Kriterien isoliert werden, die in ihrer Gesamtheit sowohl für den Begriff der (verbotenen) *Gewaltanwendung* als auch des *bewaffneten Angriffs* signifikant sein können. Da es sich bei beiden um Typusbegriffe handelt (s. o.), muss nicht jeder Einzelaspekt additiv erfüllt sein; maßgeblich ist vielmehr eine *Gesamtbetrachtung*, in welche diese Einzelaspekte kumulativ einfließen, ohne dass aber jeder Aspekt sich in der konkreten Lebenswirklichkeit notwendig wiederfinden muss. Gerade dieses *elastische* bzw. *interdependente Merkmalsgefüge* macht den Typusbegriff aus.

Ausgangspunkt ist zunächst ein objektiver Ansatz, bei dem es darum geht, einzelne relevante Kriterien herauszuarbeiten. Dazu gehören neben den Kriterien der sog. Aggressionsdefinition (6.1.) insbesondere die Fragen nach der Maßgeblichkeit des eingesetzten Instrumentes und/oder dessen Auswirkungen (6.2.), des erforderlichen Intensitätsgrades etwaiger Wirkungen (6.3.) sowie nach der Absicht zur Durchführung des bewaffneten Angriffs (6.4.).

6.1. Aggressionsdefinition

Allgemein anerkannt ist, dass die Resolution der UN-Generalversammlung vom 14.12.1974 zur „Definition der Aggression“[69] von grundlegender Bedeutung ist.

68 *Schöbener*, Gewaltverbot (Fn. 5), 132.
69 UN, GV Resolution 29/3314, 14.12.1974, A/RES/29/3314, Anhang.

Zwar hat die Generalversammlung die Resolution zur näheren Bestimmung des Begriffes *Angriffshandlung* (*act of aggression*) in Art. 39 UN-Ch. erlassen; dennoch wird sie ganz überwiegend – obwohl nicht vollständig inhaltlich deckungsgleich – auch zur näheren Bestimmung des bewaffneten Angriffs (Art. 51 S. 1 UN-Ch.) herangezogen. Die einzelnen Aggressions-Tatbestände des Art. 3 der Definition bieten „starke Indizien“[70] für eine entsprechende Auslegung auch des bewaffneten Angriffs. Dasselbe gilt für den Begriff der (Waffen-)Gewalt in Art. 2 Nr. 4 UN-Ch.,[71] soweit es dessen Kerninhalt betrifft.

Bei der Aggressions-Resolution handelt es sich um eine rechtlich nicht verbindliche, rein politische Erklärung (Art. 10 UN-Ch.: Empfehlung).[72] Ihr Art. 1 definiert den Begriff der Aggression als „die Anwendung von Waffengewalt durch einen Staat, die gegen die Souveränität, die territoriale Unversehrtheit oder die politische Unabhängigkeit eines anderen Staates gerichtet ist oder sonst mit der Charta der Vereinten Nationen unvereinbar ist“. Bereits in seinem Nicaragua-Urteil hat der IGH[73] die Resolution auszugsweise herangezogen (konkret: Art. 3 lit. g der Definition) und angemerkt, die dort gegebene Umschreibung “may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.”

Auch die anderen Art. 3-Tatbestände sind regelmäßig – obwohl 1974 noch niemand die Option eines Cyberwars voraussehen konnte – so formuliert, dass ihre grundsätzliche Anwendbarkeit (auch) auf Cyberangriffe durchaus naheliegt. So setzt etwa die „Invasion […] auf das Hoheitsgebiet eines anderen Staates“ (Art. 3 lit. a der Definition) keineswegs den körperlichen Einmarsch von Truppen und Gerät voraus, sondern ist auch denkbar durch den grenzüberschreitenden Einsatz von Computerviren; unter „Waffen jeder Art“ können nach Wortlaut- und Zweckverständnis ohne weiteres auch über Computer verbreitete Viren fallen.[74]

6.2. Instrument(e) und/oder Auswirkung(en) der Cybermaßnahme

Dass Cyberangriffe – selbst unabhängig von den Kriterien der Aggressionsdefinition – in Abhängigkeit von den konkreten Umständen als Gewaltanwendung (Art. 2 Nr. 4 UN-Ch.) qualifiziert werden können und damit – von wenigen Ausnahmefällen abgesehen (s. o.) – auch als bewaffnete Angriffe das Selbstverteidigungsrecht auszulösen vermögen (Art. 51 S. 1 UN-Ch.), dürfte heute allgemein akzeptiert sein.

