VÖLKERRECHTLICHE FRAGEN IM CYBER- UND INFORMATIONSRAUM

Verteidigungsausschuss des Deutschen Bundestages,
Öffentliche Anhörung, 14. Dezember 2020

Prof. Dr. iur. Wolff Heintschel von Heinegg,
Europa-Universität Viadrina, Frankfurt (Oder)

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)941
08.12.2020 - 19/3494
5410

Vorbemerkung

Zum Begriff des Cyberraums

Die besonderen Charakteristika des Cyberraums – Interkonnektivität und Ubiquität – verleiten mitunter dazu, den Cyberraum als virtuellen Raum zu verstehen, der sich scheinbar einer Anwendung traditioneller (völker-)rechtlicher Regeln und Prinzipien entzieht. Die damit einhergehende Mystifizierung des Cyberraums sollte jedoch unbedingt vermieden werden. Zu diesem Zweck bietet es sich an, auf allgemeine Definitionsversuche zu verzichten und sich stattdessen der auch von den U.S. Joint Chiefs of Staff verwendeten Beschreibung nach Maßgabe des – vereinfachenden, gleichwohl hilfreichen – sog. 3-Ebenen-Modells zu bedienen, wonach der Cyberraum aus einem physikalischen Netzwerk (unterseeische Kommunikationskabel, Leitungen, Server etc.), einem logischen Netzwerk (u.a. Protokolle) sowie einer personalen Ebene (Nutzer und Cyber-persona, z.B. IP-Adresse) besteht, wobei diese drei Ebenen sich gegenseitig bedingen.[1]

Zum Begriff der Cyber-Operation

Nicht jeder Rechnereinsatz oder jede Nutzung des Cyberraums ist als völkerrechtlich relevante Cyber-Operation einzuordnen. Vielmehr sollte der Fokus auf Operationen liegen ‚that involve the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace'.[2] Als Beispiel einer solchen Cyber-Operation, mit der Ziele im oder durch den Cyberraum erreicht werden sollen, kann genannt werden: ‚use of computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.'[3] Folglich sollen allein solcher Cyber-Operationen in den Blick genommen werden, die Wirkungen im oder durch den Cyberraum zeitigen oder zu zeitigen bestimmt sind. Operationen durch den Cyberraum zeichnen sich dadurch aus, dass sich ihre Wirkungen in der physischen Domäne materialisieren. Demgegenüber verbleiben die Wirkungen von Cyber-Operationen im Cyberraum innerhalb des Cyberraums.

[1] Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, S. I-2 ff. (Joint Publication 3-12, 8 June 2018), abrufbar unter: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[2] U.S. Department of Defense, Law of War Manual (June 2015, updated December 2016), Abs. 16.1.1, abrufbar unter: https://www.hsdl.org/?view&did=797480.
[3] Ebd.

Es sei jedoch darauf hingewiesen, dass mit der Einordnung als Cyber-Operation weder eine völkerrechtliche Wertung noch eine Einordnung als Angriff im völkerrechtlichen Sinne einhergeht.

I. Cyber-Operationen als Anwendung von Gewalt oder bewaffneter Angriff

In den verschiedenen nationalen Cyber-Sicherheitsstrategien wird der Begriff des ‚Cyber-Angriffs' in einem denkbar weiten Sinne verwendet. Davon erfasst werden sollen etwa 'deliberate acts that seriously compromise national security, stability or prosperity by manipulating, denying access to, degrading or destroying computers or networks or the information resident on them'.[4] Während mitunter zwischen Cyber-Angriffen und anderen maliziösen Cyber-Operationen unterschieden wird[5], darf mit Blick auf dieses weite Verständnis nicht unberücksichtigt bleiben, dass die nationalen Cyber-Sicherheitsstrategien alle erdenklichen Bedrohungen im oder durch den Cyberraum zu erfassen versuchen, einschließlich der organisierten Kriminalität, Cyber-Spionage und schädigende Cyber-Operationen, wie den STUXNET-Angriff gegen die iranische Anreicherungsanlage. Folglich rechtfertigen sie nicht die Schlussfolgerung, alle von ihnen behandelten maliziösen Cyber-Operationen stellten eine Anwendung von Gewalt i.S. von Art. 2 Abs. 4 UN-Charta oder gar einen das Selbstverteidigungsrecht auslösenden bewaffneten Angriff i.S. von Art. 51 UN-Charta dar.

