Cyberwar und völkerrechtliches Selbstverteidigungsrecht

Überlegungen zum Begriff des bewaffneten Angriffs bei Attacken im Cyberspace

Jonas Bens, Bonn*

Kriegsführung im Cyberspace ist unlängst aus dem Bereich der Science-Fiction-Literatur auf die Agenda der internationalen Sicherheitspolitik gerückt. Hieraus ergeben sich auch neue Herausforderungen für das Völkerrecht, insbesondere das ius ad bellum. Der Beitrag widmet sich der Frage, unter welchen Bedingungen Cyberangriffe als bewaffneter Angriff angesehen werden können, der im Rahmen des Art. 51 der UN-Charta den angegriffenen Staat zu Selbstverteidigungsmaßnahmen berechtigt. Hierzu erfolgt ein Überblick über den kaum fünfzehn Jahre alten, kontroversen Forschungsstand und eine Stellungnahme zu wesentlichen Streitfragen. Damit verbunden sind Überlegungen zu einem dem technischen Fortschritt angepassten Begriff des bewaffneten Angriffs.

I. Einleitung

Oft wird das 20. Jahrhundert als eine Epoche der Technologisierung des Krieges bezeichnet. Folgt man dieser Charakterisierung, so ließe sich sagen, dass das 21. Jahrhundert eine Epoche der Computerisierung des Krieges einleiten wird. Es ist gut vorstellbar, dass der Cyberspace zum Schlachtfeld und Viren oder Trojaner zu den Waffen der Zukunft werden. Dabei können Verheerungen angerichtet werden, die jenen der konventionellen Kriegsführung in nichts nachstehen. Cyberangriffe, wie beispielsweise auf Estland im Jahre 2004, sind Anfang dieses Jahrhunderts ins öffentliche Bewusstsein gerückt. Innerhalb der letzten zwei Jahre gab es nachweislich mehrere Angriffe auf Computersysteme in den USA, Kirgistan, Iran, Zimbabwe, Israel und Südkorea.[1] Auch ist zu vermuten, dass einige davon mehr oder weniger direkt von Regierungen durchgeführt worden sind.[2] Computerspezialisten sprechen in diesem Zusammenhang bereits von einem internationalen Cyberwettrüsten („cyber arms race“[3]).

Dieser Beitrag geht der Frage nach, welche Auswirkungen die neuen Bedrohungslagen durch Angriffe auf die informationstechnischen Systeme eines Staates, im folgenden als Cyberangriffe bezeichnet, auf den Begriff des bewaffneten Angriffs und damit auf die Konstruktion des Selbstverteidigungsrechts im Rahmen des Artikel 51 der Charta der Vereinten Nationen (UN-Ch) haben.

II. Erscheinungsformen des Cyberangriffs

Das Mittel von Cyberangriffen sind Computerprogramme, die zu dem Zweck erschaffen werden, Störungen in Computersystemen herbei zu führen, um deren Funktionsfähigkeit zu beeinträchtigen. Dies kann auf vielfältige Weise vor sich gehen. In der Literatur wird dabei zwischen syntaktischen Angriffen („syntactic attacks“), die die Funktionsweise des Computersystems stören, semantischen Angriffen („semantic attacks“), die die übermittelten Informationen verfälschen, und so genannten gemischten Angriffen („mixed attacks“), die beide Komponenten beinhalten, unterschieden.[4] Programme, mit denen solche Angriffe durchgeführt werden, werden zum Beispiel Trojaner, logische Bomben oder Viren genannt.[5]

Derlei Angriffe können durch die Störung von Computersystemen verschiedenste Schäden verursachen. Denkbar sind der Ausfall der Energieversorgung oder des öffentlichen Nah- oder Fernverkehrs, die Beeinträchtigung der Wasser- und Abwasserversorgung oder der Telekommunikation; möglicherweise auch die Beschädigung oder Zerstörung der entsprechenden Leitungssysteme. Ebenfalls der Ausfall von militärischen Führungs- und Leitsystemen oder der Flugsicherung sind vorstellbar. Flugzeugabstürze oder der Tod von Patienten auf Intensivstationen in Krankenhäusern aufgrund fehlender Energie könnten direkte Folgen solcher Angriffe sein. Auch Schreckensszenarien wie das Herbeiführen der Kernschmelze in einem Atomkraftwerk sind denkbar.[6]

---

* Der Autor studiert Rechtswissenschaft und Ethnologie an der Rheinischen Friedrich-Wilhelms-Universität Bonn. Der Beitrag entstand anlässlich eines Seminars zum Völker- und Europarecht.

[1] *Carr*, Under Attack from Invisible Enemies, in: The Independant (UK), 20. Jan. 2010.

[2] *Jensen*, Texas Law Review 2010, 1522 (1541).

[3] *Gertz*, China blocks US from Cyber Warfare, in: The Washington Times (US), 12. Mai 2009.

[4] *Benatar*, Göttingen Journal of International Law 2009, 375 (378).

[5] *Schmitt*, NZWehrR 1999, 177 (178).

[6] *Schmitt*, NZWehrR 1999, 177 (179).