70 *Stephan Hobe*, Bewaffneter Angriff, in: Schöbener (Fn. 5), 45 (46); dort auch zur (modifizierten) Aufnahme dieser Tatbestände in die Aggressions-Definition des IStGH-Statuts.

71 *Schöbener*, Gewaltverbot (Fn. 5), 129; *Stephan Hobe*, Selbstverteidigungsrecht, völkerrechtliches, in: Schöbener (Fn. 5) 374 (375).

72 *Peter Dreist*, Aggression (Straftatbestand), in: Schöbener (Fn. 5), 7 (9).

73 IGH, *Nicaragua Case* (Fn. 6), Rn. 210.

74 Vgl. nur *Stein/Marauhn* (Fn. 18), 4 f., m. w. Anwendungsbeispielen.

Äußerst umstritten ist hingegen, welche Voraussetzungen insoweit erfüllt sein müssen, insbesondere ob vorrangig auf die Art des eingesetzten Mittels (Instrumentes) abzustellen ist oder auf die dadurch letztlich herbeigeführten Wirkungen bzw. Folgen (s. bereits unter 3.2.2.).

Dieser Grunddissens ergibt sich unmittelbar aus den Eigenarten und Spezifika waffentechnologischer Neuerungen im Kontext des Cyberwars: Über Computer verbreitete Viren, Würmer etc. werden im Netz in vielfältiger Weise eingesetzt, sind mithin gerade nicht in einem spezifisch technischen Sinn als Waffen zu begreifen, sondern in einem funktionalen Sinn. Ihr Einsatz bedarf keiner physischen Grenzüberschreitung durch militärische Einheiten und/oder Waffen und Geschosse im klassischen Verständnis. Die Auswirkungen sind häufig nicht sofort ersichtlich, geschweige denn mit der direkten Vernichtung von Leib und Leben oder massiven Sachschäden verbunden. Gleichwohl sind die „eingenisteten" Viren jederzeit in der Lage, aktiv zu werden, um dann – zeitlich verzögert – massive Schäden auch außerhalb des Netzwerkes herbeizuführen, wie sie üblicherweise auch von konventionellen Waffen hervorgerufen werden.

Noch stark vom klassischen Verständnis geprägt ist der Ansatz, der im Schwerpunkt auf die Auswirkungen (Folgen) abstellt (*consequentiality approach*). Erst der tatsächlich eingetretene Schaden, vergleicht man ihn mit demjenigen eines unter Verwendung kinetischer Waffen herbeigeführten Schadens, erlaubt die Einordnung als hinreichend intensive Gewaltanwendung. Das ist immer dann nicht gegeben, wenn "the act (whether merely unfriendly or a transgression of international law) does not entail sufficiently grave consequences"[75]. Diese Ansicht ist ersichtlich noch vom klassischen Begriff der (Waffen-)*Gewalt* und des *bewaffneten Angriffs* geprägt. Hinzu tritt bei einzelnen Autoren eine nähere Eingrenzung und Spezifizierung der Zielobjekte, um jedenfalls für Angriffe auf Computer, die ihrerseits für die Aufrechterhaltung bestimmter Infrastrukturen oder Einrichtungen der nationalen Sicherheit verantwortlich sind, von vornherein eine Überschreitung der Grenze zum bewaffneten Angriff anzunehmen.[76]

Ein zweiter Ansatz stellt (vor allem) auf das Mittel (Instrument) ab, das grenzüberschreitend zum Einsatz kommt (*instrumentality approach*). Angesichts der häufigen Nichterkennbarkeit der „Virusinfektion" und ihres Gefahren- und Realisierungspotentials sind in der Regel aber keine frühzeitigen Gegenmaßnahmen möglich. "In cyberspace, what may appear as a 'minor attack' could evolve into something much more destructive to a nation state, taking days or months to cause observable, significant harm".[77] Ob es durch den Einsatz des Virus überhaupt zu Schäden kommt, oder welchen Umfang diese aufweisen, soll letztlich unerheblich sein. Auf diese Weise wird ein eigenständiger Begriff der Cyberwaffe ent-

75 *Dinstein*, Computer Network Attacks (Fn. 22), 105.