Allerdings kann festgehalten werden, dass sich die Staaten der durch die zunehmende Abhängigkeit zahlreicher Bereiche vom Cyberraum selbst geschaffenen Schadenanfälligkeit hinreichend bewusst sind, so dass sie heute bereit sind, Cyber-Operationen, die signifikante Wirkungen[6] zeitigen, als Anwendung von Gewalt und, soweit diese mit Blick auf ihr Ausmaß und Effekte hinreichend gravierend sind, als das Selbstverteidigungsrecht auslösende bewaffnete Angriffe anzusehen. Diese – recht allgemeine – Einordnung steht insoweit in grundsätzlichem Einklang mit der Rechtsprechung des Internationalen Gerichtshofs (IGH), als das Gewaltverbot und das Selbstverteidigungsrecht nicht auf bestimmte Einsatzmittel begrenzt werden können, sondern Anwendung finden auf ‚any use of force, regardless of the

---

[4] Australian Government, *Australia's Cyber Security Strategy* (2016), S. 15 (2016), abrufbar unter: https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf (last visited on 11 October 2019). Siehe auch Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (2016), abrufbar untert: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, in der auf S. 14 ein Cyber-Angriffe definiert wird als 'IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised.' Vgl. ferner further Public Safety Canada, *National Cyber Security Strategy* (2018), abrufbar unter: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf, in der auf S. 33 ein Cyber-Angriff definiert wird als 'an attack that involves the unauthorized use, manipulation or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information.'

[5] Cyber Security Agency of Singapore, *Singapore's Cybersecurity Strategy* (2016), S. 25, abrufbar unter: https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf.

[6] U.S. Department of Defense, *The DoD Cyber Strategy* (April 2015), S. 5, abrufbar unter: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

weapons employed.'[7] Entscheidend kommt es darauf an, ob eine Cyber-Operation dazu bestimmt ist, Tod, Verletzung, Schaden oder Zerstörung zu verursachen, oder diese Wirkungen tatsächlich zeitigt. Das ist zweifellos zu bejahen, wenn die Wirkungen denen eines Einsatzes konventioneller Mittel und Methoden der Kriegführung gleichen, was dann der Fall sein wird, wenn sie sich außerhalb des Cyberraums, mithin in der physischen Domäne, materialisieren. Schwieriger einzuordnen sind Cyber-Operationen, deren Wirkungen auf den Cyberraum beschränkt bleiben.

1. Cyber-Operationen mit Wirkungen außerhalb des Cyberraums (Operationen durch den Cyberraum) und Selbstverteidigungsrecht

a) Cyber-Operationen als Bestandteil einer traditionellen Gewaltanwendung

Eine Cyber-Operation durch den Cyberraum kann sich als Teil einer zusammengesetzten Handlung darstellt, die darauf gerichtet ist, schädigende kinetische Wirkungen zu verursachen. Beispielsweise kann eine Cyber-Operation Teil eines traditionellen militärischen Angriffs sein, wie etwa der israelische Angriff auf eine syrische Nukleareinrichtung im Jahr 2007, dem angeblich eine Cyber-Operation gegen die syrische Luftabwehr vorausging. [8] Derartige Cyber-Operationen können daher als Teile einer zusammengesetzten Handlung angesehen werden, die zusammengenommen mit dem Einsatz traditioneller Mittel der Kriegführung als Gewaltanwendung oder bewaffneter Angriff eingeordnet werden kann oder aber als bloße Vorbereitungshandlung. Insoweit bestehen folglich keine nennenswerten völkerrechtlichen Einordnungsschwierigkeiten.