III. Der bewaffnete Angriff als Voraussetzung für das Selbstverteidigungsrecht des Art. 51 UN-Ch.

Gemäß Art. 51 UN-Ch haben Staaten im Falle eines bewaffneten Angriffs das Recht zur Selbstverteidigung. Der bewaffnete Angriff ist dabei als eine gesteigerte Form der Gewaltausübung zu verstehen, die in Art. 2(4) UN-Ch, im Rahmen des allgemeinen Gewaltverbots, allen Staaten untersagt ist. Ein näherer Blick auf den Begriff der Gewalt i.S.d. Art. 2(4) UN-Ch zeigt, dass dessen Reichweite keineswegs klar ist. Seit langem wird diskutiert, ob der Begriff der Gewalt so weit zu fassen sei, dass er auch rein wirtschaftliche Zwangsausübung noch umfasse, oder ob er so eng gefasst werden müsse, dass unter ihn nur die bewaffnete Gewalt zu subsumieren sei. Vor dem Hintergrund dieser Überlegungen wird überwiegend die Meinung vertreten, der Begriff der Gewalt sei irgendwo zwischen der rein wirtschaftlichen Zwangsmaßnahme und der Waffengewalt anzusiedeln. Betrachtet man die Struktur des Art. 51 UN-Ch, wird klar: „Not every use of force contrary to Art. 2(4) may be responded to with armed self defence.“[7] Vielmehr muss diese Gewalt i.S.d. Art. 2(4) zunächst eine bestimmte Schwelle überschreiten, damit der Anwendungsbereich des Art. 51 UN-Ch eröffnet wird.

IV. Überlegungen zu einem „modernen“ Begriff des bewaffneten Angriffs

Entscheidend ist schließlich die Frage, wie genau diese Schwelle zu bestimmen ist, ab der eine Gewaltmaßnahme auch als „bewaffneter Angriff“ angesehen werden kann. Ein wichtiger Anhaltspunkt, wann ein bewaffneter Angriff vorliegt, bietet die „Definition of Aggression“- Resolution[8] der Generalversammlung der Vereinten Nationen. Hierbei muss beachtet werden, dass im Rahmen dieser Resolution die Definition des „bewaffneten Angriffs („armed attack“) nicht beabsichtigt war, vielmehr ging es um eine Definition der Aggressionshandlung („act of aggression“) in Art. 39 UN-Ch.[9] Unabhängig von dieser Debatte ist in der Völkerrechtslehre unumstritten, dass die „Definition of Aggression“-Resolution insbesondere in ihrem Artikel 3 wertvolle Indikationen für das Vorliegen eines bewaffneten Angriffs liefert.[10]

Im direkten Nachgang zur Verabschiedung der Resolution äußerst sich bereits *Meier* zum Verhältnis der Resolution zum Begriff des bewaffneten Angriffs und versucht eine Definition. Demnach sei ein bewaffneter Angriff im Sinne des Völkerrechts „die Durchsetzung eines Ansinnens, welches ein Staat an einen anderen Staat richtet, unter Verletzung der Gebietshoheit des betroffenen Staates mittels Invasion oder Bombardierung, ohne dass dieses Verhalten eine Reaktion auf einen vorangegangen bewaffneten Angriff darstellt.“[11]

Diese Definition könnte man als „klassischen“ Angriffsbegriff bezeichnen. Er enthält zwei wesentliche Komponenten: Erstens wird eine Verletzung der Gebietshoheit angenommen, bei der entweder militärisches Personal oder Sprengkörper die Grenze zum angegriffenen Staat überschreiten. Zweitens wird vorausgesetzt, dass diese Verletzung der Gebietshoheit durch Waffen im konventionellen Sinne zu erfolgen habe, die im fremden Staatsgebiet zu Zerstörungen führen. Es ist fraglich, ob ein solcher Angriffsbegriff mit Blick auf moderne Bedrohungslagen nicht zu eng ist. Vielmehr dürfte es angezeigt sein, über die Einführung eines „modernen“ Angriffsbegriffs nachzudenken.

Nimmt man zunächst das Merkmal der Grenzverletzung in den Blick, so ist dieses insbesondere bei Fragen des Selbstverteidigungsrechts gegen Angriffe terroristischer Banden in Frage gestellt worden. So bemerkt etwa *Kreß* in seinem Standardwerk über Zurechnungsprobleme zu Staaten bei Gewaltakten Privater, dass „weder der Gewalteinsatz nach Art. 2(4) SVN noch der bewaffnete Angriff im Sinne des Art. 51 SVN grenzüberschreitende im Sinne von grenzverletzender Qualität aufweisen müssen.“[12] *Stein* und *Mahraun* schlagen in dieser Diskussion “eine teleologische Auslegung des Angriffsbegriffs i.S.d. Art. 51 UN-Ch“ vor dem Hintergrund von sog. „Informationsoperationen“ vor. Art. 51 UN-Ch diene im Grundsatz dem „Schutz der Souveränität, der territorialen Unversehrtheit und politischen Unabhängigkeit der Staaten“[13]. Legt man solche Überlegungen zugrunde, fällt es tatsächlich schwer bei einer akuten Bedrohung eben dieser Schutzgüter das doch eher formale und aus Vorstellung klassischer Kriegsführung entlehnte Merkmal der Grenzverletzung- bzw. Überschreitung zur Bedingung für einen bewaffneten Angriff zu machen. Vielmehr erscheint es für einen bewaffneten Angriff „nicht erforderlich, dass Truppen die Grenzen überschreiten.“[14]

Ähnlich verhält es sich mit dem Merkmal einer klassischen bewaffneten Gewalt mit konventionellen Waffen. Das Recht auf Selbstverteidigung stelle nach *Stein* und *Mahraun* letztlich nicht darauf ab „ob das Völkerrecht ein bestimmtes neues Einwirkungsmittel schon als ‚Waffe‘ klassifiziert hat, sondern [...] ob ein Staat und seine Einrichtungen, seine Souveränität, territoriale Unversehrtheit oder politische Unabhängigkeit in massiver Weise beeinträchtigt werden.“[15] Es kann nicht davon ausgegangen werden, dass nur ein mit Handfeuerwaffen, Bomben oder Granaten geführter Angriff ein ‚bewaffneter‘ wäre. „Bewaffnet auch im Kontext von Art. 51 SVN kann heute nur bedeuten, ausgerüstet zu sein mit einem Mittel, das geeignet ist, einen militärischen Vorteil gegenüber dem Gegner zu erzielen und dabei zu zerstören oder zu töten.“[16] Hierbei sei allerdings schon ein gewisses Maß an „physischer Zerstörung“[17] erforderlich.