76 S. nur *Daniel M. Creekman*, A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China, American University International Law Review 17 (2002), 642 (653 ff.), mit der grundlegenden Differenzierung zwischen "vital and non-vital targets" (654, passim); referierend *Bens* (Fn. 52), 151 f.

77 *Todd* (Fn. 36), 77; referierend *Bens* (Fn. 52), 153.

wickelt,[78] bei dessen Anwendung es weder auf die konkreten Folgen des Einsatzes ankommt noch auf das Erreichen einer wie auch immer zu bestimmenden Intensitätsschwelle (dazu noch unten). Ausreichend ist vielmehr die generelle Eignung des Virus, entsprechende Folgen zu bewirken ("likely to impair").

6.3. Intensitätsgrad: Spürbarkeits- bzw. Erheblichkeitsschwelle

Beide Ansätze sind letztlich nur die gedanklichen Ausgangspunkte für eine Vielzahl von Differenzierungsmöglichkeiten und -notwendigkeiten. Je kleinteiliger man diese einzelnen Cyberangriffe tatsächlich erfasst und rechtlich bewertet, desto weniger wird allerdings jeder von ihnen die vom IGH abstrakt vorgegebene Spürbarkeits- bzw. Erheblichkeitsschwelle erreichen. Eine „Politik der militärischen Nadelstiche"[79] kann – zumal im Cyberspace – eine Häufung von Beeinträchtigungen der territorialen Unversehrtheit mit sich bringen, ohne dass – bei isolierter Betrachtung – jede einzelne Attacke den erforderlichen Intensitätsgrad selbst verwirklicht. Gehen die Angriffe von demselben Staat aus, dann liegt es jedenfalls nahe, die tatsächlich verschiedenen Angriffe rechtlich als eine (kumulierte) Handlung zu begreifen.[80]

Rechtliche Relevanz beansprucht die Frage nach dem Intensitätsgrad – dies wird in der IGH-Entscheidung nicht hinreichend deutlich – vor allem deshalb, weil davon abhängt, ob wirklich eine *Verletzung* der *territorialen Unversehrtheit (Integrität)* und/oder der *politischen Unabhängigkeit* des Zielstaates vorliegt. Im Regelfall dürfte es um die erste Alternative gehen und um die damit einhergehende Frage, ob bei *wertender* Analyse der Gesamtsituation die Typologie des Geschehens sich für einen objektiven Beobachter so darstellt, dass sie als *bewaffneter Angriff* zu qualifizieren ist (s. dazu noch unter 7.).

Dabei ist eines bereits gewiss: Die Frage nach dem *Intensitätsgrad* bzw. der *Spürbarkeitsschwelle* militärischer Gewaltanwendung ist einfach zu stellen, aber umso schwieriger zu beantworten. Während diese Begriffe nämlich vorgeblich den Eindruck erwecken, als seien sie mathematischer oder metrischer Beweisführung zugänglich, so handelt es sich bei ihnen doch letztlich um generalklauselartige Allgemeinformulierungen, deren Vorliegen sich erst im Rahmen einer umfassenden Bewertung der Faktenlage erschließt.

6.4. Subjektive Seite – Wissen und Wollen des bewaffneten Angriffs

Für den bewaffneten Angriff ist zudem anerkannt, wenngleich selten thematisiert, dass "the use of force must be deliberate: it cannot be caused by mistake through

78 *Todd* (Fn. 36), 83; wiedergegeben auch von *Bens* (Fn. 52), 153.

79 *Kempen/Hillgruber/Grabenwarter* (Fn. 51), 234, Rn. 103; s. dazu auch *Stein/v. Buttlar/Kotzur* (Fn. 8), Rn. 787: „gestreute Bagatellangriffe".