b) Eigenständige Cyber-Operationen

Cyber-Operationen durch den Cyberraum, die nicht (notwendige) Bestandteile einer traditionellen Gewaltanwendung sind, können darauf gerichtet sein, dem Einsatz traditioneller Schädigungsmittel vergleichbare Wirkungen zu zeitigen, indem sie Objekte außerhalb des Cyberraums (oder die physikalische Infrastruktur des Cyberraums) beschädigen oder zerstören. Auch Personen können durch Cyber-Operationen verletzt oder getötet werden, wenn etwa die Cyber-Infrastruktur eines Krankenhauses angegriffen wird und dadurch lebenserhaltende Maßnahmen nicht mehr durchgeführt werden können. In nationalen Cyber-Sicherheitsstrategien werden auch derartige Cyber-Operationen behandelt, ohne sie jedoch als das Selbstverteidigungsrecht auslösende bewaffnete Angriffe einzuordnen. So betont beispielsweise das U.S. Department of Defense seine Bereitschaft, ‚to defend the nation against cyberattacks of significant consequence'[9], jedoch erlaubt die Verwendung des Verbs ‚to defend' nicht notwendigerweise die Schlussfolgerung, derartige Cyber-Operationen würden stets als bewaffnete Angriffe angesehen. Auch das Handbuch des U.S. Department of Defense begnügt sich mit einer recht allgemeinen und daher wenig hilfreichen Feststellung:

---

[7] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1998, ICJ Reports 1998, 226-267, 224, Abs. 39.

[8] Vgl. D.E. Sanger / M. Mazzetti, 'Israel Struck Syrian Nuclear Project, Analysts Say', The New York Times, October 14, 2007, abrufbar unter: https://www.nytimes.com/2007/10/14/washington/14weapons.html.

[9] U.S. Department of Defense, The DoD Cyber Strategy (Fn. 6), S. 3.

> ‘A State’s inherent right of self-defense, recognized in Article 51 of the Charter of the United Nations, may be triggered by cyber operations that amount to an armed attack or imminent threat thereof.’[10]

Weitere Stellungnahmen erlauben aber eine deutlichere Einordnung. Die U.S. Joint Chiefs of Staff weisen darauf hin, dass Cyber-Operationen ‚are often employed with little or no associated physical destruction‘, betonen aber auch, dass ‚modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domain.’[11] Der damalige Rechtsberater des U.S. Department of State stellte 2012 fest, dass ‚cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force’[12], so dass u.a. die folgenden Cyber-Operationen als Anwendung von Gewalt und, bei hinreichender Schwere, bewaffnete Angriffe eingeordnet warden könnten:

> ‘(1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes.’[13]

Für Koh entspricht es gesundem Menschenverstand, Cyber-Operationen, deren physische Wirkungen denen traditioneller Mittel der Kriegführung gleichkommen als Gewaltanwendung einzuordnen, so dass das Selbstverteidigungsrecht eines Staates durch ‚computer network activities that amount to an armed attack or imminent threat thereof’[14] ausgelöst werden kann.

Eine vergleichbare Position hat der britische General-Anwalt vertreten:

> ‘[…]. the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter.
> If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

[10] U.S. Department of Defense, *Law of War Manual* (Fn. 2) Abs. 16.3.
[11] Joint Chiefs of Staff, Cyberspace Operations (Fn. 1), S. II-11.
[12] Harold H. Koh,’ International Law in Cyberspace’, 54 Harvard International Law Journal – Online (December 2012), 1-12, 4, abrufbar unter: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=5858&context=fss_papers.
[13] Ebd.
[14] Ebd.

> Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.'[15]

Schließlich wird auch in der südkoreanischen Cyber-Sicherheitsstrategie ausdrücklich die Möglichkeit betont, dass bestimmte Cyber-Operationen Wirkungen zeitigen können, die denen traditioneller bewaffneter Angriffe gleichstehen.[16]

Diese und vergleichbare Stellungnahmen eignen sich nicht notwendigerweise zum Nachweis einer allgemeinen Staatenpraxis oder einer Rechtsüberzeugung, die für die Geltung einer entsprechenden Gewohnheitsrechtsnorm (oder allgemein anerkannten Interpretation) erforderlich sind. In diesem Zusammenhang sind die folgenden Faktoren zu berücksichtigen: (1) Nationale Cyber-Sicherheitsstrategien beruhen auf einem integrierten Ansatz, der die Staaten in die Lage versetzen soll, auf das gesamte Spektrum von Cyber-Bedrohungen zu reagieren, so dass das Selbstverteidigungsrecht lediglich eine unter mehreren Optionen darstellt. (2) Einige Staaten scheuen sich, das Selbstverteidigungsrecht ausdrücklich in Bezug zu nehmen. Dies mag innenpolitischen Erwägungen geschuldet sein (wie etwa im Falle Deutschlands) oder dem starken Fokus auf den Schutz der eigenen Volkswirtschaft und der öffentlichen Ordnung (wie im Falle Singapurs). Gleichwohl ist davon auszugehen, dass solche und auch andere Staaten eine Gewaltanwendung oder – bei hinreichender Schwere – einen bewaffneten Angriffs bejahen würden, wenn sie Ziel einer maliziösen Cyber-Operation werden, deren Wirkungen in der physischen Domäne denen des Einsatzes traditioneller Mittel und Methoden der Kriegführung gleichkommen.