---

[7] *Simma*, The Charta of the United Nations – A Commentary, Second Edition 2002, S. 790.

[8] UN-GA Res. 3314 (1974), RES/29/3314.

[9] *Simma*, Fn. 7, S. 795.

[10] *Simma*, Fn.7, S. 796.

[11] *Meier,* AVR 1975, 374 (378).

[12] *Kreß*, Gewaltverbot und Selbstverteidigungsrecht nach der Satzung der Vereinten Nationen bei staatlicher Verwicklung in Gewaltakte Privater, 1995, S. 340.

[13] *Stein/Mahraun*, ZaöRV 2000, 1 (5).

[14] *Blumenwitz*, BayVwBl 32 (1986), 373 (739).

[15] *Stein/Mahraun,* ZaöRV 2000, 1 (5).

[16] *Stein/Mahraun*, ZaöRV 2000, 1 (6).

[17] *Stein/Mahraun*, ZaöRV 2000, 1 (6).

Weiterhin ist es auch weitgehend unumstritten, dass unter einem bewaffneten Angriff i.S.d. Art. 51 UN-Ch. nur eine „militärische Angriffshandlung, die eine gewisse Intensität erreicht“,[18] verstanden werden kann. Schon in den Genfer Abrüstungskonferenzen von 1935 findet sich die Bemerkung, dass für ein Recht auf Selbstverteidigung eine kleinere Grenzstreitigkeit nicht genüge.[19] Dies kann als besondere Ausprägung des „de minimis lex non curat“-Grundsatzes angesehen werden.[20]

Vor dem Hintergrund dieser Überlegungen könnte man tatsächlich über die Einführung eines „modernen“ Begriffs des bewaffneten Angriffs nachdenken, der auch neuartigere Bedrohungslagen, wie eben Cyberangriffe, umfassen könnte. Dieser wäre in etwa:

Jede Angriffshandlung, die einen „Staat und seine Einrichtungen, seine Souveränität, territoriale Unversehrtheit oder politische Unabhängigkeit in massiver Weise beeinträchtigt“[21] und dabei ein im Staatsgebiet des angegriffenen Staates direkte „physische Zerstörung“[22] verursacht, wobei eine „gewisse Intensität“[23] erreicht wird.

Ein solcher „moderner“ Angriffsbegriff könnte geeignet sein, auch neue Mittel der Kriegsführung wie Cyberangriffe zu erfassen. Ob dies vor dem Hintergrund der methodischen Ansätze zur Einordnung von Cyberangriffen in die Systematik des Art. 51 UN-Ch vertretbar erscheint, soll im Folgenden untersucht werden.

V. Cyberangriffe als bewaffneter Angriff – Methodische Ansätze

Um unter den Begriff des bewaffneten Angriffs i.S.d. Art. 51 UN-Ch subsumiert werden zu können, muss es sich bei dem durchgeführten Cyberangriff um Gewalt i.S.d. Art. 2(4) UN-Ch handeln, welche die Schwelle zum bewaffneten Angriff überschreitet. In der Literatur, die sich innerhalb der letzten 10 Jahre herausgebildet hat, ist weitgehend unumstritten, dass Cyberangriffe unter bestimmten Bedingungen als bewaffneter Angriff i.S.d. Art. 51 UN-Ch eingestuft werden können. Wie diese Bedingungen genau aussehen und auf welche analytischen Grundlagen sich eine Einordnung stützen kann, wird allerdings kontrovers diskutiert.

Hierbei kann im deutschen Schrifttum wohl ein Ansatz als vorherrschend bezeichnet werden, der sich bei der Einordnung eines Cyberangriffs als bewaffneter Angriff tendenziell auf die Folgen des Angriffes bezieht. Dieser wirkungsbezogener Ansatz wird unten auch als Folgentheorie bezeichnet. Im amerikanischen Schrifttum scheinen eher zwei davon abweichende Ansichten vorherrschend zu sein. Die gemäßigtere von beiden stellt vorrangig auf die Art der betroffenen Systeme ab. Dieser Ansatz wird im Folgenden als Domänentheorie bezeichnet. Ein vorrangig in Kreisen des US-amerikanischen Militärs vertretener Ansatz unterscheidet sich in mehrerer Hinsicht von den beiden vorigen. Er versucht bestimmte Computerprogramme als Waffe zu klassifizieren, deren bewusster Einsatz einen bewaffneten Angriff darstelle. Dieser Ansatz wird unten auch als Instrumententheorie bezeichnet.

