⇨ Max Weber

To Hack Back or Not?
Eine friedensethische Analyse von Cyberoperationen vor dem Hintergrund des Leitbilds des Gerechten Friedens

⇨ 1 Einleitung

Ooops your files have been encrypted. (Der Spiegel, 2017)

Nachrichten über Cyberangriffe auf Systeme und Netzwerke in Deutschland gehören zunehmend zum Alltag. In einer Umfrage im Frühjahr 2021 äußerten 46 Prozent der befragten Unternehmen in Deutschland, dass sie bereits von Cyberangriffen betroffen waren (vgl. Deutsche Welle 2021). Entsprechend wird auf politischer Ebene vermehrt die Frage diskutiert, ob nach Angriffen größeren Ausmaßes zurückgeschlagen werden kann (sog. Hackbacks). Dabei stellt sich aus (friedens-) ethischer Sicht *grundsätzlich* die Frage, inwiefern Cyberoperationen, insbesondere Hackbacks, legitimiert werden können.[1]

Zum Leitbild des Gerechten Friedens (vgl. Die deutschen Bischöfe 2000; Rat der EKD 2007) finden sich eine Reihe von Veröffentlichungen (vgl. Ebeling/Werkner 2017; Lienemann 2000; Raiser 2019; Strub/Grotefeld 2007), u.a. im Umfeld der EKD-Synode 2019 (Kirchenamt der EKD 2019; Schubert 2018; Werkner/Meireis 2019), ebenso wie, von Arquilla/Ronfeldt (1993, 2001) eröffnet, zu Cyberoperationen, u.a. im politikwissenschaft-

Max Weber, geb. 1990 in Friedrichshafen, M.A., Studium der Theologie, Politik-, Religions- und Kulturwissenschaften in Tübingen, Edinburgh, Dunedin, Berlin, Stellenbosch, arbeitet freiberuflich zu friedenspolitischen und ethischen Themen, u.a. Rüstungsexporte, Militarisierung, Migration. Editor von »Abschottung mit System. Wie Europa gegen Schutzsuchende aufrüstet« (hg. von EAK, pax christi, PRO ASYL) (2021); (gemeinsam mit Lukas Del Giudice u.a.) Was sagt Pegida? Eine Analyse von Reden in Dresden, in: Uwe Backes u.a. (Hg.): Sachsen – Eine Hochburg des Rechtsextremismus? (2020); (gemeinsam mit Thomas Nielebock) Deutsche Rüstungsexporte. Eine Handreichung, in: Pfarramt für Friedensarbeit (Hg.): Tod – Made in Germany? (2017).
GND: 124756679X

DOI: 10.18156/eug-2-2021-art-5

(1) Dieser Artikel basiert auf der Masterarbeit des Autors: Cyberwar(fare) – Ein Fall für den Gerechten Frieden? (unveröff., 2021).

lichen (vgl. Coker 2009; Riordan 2019), politisch-militärischen (vgl. Schröfl u.a. 2011), ethischen (vgl. Schmidt-Radefeldt/Meissler 2012) sowie informationstechnischen (vgl. Rid 2018) Bereich. Daneben finden Fragen zu Cyberoperationen Eingang in Foren, z.B. der DefensiveCon v02 (vgl. DefensiveCon 20/02/2020) sowie in Sachbüchern (vgl. Hofstetter 2019; Kurz/Rieger 2018). Außerdem gibt es Publikationen von staatlichen Einrichtungen, u.a. das Weißbuch der Bundeswehr (Die Bundesregierung 2016), den Bericht zur »Lage der IT-Sicherheit in Deutschland« (vgl. BSI 2019; 2020), die Tallinn Handbücher (vgl. Schmitt 2013; 2017) sowie Anfragen an die Bundesregierung (vgl. 2018b; 2019).

Die Frage nach dem Geltungsbereich des Leitbilds des Gerechten Friedens für den Cyberraum – und damit die Verknüpfung beider Themenbereiche – zeigt sich jedoch als unzureichend abgedeckt: Auch wenn das Leitbild als Ausgangspunkt von Hering/Schubert (2012) dient, lässt die Analyse zentrale Aspekte außen vor. Auch die Publikationen der evangelischen wie katholischen Militärseelsorge (vgl. Bock 2014; Bock u.a. 2019; Dörfler-Dierken u.a. 2020), der Forschungsstätte der Evangelischen Studiengemeinschaft (insb. Werkner/Schörnig 2019), in Rogg u.a. (2020) wie auch im aktuellsten Beitrag, der EKD-Denkschrift »Freiheit digital« (2021), beinhalten keine Analyse der Frage, inwiefern Cyberoperationen mit dem Leitbild *überhaupt* in Einklang gebracht werden können.