Bei bewaffneten Angriffen mit traditionellen Mitteln und Methoden der Kriegführung besteht mittlerweile weitgehende Einigkeit, dass eine Ausübung des Selbstverteidigungsrechts nicht erst dann zulässig ist, wenn sich die Schäden materialisieren. Ausreichend ist es, wenn dies unmittelbar bevorsteht, weil der Angreifer aller erforderlichen Schritte unternommen hat. In diesem Zusammenhang bestehen zwar insoweit einige semantische Verwirrungen, als die Einordnung der Selbstverteidigung als ‚präventiv', ‚präemptiv', ‚antizipatorisch', oder ‚interzeptiv' mehr Fragen aufwirft als zur Klärung beiträgt. Gleichwohl kann festgehalten werden, dass ein Staat nicht bis zum Schadenseintritt abwarten muss. Angesichts der hohen Geschwindigkeit des Datentransfers ist es jedoch durchaus schwierig, einen unmittelbar bevorstehenden Cyber-Angriff festzustellen, ohne dass es bereits zu Schäden gekommen ist. Auch die bloße Implementierung einer maliziösen Software ist nicht unbedingt ausreichend, um von einem unmittelbar bevorstehenden bewaffneten Angriff ausgehen zu können. Anders verhält es sich jedoch im Falle von Angriffszielen, die der kritischen Infrastruktur – z.B. Energieversorgung, Gesundheitssystem – zugerechnet werden können, da ein Abwarten des Schadenseintritts zu weitreichenden, nicht zumutbaren Konsequenzen führen würde. Darauf wird unter I. 2. Zurückzukommen sein.

---

[15] Attorney General Jeremy Wright, Cyber and International Law in the 21st Century, Speech delivered on 23 May 2018, available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (last visited on October 7, 2019).

[16] National Security Office (South Korea), National Cybersecurity Strategy, S. 6. Diese ist unmittelbar als pdf-Datei abrufbar.

c) Zusammengesetzte Handlung

Schließlich sei nochmals auf das auch von der Völkerrechtskommission der Vereinten Nationen anerkannte Konzept der zusammengesetzten Handlung (‚composite act') eingegangen.[17] Es ist durchaus möglich, dass eine Reihe von Cyber-Operationen nicht einzeln, aber in ihrer Gesamtheit Wirkungen zeitigen, die denen des Einsatzes traditioneller Schädigungsmittel gleichkommen. Beispielsweise kann durch eine Cyber-Operation eine sog. Hintertür im Zielsystem geschaffen werden, die es dem Angreifer erlaubt, sich jederzeit Zugang zu verschaffen, etwa um zu einem späteren Zeitpunkt eine Schadsoftware zu installieren, die dann Schäden oder Zerstörungen in der physischen Domäne verursacht, wie etwa Flugzeugabstürze, weil die Flugzeuge nicht mehr von einem Luftverkehrsleitsystem geführt werden können. In diesem Fall ist das Installieren der Hintertür Teil einer zusammengesetzten Handlung, die in ihrer Gesamtheit eine Anwendung von Gewalt bzw. einen bewaffneten Angriff darstellen kann.

d) Zwischenergebnis

Cyber-Operationen, deren Wirkungen sich außerhalb des Cyberraums materialisieren und die Tod, Verletzung, Schäden oder Zerstörungen zeitigen oder zu zeitigen geeignet sind, können als gegen den Zielstaat gerichtete Gewaltanwendung angesehen werden. Sind die Konsequenzen mit Blick auf ihre Wirkungen und ihr Ausmaß von hinreichender Schwere, sind diese Cyber-Operationen bewaffnete Angriffe, die das Selbstverteidigungsrecht des Opfers auszulösen geeignet sind. Das Opfer derartiger Angriffe ist nicht zu einer gleichartigen Reaktion verpflichtet, sondern kann sich auch für den Einsatz traditioneller Wirkmittel entschließen, solange die Schranken des Selbstverteidigungsrechts – Erforderlichkeit, Verhältnismäßigkeit, Unmittelbarkeit – gewahrt bleiben.