1. Wirkungs- oder folgenorientierter Ansatz (Folgentheorie)

Zunächst ist es denkbar, bei der Einordnung eines Cyberangriffes als bewaffneten Angriff auf die Wirkungen der in Rede stehenden Maßnahme abzustellen. Insoweit könnte ein Cyberangriff dann unter den Gewaltbegriff von Art. 2(4) UN-Ch. subsumiert werden, sofern sich seine Wirkungen so darstellen wie bei einem Angriff, der mit den traditionellen militärischen Waffen durchgeführt wird. „Ein Angriff, der speziell auf die unmittelbare physische Beschädigung materiellen Vermögens bzw. auf die Verletzung oder Tötung von Menschen abzielt, entspricht der Anwendung von Waffengewalt und wird von dem Gewaltverbot erfasst.“[24] Unter den Vertretern dieses Ansatzes ist hingegen umstritten, ob demgegenüber Cyberangriffe, die lediglich rein wirtschaftliche oder politische Folgen zeitigen, aus dem Anwendungsbereich des Art. 2(4) UN-Ch herausfallen.[25]

Dabei wird diskutiert, ob Maßnahmen, die beispielsweise den Zusammenbruch des Computersystems der Börse oder des nationalen Geldtransfersystems herbeiführen, einen bewaffneten Angriff i.S.d. Art. 51 darstellen können.[26] Auch kann fraglich sein, ob möglicherweise bereits die Ausschaltung der militärischen Führungs- und Verbindungssysteme einen bewaffneten Angriff darstellen könnte. Vorstellbar ist in diesem Zusammenhang beispielsweise die Ausschaltung der Marine und Luftwaffe durch eine Art „Digital Pearl Harbour“[27]. In beiden Fällen treten keine direkten physischen Zerstörungen ein, vielmehr entstehen im ersten Fall rein wirtschaftliche Schäden. Im zweiten Fall wird lediglich die Verteidigungsbereitschaft des angegriffenen Staates verringert, ohne dass es zu weiteren militä-

[18] *Blumenwitz*, BayVwBl 1986, 373 (379).

[19] IX Désarmément (1935) Conférence pour la réduction et limitation des arméments, IX, 4, Bd. 2, S. 684.

[20] Vgl. *Dinstein*, Computer Network Attacks and Self Defence, in: Computer Network Attack and International Law, Schmitt, Michael N/o‘Donnell, Brian T. (ed.), 2002.

[21] *Stein/Mahraun*, ZaöRV 2000, 1 (5).

[22] *Stein/Mahraun*, ZaöRV 2000, 1 (6).

[23] *Blumenwitz*, BayVwBl 1986, 373 (379).

[24] *Schmitt*, NZWehrR 1999, 177 (183).

[25] So etwa *Silver*, Computer Network Attacks as a Use of Force under Article 2(4) of the United Nations Charter, in: Computer Network Attack and International Law, *Schmitt*, *Michael N/o‘Donnell, Brian T.* (ed.), 2002, 85.

[26] Dafür *Sharp* Fn. 28, mit Einschränkungen *Silver* Fn. 25, *Schmitt* Fn. 5, wohl eher dagegen *Benatar* Fn. 32, *Stein/Mahraun* Fn. 13.

[27] *Talat*, Indian Journal of International Law 2006, 250.

rischen Handlungen käme. Dem Grunde nach steht hinter solchen Überlegungen die Frage nach der Reichweite des Gewaltbegriffs des Art. 2(4) UN-Ch.

Hierzu will beispielsweise *Sharp* schon jeden Cyberangriff, der „any destructive effect“[28] im fremden Staatsgebiet auslöse unter den Gewaltbegriff des Art. 2 (4) UN-Ch einordnen. Hierunter versteht er auch unter bestimmten Umständen rein wirtschaftliche Auswirkungen, wie zum Beispiel den durch einen Computerangriff herbeigeführten Zusammenbruch der Finanzmärkte.[29]

Den systematischen Versuch einer Ausweitung macht *Schmitt*[30]. Dabei schlägt er eine Bewertung von Maßnahmen anhand von sechs Kriterien (Härte, Unmittelbarkeit, Abhängigkeit, Eindringen in fremde Hoheitsgebiete, Messbarkeit und präsumtive Rechtmäßigkeit) vor, die eine Einordnung in den Gewaltbegriff von Art. 2(4) UN-Ch ermöglichen sollen. Dies sei gegenüber einer Einordnung nur mit Blick auf eingetretene physische Zerstörungen vorzugswürdig.[31] Die Brauchbarkeit dieser Kriterien wird allerdings aufgrund ihrer Vagheit[32] zu Recht kritisiert. Insbesondere *Silver* zeigt in eindrücklicher Weise, dass bei näherer Betrachtung und strenger Prüfung der von *Schmitt* aufgestellten Kriterien lediglich dasjenige der „Härte“ als tatsächlich unterscheidungserhebliches Kriterium übrig bleibt.[33] Hierdurch würde es also kaum ermöglicht, jenseits der tatsächlich eingetretenen physischen Zerstörungen objektive Kriterien auszumachen.

Nach der „Folgentheorie“ spielt es demnach für die Einordnung eines Angriffes als bewaffneten Angriff i.S.d. Art. 51 UN-Ch. keine Rolle, ob er auf konventionelle Weise oder als Cyberangriff erfolgt ist („From a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack.“[34]) Es komme vielmehr auf die gleichen oder ähnlichen Folgen des Angriffes an. („the same - or similar results“[35]) „Since a cyber attack is unlike a classic armed attack, the only way that a CNA [Computer Network Attack – Anm. d. Verf.] could activate Article 2(4) is if such an attack rose to the level of an armed attack, that is, to the same effect as an attack by traditional military forces.“[36] Hierbei spiele es im Rahmen einer dynamischen Auslegung keine Rolle, dass „the U.N. Charter anticipates such situations as the presence of troops and the use of traditional military weapons on another nation‘s territory, not simultaneous multimodal networks attacks on a state.“[37] Umstritten ist aber, ob nicht-physische, etwa wirtschaftliche, Folgen eines Angriffes, bereits eine Einordnung als bewaffneter Angriff i.S.d. Art. 51 UN-Ch erlauben.