80 So auch das Tallin-Handbuch von 2013 (Fn. 52) unter Rule 13 Nr. 8; für eine kumulierte Betrachtung der Einzelhandlungen auch *Christopher Greenwood*, Self-Defence, in: Rüdiger Wolfrum (Hrsg.), MPEPIL, Online Edition, Oxford: Oxford University Press 2011, Rn. 13, der aber im Hinblick auf Cyberattacken nach den ausgelösten Folgen differenziert (Rn. 14); skeptisch *Stein/Marauhn* (Fn. 18), 5.

an accident"[81]. Es bedarf mithin einer entsprechenden „Intention" desjenigen Staates, der den bewaffneten Angriff durchführt,[82] was besonders den Fall „bewusster Zerstörung" von gegnerischen Informationsinfrastrukturen erfasst.[83] Das Wissen und Wollen muss sich mithin auf den Angriff beziehen; dass es sich bei dem verwendeten Instrument (Mittel) um eine Waffe handelt, ist angesichts des funktionsbezogenen Waffenbegriffs (s. o.) in aller Regel bei einem bewussten Angriff ebenfalls vom Vorsatz bzw. der Absicht erfasst.[84]

7. Bewertende Gesamtbetrachtung: Typus des „bewaffneten Angriffs"

Die eigentliche Schwierigkeit besteht nun darin, die vom IGH verwendete Terminologie (*the most grave forms of the use of force*, wobei maßgeblich auf *scale and effects* abzustellen sei) so mit zusätzlichen Kriterien anzureichern, dass sich auch die metaphorische Versinnbildlichung (Spürbarkeits-, Erheblichkeits- oder Intensitäts*schwelle*) für rationale Überlegungen öffnet. Wie aber lassen sich die „schwersten/schwerwiegendsten" Formen der Gewalt näher bestimmen? Dabei kann es nicht allein um eine quantitative Erfassung der Zahl der Einzeltaten und ihrer tatsächlichen Konsequenzen gehen; vielmehr bedarf es ihrer rechtlichen Bewertung vor dem Hintergrund möglichst aller Einzelaspekte, die zur inhaltlichen Erkenntnis eines bewaffneten Angriffs fruchtbar gemacht werden können.

Vorauszuschicken ist den nachfolgenden Überlegungen, dass die *Urheberschaft* des angreifenden Staates jeweils als geklärt zu unterstellen ist. Eine solche Feststellung dürfte in der Realität in aller Regel mit großen Schwierigkeiten verbunden sein, da die Wege eines Virus, Wurms etc. *kaum rückverfolgbar* sind. Besonders problematisch ist insoweit die quasi endlose Verbindung zwischen den internationalen Netzwerken. Diese Aspekte sollen aber hier ausgeblendet werden. Zum anderen ist darauf hinzuweisen, dass selbst in den Fällen, in denen ein bewaffneter Angriff angenommen wird, die Reaktion des betroffenen Staates dem *Grundsatz der Verhältismäßigkeit* unterliegt, wodurch nicht erforderlichen oder unangemessenen Maßnahmen des angegriffenen Staates gerade auch im Interesse der dauerhaften Friedenswahrung rechtlich Einhalt geboten wird.

Eine am Typus ausgerichtete Normerkenntnis bedeutet insbesondere, dass die Unterscheidung des Handlungsinstrumentes („Waffe") und des Handlungserfolges („Angriff" unter Verletzung von Leib, Leben und Sachen) nicht kategorial zu verstehen ist. Vielmehr handelt es sich um einen einheitlichen Begriff des „bewaffneten Angriffs", dessen Kriterien in einem wechselseitigen Bedingungszusammenhang stehen, mit dem eine graduelle Abstufbarkeit einhergeht. Idealtypisch ist ein Angriff unter Einsatz einer kinetischen Waffe, durch die auf dem Territorium des

81 *Dinstein*, War (Fn. 51), 209.
82 *Dittmar* (Fn. 13), 154.
83 So *Stein/Marauhn* (Fn. 18), 2.
84 Vgl. *Stein/Marauhn* (Fn. 18), 6, 39 f.