2. Cyber-Operationen, deren Wirkungen auf den Cyberraum beschränkt bleiben (Cyber-Operationen im Cyberraum)

Es besteht noch keine allgemeine Einigkeit, ob und unter welchen Voraussetzungen Cyber-Operationen im Cyberraum als Anwendung von Gewalt oder bewaffneter Angriff eingeordnet werden können. Erinnert sei in diesem Zusammenhang an die im Jahr 2007 gegen Estland gerichteten DDoS-Angriffe, die trotz ihrer weitreichenden Auswirkungen auf den öffentlichen und Finanzsektor nicht als bewaffnete Angriffe i.S. von Art. 5 des NATO-Vertrags angesehen wurden. Zu berücksichtigen ist zudem, dass Daten bislang noch nicht Objekten gleichgestellt werden können, so dass das Löschen von Daten als solches nicht als Zufügung eines materiellen Schadens eingeordnet werden kann. In diesem Zusammenhang ist auch zu berücksichtigen, dass dem Völkerrecht ein Verbot der Cyberspionage fremd ist – da wohl alle

[17] Vgl. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83 vom 28. Januar 2002. Art. 15 der Entwurfsartikel lautet:

(1) The breach of an international obligation by a State through a series of actions or omissions defined in aggregate as wrongful occurs when the action or omission occurs which, taken with the other actions or omissions, is sufficient to constitute the wrongful act.

(2) In such a case, the breach extends over the entire period starting with the first of the actions or omissions of the series and lasts for as long as these actions or omissions are repeated and remain not in conformity with the international obligation.

Staaten verdeckt im und durch den Cyberraum Informationen sammeln. Das nicht-autorisierte Eindringen in ein fremdes System geht aber häufig mit einer Modifikation oder einem Löschen bestimmter, im Zielsystem residenter Daten einher. Würde mithin das bloße Löschen von Daten als Zufügung eines Schadens gewertet, würden sich die Staaten der Möglichkeit der Cyberspionage begeben. Eine dahingehende Bereitschaft oder gar Rechtsüberzeugung ist jedoch nicht feststellbar. Schließlich ist in diesem Zusammenhang auch in Erinnerung zu rufen, das wirtschaftliche oder finanzielle ‚Schäden' vom Anwendungsbereich des Gewaltverbots und des Selbstverteidigungsrechts ausgeschlossen werden.

Trotz dieses Befundes ist ein langsames Umdenken zu verzeichnen, da sich die Staaten ihrer – selbst geschaffenen – Verwundbarkeit gegenüber maliziösen Cyber-Operationen zunehmend bewusstwerden. So hat der Beirat für auswärtige Angelegenheiten des Königreichs der Niederlande die Ansicht vertreten, Cyber-Operationen als bewaffnete Angriffe einzuordnen, wenn sie die Funktionsweise des Staates nachhaltig beeinträchtigen:

> 'It is more difficult to conclude whether this is the case if there are no actual or potential fatalities, casualties or physical damage. A serious, organised cyber attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks for it to be qualified as an armed attack. A disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. However, a cyber attack that targets the entire financial system or prevents the government from carrying out essential tasks, for example an attack on the entire military communication and command network that makes it impossible to deploy the armed forces, could well be equated with an armed attack.'[18]

Auch das U.S. Verteidigungsministerium wertet gegen militärische Befehls- und Führungsstrukturen gerichtete Cyber-Operationen als bewaffnete Angriffe, wenn festgestellt wird, dass , DoD networks and key resources on which DoD relies for its operations and attacks that could impact the U.S. military's ability to operate in a contingency.'[19] Das U.S. Verteidigungsministerium geht für Konfliktzeiten davon aus, dass that 'apotential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage.'[20] Auch in der britischen Cyber-Sicherheitsstrategie werden ‚vulnerabilities in cyberspace [that] could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home'[21] im Kontext des Selbstverteidigungsrechts thematisiert.