2. Domänenorientierter Ansatz (Domänentheorie)

Ein weiterer, insbesondere im amerikanischen Schrifttum vertretener Ansatz versucht das Vorliegen von Gewalt nicht in Bezug auf die durch den Angriff eingetretenen Schäden zu bestimmen, sondern in Bezug auf die adressierten Computersysteme. Die President‘s Commission on Critical Infrastructure Protection (PCCIP) definiert für die USA acht kritische informationstechnische Infrastrukturen[38]. Diese sind Information und Kommunikation, Logistik und Transport, Energieversorgung, Bank- und Finanzwesen und kritische Komponenten des Gesundheitswesens.[39]

Creekman bezeichnet diese acht kritischen Infrastrukturen als vitale Angriffsziele („vital targets“), alle anderen Computersysteme als nicht-vitale Angriffsziele („non-vital targets“).[40] Aus dieser Unterscheidung bildet *Creekman* regelbeispielartige Fallgruppen, nach denen ein Angriff üblicherweise als Gewalt einzustufen sei: „In the case where the state-sponsored attack is directed against a vital computer system, the damage is likely to be of such magnitude so as to qualify the attack as a use of armed force.“[41] Es werden also klare Fallgruppen gebildet, nach denen - unabhängig vom tatsächlich eintretenden Schaden - das Gewaltverbot als berührt gilt, wenn solche Systeme betroffen werden, deren Beschädigung üblicherweise zu einem größeren Schaden führt.

Anforderungen an einen hierauf folgenden Schwellenübertritt hin zum bewaffneten Angriff werden allerdings nicht gestellt. Der Angriff, auf ein vitales Angriffsziel („vital target“), also ein solches, dessen Beschädigung wahrscheinlich („likely“) größeren Schaden verursacht, überschreitet mit der Gewaltschwelle des Art. 2(4) UN-Ch. zugleich auch die Schwelle zum bewaffneten Angriff i.S.d. Art. 51 UN-Ch. „This then triggers the victim State‘s right to respond with force in self-defence under Article 51 of the U.N. Charter.“[42]

Eines weiteren Schadenseintrittes bedarf es nicht: „It attempts, for the first time, to define acts designed to destabilize our (the United States‘, Anm. d. Verf.) eight most important infrastructure systems in terms of ‚aggression‘, with the concomitant right of self defence available as a lawful and effective response.“[43] Hier zeigt sich der we-

---

[28] *Sharp*, Cyberspace and the Use of Force,1999, 140.

[29] *Sharp*, Fn. 28, 102.

[30] *Schmitt*, NZWehrR 1999, 177 (184).

[31] *Schmitt*, NZWehrR 1999, 177 (185).

[32] *Benatar*, Göttingen Journal of International Law 2009, 375 (390).

[33] *Silver*, Fn. 25, S. 91.

[34] *Dinstein*, Fn. 20, S. 103.

[35] *Dinstein*, Fn. 20, S. 103.

[36] *Shackelford*, Berkeley Journal of International Law 2009, 191 (237).

[37] *Shackelford*, Berkeley Journal of International Law 2009, 191 (229).

[38] *Persico*, Commonlaw Conspectus 153 (1999), 156 (156).

[39] Übersetzung des Verfassers. Im englischen Original: „Information and Communications, Physical Distribution, Energy, Banking and Finance, and Vital Human Services“.

[40] *Creekman*, American University International Law Review 2002, 642 (656).

[41] *Creekman*, American University International Law Review 2002, 642 (671).

[42] *Creekman*, American University International Law Review 2002, 642 (671).

[43] *Terry*, Responding to Attacks on Critical Computer Infrastructu-

sentliche Unterschied zur Folgentheorie. Während im Rahmen der Folgentheorie bei einem bewaffneten Angriff ein Schaden auf fremdem Staatsgebiet in entsprechender Intensität auch tatsächlich eintreten muss, kommt es bei der Domänentheorie auf einen tatsächlich eintretenden Schaden nicht an. Es genügt vielmehr, dass ein Computersystem („vital target") angegriffen wird, dessen Störung typischerweise einen besonders intensiven Schaden nach sich zieht.

3. Instrumentenorientierter Ansatz (Instrumententheorie)

Der instrumentenorientierte Ansatz versteht sich als Versuch der Abgrenzung von den wirkungs- und folgenbasierten Ansätzen, indem er die Formen und Mittel des Angriffs selbst in den Blick nimmt. Er verweist vor allem auf Probleme der konkreten Handhabbarkeit der wirkungsbasierten Ansätze.

In einem jüngst erschienenen Sonderheft der United States Air Force Law Review zum Thema kritisiert *Todd*, dass bei einem Cyberangriff oft nicht unmittelbar erkennbar sei, ob dieser erhebliche Schäden anrichte oder nicht: „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."[44] Es bedürfe vielmehr eines klareren analytischen Ansatzes, um schnell und sicher im Interesse der nationalen Sicherheit eine eindeutige Einordnung vornehmen zu können, auf deren Basis die Gegenmaßnahmen geplant werden können. Er betont: „Asymmetric warfare may require asymmetric application of the law to provide the clarity and enforceability capable of promoting peace."[45]

Der wirkungsbezogene Ansatz („effect based analytical approach"[46]) werde – und das sei seine Schwäche – aus geschriebenen oder gewohnheitsrechtlichen Normen des Völkerrechts hergeleitet, die vor der Einführung der Massenproduktion und -benutzung von Computern entwickelt worden seien.[47] Bei einer jüngeren Norm, der Konvention über die Cyberkriminalität des Europarates von 2001[48], sei durchaus der Beginn, nicht hingegen die Folgen eines Cyberangriffes als analytischer Ansatzpunkt für die Kriminalitätsbekämpfung in den Blick genommen worden. *Todd* argumentiert, ein solcher strafrechtlicher Analyseansatz könne also auch bei der Beurteilung von Gewalt im Bereich des Völkerrechts von Vorteil sein.[49] Daher sei es unabdingbar, den Begriff der Waffe im Bereich der Cyberkriegsführung zu bestimmen. Der Gebrauch eben solcher Waffen sei es dann, der eine Einordnung unter den Gewaltbegriff des Art. 2(4) UN-Ch und letztlich auch unter den Begriff des bewaffneten Angriffs i.S.d. Art. 51 UN-Ch ermögliche.[50]