Aus der aufgezeigten Forschungslücke ergibt sich die Leitfrage, inwiefern sich (bestimmte) Cyberoperationen mit dem Framework des Gerechten Friedens erfassen und legitimieren lassen. Die Beantwortung dieser Frage soll in acht Kapiteln erfolgen: Zunächst soll das Leitbild des Gerechten Friedens eingeführt werden (Kap. 2). Während Kapitel 3 mit definitorischen Ausführungen einen Überblick zu Cyberoperationen bietet, zeigt Kapitel 4 Herausforderungen für die friedensethische Bewertung auf. Beide Stränge zusammenführend soll Kapitel 5 beantworten, ob bestimmte Arten von Cyberoperationen nach den Kriterien des Leitbilds zulässig sind. Darauf aufbauend werden Alternativen (Kap. 6) und weitere Forschungsfragen (Kap. 7) aufgezeigt, ehe eine zusammenfassende Betrachtung diesen Artikel abschließt (Kap. 8). Das Vorgehen kann sowohl als normativ-theorieprüfend als auch heuristisch-explorativ beschrieben werden und ist angelehnt an die »Sachmomente des ethischen Urteils« von

Tödt (1977).[2] Als »Reflexion von Fragen öffentlicher Bedeutung im Lichte theologischer Traditionen« (Bedford-Strohm 2015, 215) ist der Artikel in den Bereich der Öffentlichen Theologie einzuordnen.

⇨ 2 Das Leitbild des Gerechten Friedens

Als Grundlagenwerke zum Konzept des Gerechten Friedens dienen das Bischofswort (2000) sowie die EKD-Denkschrift (2007). Dabei werden drei »Grundorientierungen« festgehalten, die die neue Perspektive und Zielrichtung in der Konfliktbewältigung zum Ausdruck bringen sollen: 1. Vorrang ziviler Konfliktbearbeitung, 2. Verständnis einer Friedensordnung als Rechtsordnung und 3. Beschränkung militärischer Gewalt zur Rechtsdurchsetzung (vgl. Hoppe/Werkner 2017, 349). Da Recht »auf Durchsetzbarkeit angelegt« (Zi. 98)[3] ist, ergibt sich die Notwendigkeit einer Ethik rechtserhaltender Gewalt (vgl. Schubert 2013).[4] Um die »Anwendung von Zwangsmitteln an strenge ethische und völkerrechtliche Kriterien [zu] binden« (Zi. 196), lehnt sich die EKD-Denkschrift an die sieben Kriterien des Gerechten Krieges an (Zi. 102), die durch weitere Ausführungen ergänzt werden (Zi. 103-123). Dabei ist von zentraler Bedeutung, dass »nach herkömmlichem Verständnis für den Gebrauch von legitimer Gegengewalt *alle* diese Kriterien erfüllt sein [müssen], gleichgültig ob im Fall eines innerstaatlichen Widerstands, eines Befreiungskampfes oder militärischer Konflikte zwischen Staaten« (Zi. 103, Hervorhebung mw). Zu betonen bleibt, dass ein wesentlicher Meilenstein des Leitbilds in der Überwindung der ausschließlichen Prüfung der Kriterien zur Anwendung von Gewalt liegt: Während dies bei der Lehre des Gerechten Krieges den Fokus darstellte, zeichnet sich das Leitbild des Gerechten Friedens durch einen weitreichenden Wandel auf ein umfassendes Friedensverständnis sowie eine Friedensorientierung mit der grundsätzlich neuen Zielrichtung unter dem Primat des Zivilen aus (vgl. Meireis 2019a, 149; Zi. 99).

(2) Tödt gliedert die »sechs Schritte bzw. Sachmomente« in Problemfeststellung, Situationsanalyse, Verhaltensalternativen, Normenprüfung, Urteilsentscheid und rückblickende Adäquanzkontrolle (1977, 84).

(3) Literaturangaben, die aus »Zi.« und Nummer bestehen, entstammen Rat der EKD (2007).

(4) Zur Kritik an der Formulierung und Implikation des Terms »rechtserhaltend« s. u.a. Klein/Kümmel (2012); Meireis (2019a, 150). Dabei ist festzuhalten, dass sich mit Reuter (2012, 13) der »Begriff des Rechts (…) nicht auf ein faktisch gegebenes Rechtssystem [bezieht], sondern normativ auf die in den basalen Menschenrechten und einer legitimen Völkerrechtsordnung konkretisierte Rechtsidee.«