Die weiteren vom niederländischen Beirat angeführten Cyber-Operationen, die zu einer erheblichen Beeinträchtigungen öffentlicher oder gesellschaftlicher Funktionen führen, sind

---

[18] Advisory Council on International Affairs, Cyber Warfare, S. 21 (No 77, AIV/No 22, CAVV December 2011).
[19] U.S. Department of Defense, The DoD Cyber Strategy (Fn. 3), S. 10.
[20] Ebd., S. 2.
[21] The UK Cyber Security Strategy, S. 15 (November 2011), abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

eng mit der zunehmenden Sorge der Staaten hinsichtlich ihrer verwundbaren kritischen Infrastrukturen verbunden.

In der nationalen Cyber-Sicherheitsstrategie der USA aus dem Jahr 2018 wird nachdrücklich auf die Notwendigkeit zum Schutz von ‚networks, systems, functions, and data'[22], der , domestic critical infrastructure and global supply chains'[23] ebenso hingewiesen wie auf die Verwundbarkeit der USA gegenüber ‚peacetime cyber attacks against critical infrastructure'.[24] Sorgen bereiten dem U.S. Verteidigungsministerium ‚a cyberattack of significant consequence on the U.S. homeland and U.S. interests'[25] sowie ‚a sophisticated actor [who] could target an industrial control system (ICS) on a public utility to affect public safety, or enter a network to manipulate health records to affects an individual's well-being. A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.'[26] Die U.S. Joint Chiefs of Staff befassen sich mit ‚methods producing WMD-like effects' and the 'catastrophic effects […] possible in cyberspace because of the existing linkage of cyberspace to critical infrastructure SCADA systems.'[27] Schließlich wird in einer weiteren U.S. Strategie Die Bedeutung nationaler Sicherheitsinteressen betont, zu denen ‚the survival of the Nation; the prevention of catastrophic attack against U.S. territory; the security of the global economic system; the security, confidence, and reliability of our allies; the protection of American citizens abroad; and the preservation of universal values.'[28] gezählt werden.

Auch andere Staaten haben die Notwendigkeit des Schutzes ihrer kritischen Infrastrukturen erkannt. Deutschland fasst unter den Begriff der kritischen Infrastruktur ‚organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences.'[29] Genannt werden die folgenden Sektoren: ‚energy, information technology and telecommunication, transport, health, water, food, finance and insurance, State and public administration, media and culture.'[30] Singapur verweist auf ‚essential services such as energy, banking, healthcare and transport [that] are powered by infocomm technology.'[31] Kanada definiert kritische Infrastruktur als , processes, systems, facilities, technologies, networks, assets and services essential to health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.'[32]

---

[22] President of the United States of America, National Cyber Security Strategy of the United States of America, S. 3 (September 2018), available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[23] Ebd., S. 26.
[24] Ebd. S. 3.
[25] U.S. Department of Defense, The DoD Cyber Strategy (Fn. 6), S. 14.
[26] Ebd., S. 2.
[27] Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Fn. 1), S. C1
[28] Chairman of the Joint Chiefs of Staff, The National Military Strategy of the United States of America 2015, S. 5 abrufbar unter: https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
[29] German Cyber Security Strategy (Fn. 4), S. 15.
[30] *Ibid*.
[31] *Singapore's Cybersecurity Strategy* (Fn. 5), S. 8.
[32] Canadian Cyber Security Strategy (*supra* Fn. 4), S. 33.

Die NATO-Staaten haben erkannt, dass , cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.'[33]

Den nationalen Cyber-Sicherheitsstrategien und weiteren Stellungnahmen ist gemein, dass sie gegen die kritische Infrastruktur gerichteten Cyber-Operationen ein dem Einsatz traditioneller Mittel und Methoden der Kriegführung gleichkommendes Schädigungspotential zuerkennen. Sie rechtfertigen aber nicht die Schlussfolgerung, die Staaten würden jede gegen die kritische Infrastruktur gerichtete Cyber-Operation als einen das Selbstverteidigungsrecht auslösenden bewaffneten Angriff einordnen. Die Bandbreitet derartiger Cyber-Operationen ist derart groß, dass ihre Wirkungen im besten Fall lediglich Unannehmlichkeiten bereiten, im schlimmsten Fall aber das Funktionieren des Staates schwer beeinträchtigen können. Angesichts dessen ist es schwerlich möglich, eine allgemeine Rechtsüberzeugung nachzuweisen, die zu einer anerkannten Klassifizierung solcher Cyber-Operationen führt ‚that do not have a clear kinetic parallel'.[34]