Hierbei stellt *Todd* auf eine Zusammenschau der entsprechenden Definitionen aus dem Bereich der nationalen und internationalen Regelungen im Bereich der Cyberkriminalität ab und kommt zu folgender Definition von Cyberwaffe: „Any capability, device, or combination of capabilities and techniques, which if used for its intended purpose, is likely to impair the integrity or availability of data, a program, or information located on a computer or information processing system."[51] Der Einsatz einer solchen Cyberwaffe zum Zwecke der Schädigung von Computersystemen stellt nach *Todd* Gewalt i.S.d. Art. 2(4) UN-Ch dar.

Zunächst stellt also der instrumentenorientierte Ansatz auf die Art des Angriffswerkzeuges ab und gibt eine Definition der Cyberwaffe. Dann wird ein subjektives Element in die Überlegungen eingeführt, indem auf die Motivlage desjenigen abgestellt wird, der das zerstörerisch wirkende Computerprogramm einsetzt. Setzt der Angreifer also wissentlich und willentlich eine Cyberwaffe ein, um Computersysteme zu beschädigen, handelt es sich um Gewalt i.S.d. Art. 2(4) UN-Ch. So kann die Instrumententheorie, im Gegensatz zu den beiden vorigen Theorien, auch als subjektive Theorie bezeichnet werden. Der Begriff des bewaffneten Angriffs erhält gleichsam einen objektiven (Einsatz der Cyberwaffe) und einen subjektiven Tatbestand (wissentlicher und willentlicher Einsatz).

In der Bestimmung, wann bei einem Cyberangriff ein bewaffneter Angriff vorliegt, verzichtet die Instrumententheorie auf ein Abstellen auf die Größe des eintretenden Schadens. „Therefore, in order to determine when the use of a cyberspace weapon constitutes an ‚armed attack' under international law, one must look to how the cyberspace weapon is used rather than its effects."[52] Vielmehr kommt es nach der Instrumententheorie darauf an, ob das als Cyberwaffe klassifizierte Programm, das üblicherweise zur Störung von Computersystemen zum Einsatz kommt, auch zu eben diesem Zweck eingesetzt wird (objektiver Tatbestand) und dies auch vorsätzlich geschieht (subjektiver Tatbestand). Hierbei lässt *Todd* auch den dolus eventualis genügen, also das bloße Wissen und In-Kauf-Nehmen der schädlichen Folgen des Einsatzes: „A cyberspace attack occurs when a state knowingly uses or knowingly acquiesces to an entity under its legal control or within its territory using a cyberspace weapon against the people or property of another state."[53]

re, in: in: Computer Network Attack and International Law, Schmitt, Michael N/o'Donnell, Brian T. (ed.), 2002, S. 435.

[44] *Todd*, The Air Force Law Review, 2010, 65 (74).

[45] *Todd*, The Air Force Law Review, 2010, 65 (77).

[46] *Todd*, The Air Force Law Review, 2010, 65 (69).

[47] *Todd*, The Air Force Law Review, 2010, 65 (70).

[48] Convention on Cybercrime**,** 2296 U.N.T.S, Budapest, 23.XI.2001, Council of Europe.

[49] *Todd*, The Air Force Law Review 2010, 65 (79).

[50] *Todd*, The Air Force Law Review 2010, 65 (79).

[51] *Todd*, The Air Force Law Review 2010, 65 (83).

[52] *Todd*, The Air Force Law Review, 2010, 65 (86).

[53] *Todd*, The Air Force Law Review, 2010, 65 (87).

VI. Stellungnahme zu den verschiedenen Ansätzen

Die Instrumententheorie will sich auf eine strafrechtliche Logik stützen. Es wird behauptet, im Strafrecht werde bereits der Beginn einer Handlung in den Blick genommen, um ein frühes Einschreiten der Gesellschaft zu ermöglichen. Für das Strafrecht sei es ineffektiv auf den eingetretenen Schaden am Rechtsgut zu rekurrieren. [54]

Tatsächlich setzen die meisten strafrechtlichen Normen einen Erfolgseintritt voraus. Strafnormen, die ein Verhalten als strafwürdig einstufen ohne dass es auf den Erfolgseintritt ankäme, werden als abstrakte Gefährdungsdelikte bezeichnet und sind eher die Ausnahme. Zudem werden im Schrifttum gegen die abstrakten Gefährdungsdelikte verfassungsrechtliche Bedenken erhoben, da es unter dem Blickwinkel des Schuldprinzips und des Verhältnismäßigkeitsgrundsatzes staatlichen Handelns zumindest bedenklich erscheint, einem Täter ein tatsächlich ungefährliches Verhalten als abstrakt gefährlich zuzurechnen.[55]

Ähnliche Bedenken, wenn auch mit anderer Stoßrichtung, sind auch auf völkerrechtlicher Ebene anzubringen. Es erscheint kaum vertretbar, dass ein potentiell gefährliches Verhalten, dass allerdings zu keinerlei Schaden geführt hat, bereits den Begriff der Gewalt i.S.d. Art. 2(4) UN-Ch. erfüllen soll. Die UN-Ch will die Staaten in ihrer Souveränität schützen, die in einem solchen Falle nicht tatsächlich, sondern nur potentiell in Gefahr ist.