Während das Konzept nicht frei von Kritik ist (vgl. Brock 2019; Hahn 2008, 5; Haspel 2009, 75; Hoppe/Werkner 2017, 349; Rudolf 2017, 34; van Baarda 2018, 17; Werkner 2010, 149), zeugen Veröffentlichungen u.a. durch den früheren Friedensbeauftragten des Rates der EKD (2015), auf den EKD-Synoden seit 2019 sowie in der EKD-Denkschrift »Freiheit digital« (2021) von dessen Stellenwert im kirchlichen Diskurs, und es soll als Framework dieser Analyse zugrunde liegen. Da es keine in sich unumstößlichen Konkretisierungen beinhaltet, lädt es zu einem Auseinandersetzungsprozess ein, den Mielke dergestalt einordnet, dass die Tatsache,

> [d]ass es oft keine »klare« und »eindeutige« evangelische Stimme im politischen Feld gibt, (…) mitunter bedauerlich sein [mag]. Diese Unklarheit verweist aber auf vielfältige Prozesse der ethischen Deliberation, in denen sich Konsense ausbilden und auch wieder brüchig werden. Diese Prozesse sind die eigentlich orientierende Ressource, die die evangelische Kirche in den politischen Prozess der freiheitlichen Gesellschaft einbringt (2018, 45).

⇨ 3 Cyberoperationen – ein Überblick

Nachfolgend sollen ein Situationsüberblick (3.1) gegeben und staatliche Cyberaktivitäten dargestellt werden (3.2). Hiernach wird auf die Frage, ob bzw. inwiefern eine Distinktion von Cyberoperationen (3.3) gelingen kann, eingegangen.

⇨ 3.1 Cyberangriffe: Ein Situationsüberblick

Mit der nahezu universalen Nutzung von Computern und Smartphones steigen auch damit verbundene Risiken: Der Zuwachs von im Schnitt täglich (!) etwa 322.000 Schadprogrammvarianten allein in Deutschland macht dies deutlich (vgl. BSI 2020, 10). Angriffe finden in der Regel durch Schwachstellen statt, die sich mithilfe eines dreistufigen Modells ordnen lassen (vgl. die Abb. in Koch, R. 2020, 3): Die pyramidenförmige Anordnung beschreibt als größten Bereich das »Ausnutzen vorhandener Schwachstellen«, worunter »öffentlich verfügbare Exploits und fehlerhafte Programme« verstanden werden (ebd.). Die mittlere Stufe umfasst das »Entdecken neuer Schwachstellen«, die auf neu entdeckten und öffentlich noch unbekannten Schwachstellen, sog. *Zero-Days*, beruhen. Die »Königsdisziplin« liegt

im »Einbringen neuer Schwachstellen«, wobei Angriffsvektoren neben dem Einschleusen in »Software, Firmware oder Hardware (…) auch in mathematischen Verfahren (Algorithmik oder Zahlen) versteckt werden« können (ebd., 4).

Als Beispiel für die Bandbreite von Cyberangriffen sollen drei Arten vorgestellt werden.[5] Die erste zielt auf ein Überlasten von Servern durch *Distributed Denial of Service (DDoS)*-Attacken, bei denen gleichzeitig eine Vielzahl von Anfragen an einen Server geschickt wird. Eines der bekanntesten Beispiele ist ein Cyberangriff auf Estland, bei dem 2007 über mehrere Wochen Regierungsinstitutionen, Bankdienste und Medien temporär lahmgelegt wurden (vgl. Reuter u.a. 2019, 24). Die zweite Art liegt im Ausspionieren von Systemen durch *Spyware*: Das Eindringen in ein externes System gelingt meist mittels Software, die dort vorhandene Daten abruft. Ein Beispiel hierfür ist der sog. »Bundestagshack« 2015 (vgl. Biselli 2016). Der dritte Bereich ist ein direktes Eingreifen in externe Systeme und eine dortige »Wirkung«, i.e. eine Veränderung oder Löschung von Inhalten. Beispielhaft hierfür kann der Stuxnet-Angriff gesehen werden, bei dem die Veränderung von Software zu irreparablen Schäden an iranischen Atom-Zentrifugen führte (vgl. Rid 2018, 66). Während die ersten beiden Beispiele keine Seltenheit darstellen, ist ein Angriff wie Stuxnet bisher die Ausnahme.

Grundsätzlich können als Ziele sowohl das Erlangen (wie auch Verändern oder Zerstören) von Daten oder Geldern, aber auch das Lahmlegen von kritischer Infrastruktur (KRITIS) bis hin zur Zerstörung materieller Güter verfolgt werden. Den meisten Cyberangriffen ist gemein, dass keine direkten letalen Wirkungen erzielt wurden.