Gleichwohl ist es vertretbar, bestimmte Cyber-Operationen als Anwendungen von Gewalt oder bewaffnete Angriffe anzusehen. Dies gilt für (1.) Cyber-Operationen gegen die für die nationale oder Bündnisverteidigung wesentlichen Infrastrukturen; (2.) Cyber-Operationen die die Staatsfunktionen nachhaltig erschüttern; (3) Cyber-Operationen gegen die Energieversorgung, das Gesundheitswesen oder lebensnotwendige Versorgungsketten. Wohl nicht gefolgt werden kann der Auffassung, nach der Cyber-Operationen gegen das gesamte Finanzsystem unter Art. 2 Abs. 4 und Art. 51 UN-Charta fallen.

3. Herausforderungen

Wenngleich es möglich ist, bestimmte Cyber-Operationen als Anwendungen von Gewalt oder gar bewaffnete Angriffe einzuordnen, sehen sich Staaten vergleichsweise großen Schwierigkeiten gegenüber.

Erstens besteht das Problem der **Zurechenbarkeit** einer Cyber-Operation zu einem bestimmten Staat fort. Die Handlungen, die einem Staat nach Maßgabe des Völkerrechts zugeordnet werden können, beschränken sich zwar nicht auf Organverhalten, sondern auch auf das Verhalten von Privatpersonen.[35] Gleichwohl steht die dem Cyberraum eigene Anonymität, aber auch die Möglichkeit, dass ein sog. Botnet zum Einsatz kommen kann, einer hinreichend sicheren Zurechnung häufig entgegen. Obgleich es mitunter gelungen ist,

[33] NATO, Wales Summit Declaration, Abs. 72 (5. September 2014), abrufbar unter: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/sede240914walessummit_en.pdf.

[34] Harold H. Koh, International Law in Cyberspace (*supra* note 9), p. 7.

[35] Vgl. dazu die Art. 4 ff. der Entwurfsartikel der Völkerrechtskommission zur Staatenverantwortlichkeit (Fn. 17).

maliziöse Cyber-Operationen einem bestimmten Staat zuzurechnen[36], bedarf es immer noch einer erheblichen Verbesserung cyber-forensischer Fähigkeiten, ohne die eine wirksame Reaktion nur unter engen Voraussetzungen möglich wäre. Daher hat der Befund der U.S. Joint Chiefs of Staff immer noch Gültigkeit:

> 'To initiate an appropriate defensive response, attribution of threats in cyberspace is crucial for any actions external to the defended cyberspace beyond that authorized as authorized self-defense. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state, with sufficient confidence and verifiability to hold them accountable.'[37]

Zweitens ist es, wie bereits erwähnt, äußerst schwierig, einen **unmittelbar bevorstehenden** oder bereits begonnenen **Angriff** im oder durch den Cyberraum hinreichend sicher festzustellen. Daher mögen die Konzepte der ‚antizipatorischen', ‚präventiven', ‚präemptiven' oder ‚interzeptiven' Selbstverteidigung im Cyberraum wenig ergiebig sein. Soweit ein unmittelbar bevorstehender Angriff im oder durch den Cyberraum in Frage steht, sind die im Tallinn-Handbuch 2.0 gegebenen Beispiele durchaus hilfreich:[38] (1) die Implementierung einer ‚logischen Bombe', wenn es hinreichend wahrscheinlich ist, dass zur Aktivierung notwendigen Bedingungen erfüllt werden; (2) die Implementierung einer maliziösen, aus der Ferne auszulösenden Software, wenn und soweit der Auslösende sich tatsächlich zum Angriff entschlossen hat.

Drittens besteht ein letztes praktisches Problem, wenn für das Vorliegen einer Gewaltanwendung oder eines bewaffneten Angriffs ein **subjektives Element** in Form von Vorsatz oder Absicht gefordert wird. Dies lässt sich weder in der physischen Domäne noch im Cyberraum feststellen. Zudem ist Art. 2 Abs. 4 und Art. 51 UN-Charta ein dahingehendes Erfordernis nicht zu entnehmen. Im Übrigen besteht stets die Möglichkeit, dass eine Cyber-Operation unbeabsichtigte Wirkungen bzw. Sekundärwirkungen zeitigt, die objektiv geeignet sind, eine Gewaltanwendung oder einen bewaffneten Angriff zu indizieren.