Jedenfalls erscheint es kaum vertretbar, in solchen Fällen schon einen bewaffneten Angriff i.S.d. Art. 51 UN-Ch anzunehmen. Vorrangiges Ziel des Gewaltsystems der Charta ist es, kriegerische Eskalation zu verhindern. Nur wenn die Gewalt bereits eskaliert ist, soll das Selbstverteidigungsrecht greifen. Ob dies auch schon bei einem Cyberangriff angenommen werden kann, der zwar potentiell gefährlich war, in Wahrheit aber keine Schäden angerichtet hat, ist höchst zweifelhaft.

Die Instrumententheorie nimmt weiterhin für sich in Anspruch im Gegensatz zu den folgenbasierten Ansätzen ein klares Schema zu liefern, mit dem eine Einordnung als unerlaubte Gewalt und zugleich bewaffneter Angriff vorgenommen werden kann. Es darf aber hinterfragt werden, ob das „klare Schema" der Instrumententheorie die in der Realität bestehenden Beweisprobleme aufwiegen kann, die sie gleichzeitig aufwirft. Es dürfte auf den ersten Blick weder erkennbar sein, ob ein Computerprogramm eine Waffe darstellt, noch in welchem Staat die „Cyberwaffe" entwickelt oder zum Einsatz (etwa durch das Internet) losgeschickt wurde.

Es darf bezweifelt werden, ob der methodische Ansatz der „Verstrafrechtlichung" des Völkerrechts in der Frage des Selbstverteidigungsrechts wirklich weiter führt. Ein solcher Ansatz muss immer mit subjektiven Tatbeständen und potentiellen Gefahren operieren. Dies sind gerade in Zeiten von Cyberkriegsführung kaum beweisbare Merkmale. Zwar ist das Bestreben verständlich, in Zeiten asymmetrischer Kriegsführung zu einem effektiven Einsatz des Selbstverteidigungsrechts zu kommen. Allerdings führt ein in Anspruch genommenes Selbstverteidigungsrecht der Staaten, obwohl für die Weltöffentlichkeit erkennbar nichts Schädliches im Rahmen eines Angriffes passiert ist, zu einer allgemeinen rechtlichen Verunsicherung und zu einem Infragestellen des Gewaltverbots; zumal die Missbrauchsgefahr immens gesteigert wird.

Ähnliche Argumente sind auch gegen die Domänentheorie vorzubringen, die wohl auch die dogmatisch schwächste der dargelegten Ansätze darstellt. Eine Einteilung in kritische und nicht-kritische Computersysteme berücksichtigt nur unzureichend die Genese eines Cyberangriffes. In der Realität besteht eine derartige Vernetzung aller zivilen und militärischen Computersysteme mit den genannten acht kritischen Infrastrukturen, dass deren Isolierung in der Praxis kaum möglich ist. Tatsächlich werden im Rahmen von Cyberangriffen auch „Angriffsrouten" gewählt werden, die über nicht kritische Systeme in die kritischen Systeme führen. In der Praxis läuft die Domänentheorie also – wie übrigens auch die Instrumententheorie – darauf hinaus, dass jeder Cyberangriff auf die Computersysteme eines Staates, unabhängig vom eintretenden Schaden, das Selbstverteidigungsrecht auslöst. Eine solche Lösung kann im Ergebnis nur als Überspannung des Selbstverteidigungsrechts eingestuft werden.

Letztlich muss *Silver* Recht gegeben werden, wenn er bemerkt: „The one basis that seems most reliable is that physical injury or property damage must arise as a direct and foreseeable consequence of the CNA and must resemble the injury or damage associated with what, at the time, are military weapons."[56] Es ist also nicht richtig, den Cyberangriff selbst, unabhängig vom eintretenden Schaden, als bewaffneten Angriff i.S.d. Art. 51 UN-Ch. zu qualifizieren. „The Computer Network Attack itself is only an instrument to carry out that attack in the same way that any other weapon would be."[57]

Der bewaffnete Angriff besteht nicht im Einsatz einer bestimmten Waffe, wie bei der Instrumententheorie oder in der Adressierung eines bestimmten Ziels wie bei der Domänentheorie, sondern im Zusammenwirken von Mitteleinsatz, Zielauswahl und Schaden. Erst wenn der schädigende Erfolg auch tatsächlich eingetreten ist, kann von einem bewaffneten Angriff gesprochen werden. Nur in solchen Fällen kann von einer Gewalteskalation ausgegangen werden, die so schwerwiegend ist, dass der betroffene Staat nicht mehr auf Gegenmaßnahmen der Weltgemeinschaft (etwa des UN-Sicherheitsrats im Rahmen von Ka-

[54] *Todd*, The Air Force Law Review, 2010, 65 (79).

[55] *Kindhäuser*, Strafrecht Besonderer Teil I, 4. Auflage 2009, § 48, Rn. 7.

[56] *Silver*, Fn. 25, S. 92.

[57] *Shackelford*, Berkeley Journal of International Law 2009, 191 (231).

pitel VII der UN-Ch) zu warten braucht, sondern selbst zu seinem Schutze handeln darf.

In dieser Logik ist es auch kaum nachvollziehbar, bereits in der Störung oder Ausforschung militärischer Computersysteme einen bewaffneten Angriff i.S.d. Art. 51 UN-Ch. zu sehen. „Für die völkerrechtliche Bewertung ist zunächst die Intention maßgeblich, gegebenenfalls das Ausmaß des jenseits der Informationssysteme eingetretenen Schadens, nicht aber primär die Ausforschung oder Störung der 'gegnerischen Informationsinfrastruktur' als solcher."[58]

Es bleibt zu klären, wie es mit der Einordnung von Cyberangriffen mit rein wirtschaftlichen Folgen als bewaffnete Angriffe aussieht, obwohl keine physische Schäden verursacht wurden. Vor dem Hintergrund der momentan für jeden spürbaren Auswirkungen der weltweiten Wirtschafts- und Finanzkrise erscheint eine solche Einordnung auf den ersten Blick nachvollziehbar.