⇨ 3.2 Staatliche Cybersicherheitspolitik in Deutschland

In Deutschland wird die »Gewährleistung von Freiheit und Sicherheit (…) auch im Cyber-Raum« (BSI 2020, 8) als staatliche Kernaufgabe angesehen, mit der eine Vielzahl von Akteur*innen betraut ist (vgl. Rupp/Herpig 2021).[6] Dabei ist grundsätzlich zu fragen, wo deren institutionelle Zuständigkeit verortet wird, womit der Fragehorizont einhergeht, ob aus einem »Rechtsparadigma« oder »Feindabwehrparadigma« (Meireis 2019b, 111) heraus argumentiert wird. Auch Schörnig

(5) Für eine ausführliche Übersicht s. BSI (2020).
(6) Für Hintergründe zu Aufgaben und Akteur*innen s.a. Herpig (2020a); Zimmermann (2019).

(2019a) und die EKD-Denkschrift »Freiheit digital« weisen auf die Bedeutung dieser Frage hin, wobei es »alles andere als selbstverständlich [sei], elektronische Schädigungen im Kriegsparadigma zu verstehen« (EKD 2021, 130).[7]

Trotzdem zeigt sich u.a. in der Einrichtung des Zentrums für Cyberoperationen mit 14.500 Personen im Jahr 2018 (vgl. Die Bundeswehr 2020), dass militärischen Aktivitäten zunehmend mehr Gewicht beigemessen wird. Dabei bezieht sich deren Aufgabenbereich auch auf »Wirkungen«:[8] So seien »[o]ffensive Cyber-Fähigkeiten der Bundeswehr (…) als unterstützendes, komplementäres oder substituierendes Wirkmittel anzusehen« (Meister 2015). Was genau unter offensiven Cyber-Fähigkeiten zu verstehen ist, bleibt unklar,[9] auch wenn beispielhaft im Abschlussbericht des Aufbaustabs CIR (Organisationsbereich Cyber- und Informationsraum der Bundeswehr) »[o]hne Scheuklappen« (Busch 2020, 2) argumentiert wird: »Hat ein Akteur die Fähigkeit zur Verteidigung, so kann er auch weltweit angreifen« (BMVg 2016, 4). Bezüglich der Verteidigungsaspekte wurde 2016 festgelegt, dass auch Cyberangriffe einen NATO-Bündnisfall auslösen können (vgl. NATO 2020).

⇨ 3.3 Unterscheidungsansätze von Cyberoperationen

Nicht selten wird die Schwierigkeit einer Unterscheidung von Cyberoperationen benannt: So führe der Zustand der »permanenten Ambiguität« dazu, dass es »weder Trennlinien zwischen innerer und äußerer Sicherheit« gebe, noch sich eindeutig bestimmen ließe, »welche Cyberressourcen defensiven oder offensiven Zwecken zugeordnet werden können« (Reuter u.a. 2019, 34). Um dieser Problematik zu begegnen, soll ein neu entwickelter Ansatz vorgeschlagen werden.[10]

(7) Auch wenn dieser Artikel zunächst primär Cyberoperationen/Hackbacks analysiert, zeigt Kap. 6.2 darüberhinausgehende zivile Ansätze.

(8) S. für weitere Ausführungen Schulze (2020b), für eine Kritik daran Koch, R. (2020, 6).

(9) S.a. Schörnig (2019b, 129); Schulze (2020b, 9). Vgl. auch den Bericht über Aussagen des Bundesmajors Bernd Kammermeier: »Die Jungs und Mädels [des KdoCIR] hier sind die einzige Einheit der Bundeswehr, die permanent im Krieg ist« (in Rehage 2019; vgl. Reinhold 2019).

(10) Mit Kreuzer (2019, 69) aus völkerrechtlicher und Meireis (2019b, 107) aus ethischer Perspektive geht damit die Abgrenzung von Ansätzen, in denen »Cyberwar(fare)« als Kategorie eingeführt bzw. verwendet wird, einher.

⇨ 3.3.1 Ein alternativer Ansatz: What do you do?

Bei diesem Ansatz soll zunächst dem zweiteiligen Vorgehen von Schmahl (2020, 89) gefolgt werden (s.u. Abb. 1):[11] Im ersten Schritt stellt sich die Frage, ob Cyberoperationen *intrusiv* oder *nicht-intrusiv* durchgeführt werden.[12] Bei nicht-intrusiven wird zum Beispiel »über mit Schadsoftware (Malware) infiltrierte Rechner die Funktionsfähigkeit eines Computernetzwerkes« *verringert* oder *unterbunden* (z.B. *DDoS*-Angriffe, s.o.), die Cyberoperationen finden dementsprechend *nicht in* einem externen Netzwerk statt. Als intrusiv können dagegen Cyberoperationen eingeordnet werden, die »auf ein informationstechnisches System mittels Spyware oder Malware gezielt zu[greifen]« und *in* einem *fremden* Netzwerk agieren.