II. Weitere völkerrechtliche Fragestellungen

1. Due diligence

Der IGH hat im Korfu-Kanal-Fall festgestellt, ‚it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[39] Angewendet auf maliziöse Cyber-Operationen, die auf dem Territorium eines Staates vorgenommen, ohne dass sie diesem Staat zugerechnet werden können, und gegen einen anderen Staat gerichtet sind, ist der Ausgangsstaat verpflichtet, diese Cyber-Operationen zu beenden, sobald er davon

[36] Verwiesen sei lediglich auf den Mandiant Report aus dem Jahr 2013, in dem der Nachweis erbracht wurde, dass gegen die USA gerichtete maliziöse Cyber-Operationen der Volksrepublik China zurechenbar waren. Vgl. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html. Joint Chiefs of Staff, Cyberspace Operations (Fn. 1), S. I-12. Vgl. auch die deutsche Cyber-Sicherheitsstrategie (Fn. 4), S. 3

[38] Michael N. Schmitt (gen. ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge 2017), Kommentierung zur Regel 73, Abs. 7 f..

[39] International Court of Justice, Corfu Channel Case (United v. Albania), ICJ Rep. 1949, 4, 22.

Kenntnis erlangt hat oder hätte erlangen können. Dabei macht es keinen Unterschied, ob Ziele der Cyber-Operationen staatliche Einrichtungen oder private Infrastrukturen sind, da es um den Schutz der territorialen Integrität des Zielstaates geht. Allerdings impliziert dies keine Pflicht zur Prävention oder gar zu einer umfassenden Überwachung der sich auf dem Territorium ereignenden Cyber-Operationen.

2. Abwehr von maliziösen Cyber-Operationen, die unterhalb der Gewalt- bzw. Angriffsschwelle verbleiben

Selbst wenn maliziöse Cyber-Operationen unterhalb der Gewalt- oder Angriffsschwelle verbleiben, können sie wegen der mit ihnen einhergehenden Verletzungen der Souveränität des Zielstaates als völkerrechtwidrig eingeordnet werden.[40] Der Opferstaat bleibt dann nicht auf Proteste oder andere diplomatische Reaktionen beschränkt, sondern darf seinerseits mit einer verhältnismäßigen Gegenmaßnahme, also einem völkerrechtswidrigen Akt, reagieren, um den betreffenden Staat zu veranlassen, von seinem völkerrechtswidrigen Handeln abzulassen.[41] Freilich setzt dies die Zurechenbarkeit zu dem anderen Staat voraus.

Zudem besteht unter engen Voraussetzungen die Möglichkeit zur Verfügung, einen Notstand geltend zu machen, wenn eine nicht zurechenbare maliziöse Cyber-Operation eine schwere und unmittelbar drohende Gefahr für ein wesentliches Interesse (‚essential interest') des Staates verursacht.[42] Dann darf, soweit die weiteren Schranken beachtet werden, diese Gefahr abgewehrt werden, selbst wenn dadurch die Rechte anderer (unbeteiligter) Staaten beeinträchtigt werden.

3. Unterscheidung zwischen defensiven und offensiven Cyber-Operationen

Schließlich sollte erwogen werden, die gängige Unterscheidung zwischen defensiven und offensiven Cyber-Operationen insoweit aufzubrechen, als es um effektive Gegenmaßnahmen gegen maliziöse Cyber-Operationen geht. Gegenmaßnahmen im und durch den Cyberraum können nur dann hinreichend wirksam sein, wenn sie nicht allein auf die Abwehr beschränkt sind und wenn die Verantwortlichen mit Blick auf offensive Cyber-Operationen nicht allein über theoretische Kenntnis, sondern auch über hinreichende praktische Fähigkeiten verfügen.

---

[40] Vgl. dazu Tallinn Manual 2.0 (Fn. 38), Rules 1 ff.

[41] Vgl. dazu allein die Art. 22, 49 ff. der Entwurfsartikel der Völkerrechtskommission zur Staatenverantwortlichkeit (Fn. 17).

[42] Vgl. ebd., Art. 25:

‘1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:

(*a*) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and

(*b*) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:

(*a*) the international obligation in question excludes the possibility of invoking necessity; or

(*b*) the State has contributed to the situation of necessity.’