Nachbarstaates z. B. ein Flughafen bombardiert wird mit dem Ergebnis von mehreren hundert Toten und Verletzten und einem fast völlig zerstörten Flughafen. Ein *bewaffneter Angriff* ist dann zweifellos gegeben. Nichts anderes gilt aber auch dann, wenn dasselbe Resultat herbeigeführt wird durch eine gezielt eingesetzte Malware.

Ergeben haben die vorstehenden Überlegungen aber auch, dass auf der Grundlage eines untechnischen, funktionalen Verständnisses entsprechend programmierten Viren, Würmer etc. als Anwendung militärischer Gewalt bzw. von Waffengewalt einzuordnen sind. Die nähere rechtliche Qualifikation insbesondere als *bewaffneter Angriff* (Art. 51 S. 1 UN-Ch.) ist kein klassischer juristischer Subsumtionsvorgang, sondern das Ergebnis eines komplexen, aber dennoch regelgeleiteten Zuordnungsvorgangs, dessen zentrale Maßgaben sich im Rahmen der völkerrechtlichen Konzeption der Friedenssicherung insbesondere mit der Frage zu befassen haben, ob eine *spürbare* Verletzung der *territorialen Unversehrtheit* (Integrität) des Zielstaates vorliegt. Dabei handelt es sich um eine Wertungsfrage, deren Beantwortung im Wege einer Gesamtbetrachtung des Geschehens nicht nur von der Zahl der dadurch getöteten und verletzten Personen sowie der Höhe des Sachschadens abhängt, sondern – selbst für den Fall, dass solche Schäden noch nicht eingetreten sind – auch Aspekte zu berücksichtigen hat wie das tatsächliche Bedrohungspotential für diese Rechtsgüter, die Wahrscheinlichkeit des Schadenseintritts oder die eigene Fähigkeit, falls das Virus sich im bedrohten Netzwerk des Zielstaates bereits „eingenistet“ hat, dieses Virus kurzfristig und rückstandslos zu entschärfen. Bedeutsam ist zudem, ob es Anzeichen dafür gibt, dass das Virus ohne Wissen und Wollen des anderen Staates sich verselbständigt hat, so dass es an der subjektiven Seite eines bewaffneten Angriffs fehlen würde – ein absoluter Ausschlussgrund für die Aktivierung des Selbstverteidigungsrechts. Letztlich lassen sich die möglicherweise im Einzelfall einschlägigen Kriterien – wie bei einem *interdependenten Merkmalsgefüge* üblich – nicht abschließend aufzählen. Sie sind aber – und das ist das Entscheidende – jeweils darauf zu befragen, ob und ggf. welche Relevanz und welches Gewicht sie im Hinblick auf die Beeinträchtigung der territorialen Unversehrtheit (Integrität) beanspruchen und dementsprechend in die Gesamtbewertung einzustellen.

Damit ist eine argumentative Grundstruktur offengelegt, die sich zweifellos nach Maßgabe der Besonderheiten eines konkreten Falles weiter ausdifferenzieren lässt. Maßgeblich ist aber immer, dass die – tatsächlichen oder potentiellen (wenngleich mit hoher Wahrscheinlichkeit eintretenden) – Auswirkungen auf die territoriale Unversehrtheit einen entsprechenden Intensitätsgrad (Spürbarkeitsschwelle) erreichen.

8. Fazit

Neuartige Bedrohungsszenarien bedürfen regelmäßig auch neuer rechtlicher Regelungen – das gilt ganz besonders im Völkerrecht. Die in diesem Beitrag niedergelegten Erwägungen verfolgten hingegen den Zweck, auf dem rechtlichen Fundament des geltenden Friedenssicherungsrechts neue Wege aufzuzeigen, um die