Der zweite Schritt geht auf Fragen nach den *Wirkungen* innerhalb des Systems ein, in welches *intrusiv* eingedrungen wurde: Werden in diesem Änderungen vorgenommen, Daten beispielsweise gelöscht, kann von »netzwerkexternen Wirkungen« bzw. *Computer Network Attacks (CNA)* gesprochen werden.[13] Werden die vorgefundenen Inhalte ohne Veränderung belassen und beispielsweise mittels *Spyware* Daten ausspioniert, können diese als »netzwerkintern bzw. -intrinsisch« bezeichnet werden (*Computer Network Exploitation, CNE*).[14]

Diese Definition bringt unter anderem den Vorteil mit sich, dass auch Cyberoperationen innerhalb des intrusiven Bereichs unterschieden werden können, was sich beispielhaft am sog. Bundestrojaner sowie an »Wirkung« erzielenden Einsätzen der Bundeswehr zeigen lässt. Beide Operationen sind intrusiv. Während jedoch das Mandat beim

(11) Für die Zitate dieses Abschnitts s. Schmahl (2020, 89), nach der »Kategorisierungsmodelle, etwa nach Autoren oder Adressaten einer Computernetzwerkoperation, keinen klaren Erkenntnisgewinn [versprechen], da sowohl nichtstaatliche als auch staatliche Akteure im Cyberraum agieren und es infolgedessen zu Ambivalenzen und Doppeladressierungen kommen kann.«

(12) Schmahl führt als dritte Kategorie »Cyberkommunikation« an, die das Verwenden von Plattformen u.a. für Fake News beschreibt. Gleichzeitig wird die Kategorie von ihr bereits separiert, da sie »keine Computernetzwerkoperation im engeren Sinne« darstelle (ebd.). Zur besseren Übersichtlichkeit soll diese Kategorie hier nicht aufgeführt werden.

(13) CNA sollen damit als »actions taken ›through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves‹« (Romanosky/Goldman 2016, 11) definiert werden.

(14) CNE sollen damit als »operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks« (Romanosky/Goldman 2016, 11) definiert werden.

Einsatz eines Bundestrojaners auf die Überwachung bzw. Spionage beschränkt ist (vgl. Meister 2020a),[15] der Einsatz also als CNE kategorisiert werden kann, gehen die Befugnisse der Bundeswehr darüber hinaus. So wird expliziert, dass die »Fähigkeiten zur Aufklärung und *Wirkung* im Cyber- und Informationsraum« gestärkt und weiterentwickelt werden sollen (Die Bundeswehr 2019a). Die Einsätze können dabei vielfältig sein: »Zum Beispiel können die Spezialisten des CIR feindliche Webseiten übernehmen, eigene Inhalte erstellen und seine Kommunikation des Einsatzkontingents über dieses Medium laufen lassen« (Die Bundeswehr 2019b). Durch die Definition ist hier eine analytische Trennschärfe möglich und Einsätze mit »Wirkung« können als CNA kategorisiert werden. Da der Fokus auf Handlungen liegt, besteht ein weiterer Vorteil in der akteur*innenübergreifenden Anwendbarkeit, die sich ebenso wenig auf eine Dichotomie in innere oder äußere Sicherheit beschränkt (vgl. Rid 2018, 42).

Mitnichten können hiermit alle definitorischen Probleme als gelöst betrachtet werden. So befreit dieser Ansatz beispielsweise nicht davon, die Urheber*innen eines Angriffs ausfindig zu machen.[16] Die Frage, inwiefern bei einem Angriff überhaupt von »Gewalt« gesprochen werden kann, soll im nachfolgenden Abschnitt ausgeführt werden.

⇨ 3.3.2 Wer spricht hier von Gewalt?

Im Hinblick auf die Frage, inwiefern Cyberoperationen Gewalt sind oder beinhalten, gehen die Ansichten auseinander: Rid zufolge wird »bei den meisten Cyberattacken (…) keine Gewalt angewendet« (2018, 35), die bisher einzige Ausnahme sei Stuxnet gewesen.[17] Den Gegenpol hierzu stellt Schörnig dar, demzufolge

(15) Ein entsprechendes Framing als »Online-Durchsuchungen« verstärkt dies. Gleichzeitig überschneiden sich beim Einsatz von Staatstrojanern, die seit Ende 2020 von Geheimdiensten in Deutschland einsetzbar sind (vgl. Meister 2020b), Herausforderungen von CNA und CNE (vgl. Meister 2020c; EKD 2021, 136).

(16) Dies ist jedoch auch bei anderen Ansätzen notwendig, insofern liegt hierbei kein Nachteil bei der Verwendung dieser Definition.

(17) Rid begründet dies u.a. damit, dass »[i]n mindestens vier Hinsichten (…) eine im Cyberspace ausgeübte Gewalt weniger direkt [sei] als andere Formen von Gewalt: Sie ist weniger körperlich, weniger emotional, weniger symbolisch und infolgedessen weniger instrumentell als konventionellere Formen politischer Gewaltanwendung« (2018, 35).