Nichtsdestoweniger dürfte eine derartige Ausdehnung des Gewaltbegriffs eine Überspannung des oben bereits herausgearbeiteten Gehaltes von Art. 2(4) UN-Ch darstellen. Dieser erfasst weitgehend unumstritten keine Wirtschafts- und Handelsboykotte. Auch solche haben massive Auswirkungen auf den betroffenen Staat und damit auf die Lebensverhältnisse der Menschen. Dies kann in letzter Konsequenz und bei entsprechender Härte des Boykotts auch zu physischen Zerstörungen durch Plünderungen oder auch zu durch Hunger getöteten Staatsbürgern führen. Diese Folgen treten allerdings nur mittelbar ein. Ziel des Gewaltverbotes der UN-Ch ist in erster Linie ein Verbot derjenigen Gewalt, die „gewöhnlich zu irgendeiner Form der physischen Zerstörung oder Verletzung" führt, weil bei bewaffneter Gewalt, „das Risiko einer Konflikteskalation [...] viel höher ist als im Falle wirtschaftlicher oder politischer Zwangsmaßnahmen", da „die Folgen der Gewaltanwendung fast unverzüglich sichtbar werden."[59] Insoweit kann ein Cyberangriff, der nicht direkt zu einer physischen Zerstörung führt, sondern nur rein wirtschaftliche, auch erhebliche, Auswirkungen hat, nicht unter den Gewaltbegriff des Art. 2(4) UN-Ch und damit auch nicht unter denjenigen des bewaffneten Angriffs i.S.d. Art. 51 UN-Ch gefasst werden.

Nimmt man nun erneut den oben angeführten „modernen" Angriffsbegriff in den Blick, so erscheint dieser als geeignet, auch den Anforderungen an Cyberangriffe zu entsprechen. Danach stellt jede Angriffshandlung, die einen „Staat und seine Einrichtungen, seine Souveränität, territoriale Unversehrtheit oder politische Unabhängigkeit in massiver Weise beeinträchtigt"[60] *und dabei ein im Staatsgebiet des angegriffenen Staates direkte „physische Zerstörung"*[61] *verursacht, wobei eine „gewisse Intensität"*[62] *erreicht wird einen bewaffneten Angriff i.S.d. Art. 51 dar*. Dieser „moderne" Angriffsbegriff ist weiter als der „klassische" Begriff des bewaffneten Angriffs, weil er auf die Merkmale der Grenzüberschreitung und den konventionellen Waffeneinsatz verzichtet. Es bleibt aber das Merkmal, dass physische Zerstörungen von gewisser Intensität erforderlich sind, unverzichtbar.

VII. Abschließende Überlegungen

Cyberangriffe können durchaus Gewalt i.S.d. allgemeinen Gewaltverbots des Art. 2(4) UN-Ch darstellen und die Schwelle zum bewaffneten Angriff überschreiten. Maßgabe ist hierbei der entstehende Schaden im Sinne einer Folgen- bzw. Wirkungstheorie. Ansätze, die in pauschalisierender Weise die Angriffsart selbst oder das adressierte Ziel zur Maßgabe einer solchen Einordnung machen, und dabei auf das Kriterium eines tatsächlichen Schadenseintritts verzichten, können letztlich nicht überzeugen, sondern stellen eine Überdehnung des in Art. 51 UN-Ch garantierten Selbstverteidigungsrechts dar.

Vorzugswürdig ist daher ein „moderner" Begriff des bewaffneten Angriffs, der insofern gegenüber dem „klassischen" einen weiteren Anwendungsbereich aufweist, als dass er auf die Merkmale der Grenzüberschreitung und des konventionellen Waffeneinsatzes verzichtet, allerdings auf das Herbeiführen physischer Schäden abstellt. Bloß wirtschaftliche Schäden genügen für die Klassifizierung als bewaffneter Angriff hingegen nicht.

Im Rahmen der internationalen Sicherheitspolitik ist das Thema Cyberkrieg längst auf der Agenda. So fanden Passagen zur Verteidigung gegen Cyberangriffe auch Eingang in das erneuerte strategische Konzept der NATO. Umso wichtiger werden Überlegungen in Bezug auf eine klare Begriffsbestimmung, wann bei einem Cyberangriff von einem das kollektive Selbstverteidigungsrecht auslösenden bewaffneten Angriff auszugehen ist. Diese Entwicklung sollte weiter beobachtet und kritisch begleitet werden. Es lassen sich leicht praktische Einwände gegen die an vielen Stellen und auch in diesem Beitrag vorgebrachten Restriktionen erheben, die sich im Rahmen des konkreten Verteidigungsfalls für den angegriffenen Staat ergeben. Entscheidend muss aber letztlich immer eine Gesamtabwägung aller völkerrechtlichen Gesichtspunkte bleiben, die auch über die legitimen Sicherheitsinteressen einzelner Staaten hinaus gehen können.

---

[58] *Stein/Mahraun*, ZaöRV 2000, 1 (2).

[59] *Schmitt*, NZWehrR 1999, 177 (183).

[60] *Stein/Mahraun*, ZaöRV 2000, 1 (5).

[61] *Stein/Mahraun*, ZaöRV 2000, 1 (6).

[62] *Blumenwitz*, BayVwBl 1986, 373 (379).