bereits stark ausdifferenzierte Diskussion über die Einordnung von Cyberangriffen als Anwendung von (*Waffen-*)*Gewalt* (Art. 2 Nr. 4 UN-Ch.) und als *bewaffneter Angriff* (Art. 51 S. 1 UN-Ch.) methodologisch zu erweitern. Versteht man die beiden – neben Art. 39 ff. UN-Ch. – zentralen Rechtsbegriffe des UN-Friedenssicherungssystems als Typusbegriffe, was in einem Teil der Literatur praktisch bereits geschieht, allerdings ohne den methodischen Unterschied zu abstrakt-allgemeinen Rechtsbegriffen wirklich offenzulegen, dann ist damit einer Rechtserkenntnis der Weg bereitet, die der unendlichen Vielfalt der Einsatzszenarien von entsprechend programmierter Malware ebenso Rechnung trägt wie dem komplexen rechtlichen Anforderungen der einschlägigen völkerrechtlichen Vorschriften.

Literaturverzeichnis

a) Monographien und Sammelbände

Derek William Bowett, Self-Defence in International Law, Manchester: Manchester University Press 1958.

Ian Brownlie, International Law and the Use of Force by States, Oxford: Oxford University Press 1963.

Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge: Cambridge University Press 2012.

Yoram Dinstein, War, Aggression and Self-Defence, 6. Aufl., Cambridge: Cambridge University Press 2017.

Falko Dittmar, Angriffe auf Computernetzwerke, Berlin: Duncker & Humblot 2005.

Bernhard Kempen/Christian Hillgruber/Christoph Grabenwarter, Völkerrecht, 3. Aufl., München: Vahlen 2021.

Nico Krisch, Selbstverteidigung und kollektive Sicherheit, Berlin: Springer 2001.

Karl Larenz, Methodenlehre der Rechtswissenschaft, 5. Aufl., Berlin: Springer 1983.

Detlef Leenen, Typus und Rechtsfindung, Berlin: Duncker & Humblot 1971.

Burkhard Schöbener/Matthias Knauff, Allgemeine Staatslehre, 4. Aufl., München: C.H. Beck 2019, § 7.

Theodor Schweisfurth, Völkerrecht, Tübingen: Mohr Siebeck 2006.

Burkhard Schöbener/Jochen Herbst/Markus Perkams, Internationales Wirtschaftsrecht, Heidelberg: C.F. Müller 2010.

Torsten Stein/Christian v. Buttlar/Markus Kotzur, Völkerrecht, 14. Aufl., München: Vahlen 2017.

Julius Stone, Aggression and World Order, Berkeley: University of California Press 1958.

Andreas v. Arnauld, Völkerrecht, 4. Aufl., Heidelberg: C.F. Müller 2019.

b) Beiträge in Festschriften und Sammelbänden

Thomas Bruha, Ein Recht zum Krieg gibt es nicht mehr, in: Dieter S. Lutz/Hans J. Gießmann (Hrsg.), Stärke des Rechts gegen Recht des Stärkeren, Baden-Baden: Nomos 2003, 289 ff.

Peter Dreist, Aggression (Straftatbestand), in: Burkhard Schöbener (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg: C.F. Müller 2014, 7.

Horst Ehmann, Vom logischen Begriff zum Typus, in: Peter Hanau (Hrsg.), FS für Klaus Adomeit, Köln: Luchterhand 2008, 131.

Christopher Greenwood, Self-Defence, in: Rüdiger Wolfrum (Hrsg.), MPEPIL, Online Edition, Oxford: Oxford University Press 2011.

Wolff Heintschel von Heinegg, in: Knut Ipsen, Völkerrecht, 7. Aufl., München: C.H. Beck 2019, § 56.

Wolff Heintschel von Heinegg, Informationskrieg und Völkerrecht, in: Volker Epping/Horst Fischer/Wolff Heintschel von Heinegg (Hrsg.), FS für Knut Ipsen zum 65. Geburtstag, Etschberg: Kuselit 2000, 129.

Christian Hillgruber, Interventions- und Gewaltverbot, Kriegsrecht, in: Jörg Menzel/Tobias Pierlings/Jeannine Hoffmann (Hrsg.), Völkerrechtsprechung, Tübingen: Mohr Siebeck 2005, 812.

Stephan Hobe, Bewaffneter Angriff, in: Burkhard Schöbener (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg: C.F. Müller 2014, 45.