> sich erkennen [lässt], dass die physische Schädigung von Menschen in bestimmten Formen digitaler Gewaltanwendungen nicht zwingend zum Tragen kommen muss. Es sind im Rahmen der Digitalisierung (…) Konstellationen denkbar, bei denen die Vorfälle eher an Formen struktureller Gewalt nach Johan Galtung erinnern, statt Ähnlichkeiten zu physischen/kinetischen Angriffen [zu] haben (2020, 68).

Während entsprechend bei der ersten Definition CNA in der Regel als gewaltfrei, bei der zweiten in der Tendenz jede CNA als gewaltsam einzustufen wäre, soll hier ein dritter Ansatz vorgeschlagen werden.[18] Dieser beruht auf dem von Finlay (2017) entwickelten Konzept eines »Double-Intent Accounts«. Diesem folgend ist Gewalt

> defined by the presence of Violent Agency consisting of the intentional infliction of [1] destructive harm by human agents on targets using a technique chosen with the further intention [2] of eliminating or evading the target's means of escaping it or defending against it (2017, 73).

Um als gewaltsam eingestuft zu werden, muss also ein Schaden intendiert bzw. zugefügt und gleichzeitig dem »Opfer« die Chance genommen werden, diesem zu entkommen oder sich zu verteidigen. Zusätzlich ist die Unterscheidung zwischen »destructive harming« und »appropriative harm« zentral:

> On the one hand, appropriative harming occurs where the harm an assailant causes to her victim is the same as the benefit enjoyed as a result by the assailant—i.e. they are commensurable in kind and commensurate in scale. By contrast, where the benefit to an assailant is very different (incommensurable perhaps or just very different in scale), then we are more likely to interpret it as a »violent attack« rather than some sort of theft (Finlay 2018, 367).

Bezogen auf den Cyberbereich bedeutet dies, dass hinsichtlich der Anwendung von Gewalt eine Differenzierung vorgenommen werden kann: Während Cyberangriffe, die zur Erpressung von Geldern oder

(18) Für einen weitergehenden Überblick s. Meireis (2012). Dass Cyberoperationen hierbei keine zentrale Rolle spielen, zeigt die Aktualität und Neuheit der Thematik.

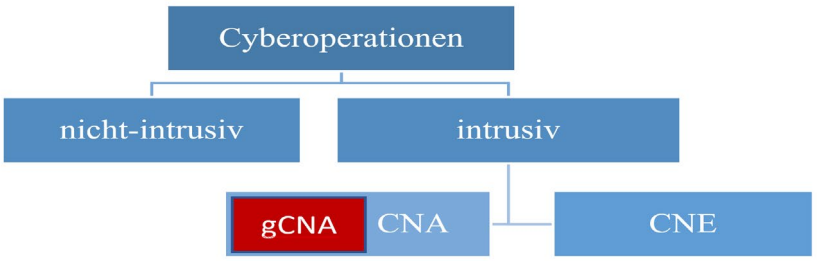
zum Sammeln von Informationen durchgeführt werden, nach dieser Definition nicht als Gewaltanwendung eingestuft werden, sind Cyberangriffe, bei denen Daten zerstört oder dauerhaft verändert werden, als (Formen von) Gewalt zu bezeichnen:[19] Diese als »Violent Cyber-Attacks« (ebd., 372) bezeichneten Angriffe stuft Finlay entweder direkt als Gewalt (bspw. Stuxnet), als Teil von Gewalt (bspw. durch das Ausschalten von Radarsystemen als Teil einer größeren Operation) oder als Androhung von Gewalt (bspw. die DDoS-Attacke auf Estland 2007, s.o.) ein (vgl. ebd., 370).

⇨ 3.4 Vorschlag einer neuen Definition: gCNA (gewaltsame Computer Network Attacks)

Finlays Definition bietet die Möglichkeit, jede Form von Cyberoperation auf ihren »Gewaltcharakter« zu untersuchen. Wie obig ausgeführt, zeigt sich diese Problematik insbesondere bei der Frage nach »Wirkungen«. Um schließlich aus der Perspektive des Leitbildes des Gerechten Friedens eine Analyse zu ermöglichen, sollen beide vorgestellten Definitionen verbunden und mithin ein neuer Definitionsvorschlag entwickelt werden: Dabei wird die obige Definition von Schmahl als Grundlage beibehalten und um die eingeführte Definition von Gewalt erweitert, sodass CNA, die Gewalt anwenden, im Folgenden als »gewaltsame Computer Network Attacks« (gCNA) bezeichnet werden.