Stephan Hobe, Selbstverteidigungsrecht, völkerrechtliches, in: Burkhard Schöbener (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg: C.F. Müller 2014, 374.

Albrecht Randelzhofer/Oliver Dörr, in: Bruno Simma (Hrsg.), The Charter of the United Nations, 3. Aufl., Oxford: Oxford University Press 2012, Art. 2 (4).

Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, in: Raul (Pete) Pedrozo/Daria P. Wollschlaeger (Hrsg.), International Law and the Changing Character of War, International Law Studies 87 (2011), 89 ff.

Burkhard Schöbener, Gewaltverbot, universelles, in: Burkhard Schöbener (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg: C.F. Müller 2014, 126.

Burkhard Schöbener, Verfassungsstaatliche Verantwortung für eine internationale Friedensordnung, in: Horst Dreier/Hans Forkel/Klaus Laubenthal (Hrsg.), Raum und Recht, FS 600 Jahre Würzburger Juristenfakultät, Berlin: Duncker & Humblot 2002, 407.

c) Aufsätze

Marco Benatar, The Use of Cyber Force: Need for Legal Justification?, Goettingen Journal of International Law 1 (2009), 375.

Jonas Bens, Cyberwar und grenzüberschreitendes Selbstverteidigungsrecht, Bonner Rechtsjournal 2011, 149.

Dieter Blumenwitz, Das universelle Gewaltanwendungsverbot und die Bekämpfung des grenzüberschreitenden Terrorismus, BayVBl. 1986, 373.

Russell Buchan, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, Journal of Conflict and Security Law 17 (2012), 211.

Daniel M. Creekman, A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China, American University International Law Review 17 (2002), 642.

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

Christopher C. Joyner/Catherine Lotrionte, Information Warfare as International Coercion, EJIL 12 (2001), 825.

Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law, Colum. J. Transnat'l L. 37 (1999), 885.

Burkhard Schöbener, Schutz der Menschenrechte mit militärischer Gewalt: die humanitäre Intervention zwischen Völkerrecht und internationaler Politik, Zeitschrift für Politik 47 (2000), 293.

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

Graham H. Todd, Armed Attack in Cyberspace: Deterring Assymetric Warfare with an Asymmetric Definition, Air Force Law Review 64 (2009), 65.

Humphrey Waldock, The Regulation of the Use of Force by Individual States in International Law, RdC 81 (1952/II), 451.

Matthew C. Waxman, Cyber Attacks as „Force" under UN Charter Article 2 (4), International Law Studies 87 (2011), 43.

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

d) Gerichtsentscheidungen

Bruno Simma, Sondervotum zu IGH, *Oil Platforms Case (Islamic Republic of Iran v. United States of America)*, Urteil v. 6.11.2003, ICJ Reports 2003, 324.

IGH, *Nicaragua Case (Nicaragua v. United States of America)*, Urteil v. 27.6.1986, ICJ Reports 1986.

IGH, *Oil Platforms Case (Islamic Republic of Iran v. United States of America)*, Urteil v. 6.11.2003, ICJ Reports 2003, 161.

e) Internationale Dokumente

IGH, *Gutachten über die Legalität von Nuklearwaffen*, Gutachten v. 8.7.1996, ICJ Reports 1996, 226.

ILC, *Entwurf über das Recht der Verträge, Artikel 50*, ILCYB 1966 Vol. II, 248.

UN, GV Resolution 29/3314, 14.12.1974, A/RES/29/3314, Anhang.

f) Sonstiges

Stephan Hobe, Das Selbstverteidigungsrecht im Cyberspace, Vortrag auf einer Akademietagung für Offiziere der Bundeswehr am 16./17.11.2021 in Bensberg, Manuskript.

Joint Chiefs of Staff, Joint Publication 3–13, Department Of Defense Dictionary of Military and Associated Terms (31 January 2011), 92.

Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2013.

Michael N. Schmitt (ed.), Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2017.

Elizabeth Wilmshurst, Principles of International Law on the Use of Force by States in Self-Defence, Chatham House, International Law Programme WP 05/01 (2005), 1.