(19) Finlay führt hierzu aus: »By contrast with the hacker who steals funds or secrets, inflicting harm appropriatively (analogously with a pickpocket or eavesdropper), one who uses computer viruses to corrupt data or delete it, making it unusable, thereby inflicts destructive harms. If she does so under cover of a shielding device making her attack undetectable until it is too late (or in any other way that makes it impossible to defend against the attack), then the attack has the same agential complexion as an act of conventional, physical violence« (2018, 370).

Abbildung 1:
Entwurf einer Definition für gewaltsame Computer Network Attacks (gCNA)



Zwei Beispiele sollen dies verdeutlichen: Ein Angriff eines Hackers, der in das Netzwerk einer Politikerin eindringt, Daten entwendet und Geld erpresst, würde als CNA kategorisiert werden. Ein Angriff einer Hackerin wiederum, die in das Netzwerk eines Politikers eindringt und Daten löscht oder unbenutzbar macht, kann als gCNA bezeichnet werden. Entsprechend sind bei gCNA weder nicht-intrusive Cyberoperationen und CNE, sondern nur bestimmte Formen von CNA inkludiert (s. Abb. 1).

⇨ 3.5 Zwischenfazit Kapitel 3

Die vorangehenden Ausführungen machten deutlich, dass einerseits durchaus von einer »Gefahr« durch Cyberangriffe gesprochen werden kann (3.1), auf die in Deutschland unter anderem mit dem Aufbau eines militärischen Organisationsbereichs reagiert wurde (3.2). Da klassische Definitionen hier nicht in bekannter Form greifen, wurde mithilfe eines zweistufigen Verfahrens eine Distinktion von Cyberoperationen zunächst in intrusiv sowie nicht-intrusiv, dann mit netzwerkintrinsischen sowie -externen »Wirkungen« als möglich gezeigt (3.3.1). Dass nicht jede CNA eine Gewalttat darstellt, wurde schließlich mithilfe der Definition von Finlay (2017; 2018) verdeutlicht (3.3.2) und ein Entwurf für eine eigene Definition vorgeschlagen (3.4). Diese Schritte werfen bereits Licht auf einige der Herausforderungen, die im nachfolgenden Kapitel ausgeführt werden. Der weitere Verlauf der Arbeit soll sich hauptsächlich mit intrusiven, netzwerkexterne Wirkungen hervorrufenden und Gewalt anwendenden Cyberoperationen

(gCNA) beschäftigen, da sich im Besonderen bei diesen die Frage einer »Zuständigkeit« des Leitbilds des Gerechten Friedens stellt.

⇨ 4 Herausforderungen für die friedensethische Bewertung von Cyberangriffen

Nachfolgend soll gezeigt werden, dass mit Cyberaktivitäten eine Reihe neuer Herausforderungen einhergehen. Dabei sollen zunächst allgemeine, dann speziell für gCNA geltende Herausforderungen beleuchtet werden.

⇨ 4.1 Allgemeine Herausforderungen

⇨ 4.1.1 (Un-)Möglichkeit von Attributionen

Im Cyberraum liegt die größte Herausforderung darin, einen Angriff einer*m Urheber*in zu attribuieren, wenn das Erkanntwerden kein Teil der Strategie ist.[20] Dabei ist die Schwierigkeit sowohl technischer wie auch sozialer Natur: Die*der Besitzer*in des Geräts, der physische Ort des Geräts sowie die tatsächlich handelnde Person müssen erkannt werden (vgl. Clark/Landau 2011, 2). Aufgrund der sich durch diese dreifache Unterscheidung ergebenden Schwierigkeiten werden das sog. »Attributions-Problem« auch als »Dreh- und Angelpunkt der Cybersicherheit« (Rid 2018, 16) und »Zurechnungs- und Beweisfragen« als »größte Herausforderung bei Cyberoperationen« (Schmahl 2020, 93) bezeichnet. Die meisten Begründungen verweisen darauf, dass »[t]ypical computer network environments are not designed to support attribution of attackers« (Wheeler/Larsen 2003, 4). Auch wenn vereinzelt Attributionen erfolgreich zu sein scheinen,[21] weist die überwiegende Zahl der Fälle darauf hin, dass das Problem der »Anonymität und Nicht-Attribuierbarkeit« (Schubert 2020, 6) bestehen bleibt und somit Angreifer*innen nicht »eindeutig identifizierbar« (Schmahl 2020, 95) sind. Noch weitreichender ist die Einschätzung

(20) Attribution wird hierbei verstanden als das Identifizieren der Akteur*innen, die verantwortlich sind für eine Operation, »determining the identity or location of an attacker or an attacker's intermediary« (Wheeler/Larsen 2003, 1).

(21) Ein Beispiel könnte die im Mai 2020 gestellte Strafanzeige der Bundesstaatsanwaltschaft Deutschlands gegen einen russischen Staatsbürger in Verbindung mit dem Cyberangriff auf den Bundestag 2015 (vgl. Flade/Mascolo 2020) werden: Sollte der Prozess eröffnet werden und eine Verurteilung stattfinden, wäre dies ein Novum. Zu beachten ist jedoch, dass zwischen Attacke und Anzeige ein Zeitraum von fünf Jahren lag.

von Gaycken, demzufolge »Cyberangreifer (…) unmöglich identifiziert werden« können (2012, 101). Er begründet dies mit der Möglichkeit des unmittelbaren Verwischens von physischen Spuren, aber auch dem »apologetische[n] Charakter der Datenspuren«, da »[d]er informatische Gehalt des Cyberangriff [sic!] (…) konsequent manipulierbar« ist (2012, 102). Die »Manipulation« kann sich dabei auch in sog. False Flags zeigen, also indem ein Angriff derart gestaltet ist, dass die Angegriffenen durch vermeintliche Indizien einen Angriff einer*m falschen Akteur*in zuordnen (vgl. Lindsay 2013, 377). Damit geht einher, dass die Gefahr einer »false attribution and political instrumentalization (…) tremendously high« (Schulze 2018, 286) ist.

⇨ 4.1.2 Die (Unendlichkeit bis zur) Erkennung eines Angriffs

Eine weitere Herausforderung stellt das Erkennen eines Angriffs dar: Während dies beispielsweise bei DDoS- oder Ransomware-Attacken durch finanzielle Forderungen recht unmittelbar geschehen kann, zeichnen andere CNA deutlich längere Zeiträume aus: Reinhold/Schulze zufolge können »[d]ie meisten Cyber-Angriffe (…) erst nach durchschnittlich 150-200 Tagen als solche identifiziert« (2017, 9) werden. Dass Cyberangriffe häufig gänzlich unerkannt bleiben, muss dabei als weitere Herausforderung gesehen werden: Nach Döge liegt der Anteil des nicht-Erkennens sogar bei etwa 96% (2010, 498; vgl. Wissenschaftliche Dienste des Deutschen Bundestags 2015, 4). Dabei ist zusätzlich zu beachten, dass mitunter auch lange nach einem Angriff unklar ist, wie groß der Angriff war und ob bzw. welche Daten abgeflossen sind oder geändert wurden, ob ein Angriff also (g)CNA oder CNE ist (vgl. Riordan 2019, viii).

⇨ 4.1.3 Verschwimmende Grenzen zwischen Zivilem und Militärischem

Bereits die definitorische Klärung hat gezeigt, dass die Grenze zwischen zivilem und militärischem Bereich fluide ist. Gründe sind u.a., dass »[d]ie Kriegsführung (…) mit zivilen Mitteln geführt« (Werkner 2019, 6) wird. Herausforderungen dieser als »Verschmelzung« beschriebenen Konvergenz zeigen sich in verschiedener Weise: So erschwert der Umstand einer selten gelingenden Attribution auch die von Werkner obig zitierte »Auffassung« als »zivile oder militärische Bedrohung«.[22] Reinhold macht zudem darauf aufmerksam, dass

(22) Damit einher geht die Herausforderung der institutionellen Zuständigkeit (s.o. 3.2.).

durch die notwendigen »Aufklärungsaktivitäten« bei Cyberoperationen

> zum einen zunehmend die Grenzen zwischenstaatlicher Konflikte [verschwimmen]. Andererseits verstärkt der Bedarf an Informationen die weitere Verzahnung geheimdienstlicher und militärischer Aktivitäten um bspw. dem für Deutschland geltenden Primat der defensiven Ausrichtung der Bundeswehr Rechnung tragen zu können (2020, 7).

Parallel zeigt sich, dass sich auch im Bereich der Privatwirtschaft Akteur*innen profilieren, deren Expertise für die Systemsicherheit herangezogen wird und die beispielsweise eigene Hackertools entwerfen und nutzen (u.a. FireEye). Auch Hackbacks sowie Attributionen werden inzwischen teils von Unternehmen wie Microsoft durchgeführt (vgl. Lemos 2018). Ein weiterer Aspekt dieser Verschmelzung ist eine grundsätzliche Allverfügbarkeit und Allmöglichkeit für Cyberangriffe durch Components-Off-The-Shelve (COTS), ergänzt durch frei verfügbare Anleitungen zum Bau von Programmen (vgl. BSI 2020, 29). Abschließend ist zu nennen, dass Staaten im Regelfall nicht selbst zu den Herstellern von Soft- und Hardware zählen, woraus resultiere, dass die Anreize für Unternehmen, kostspielige Sicherheitssysteme freiwillig einzubauen, gering seien (vgl. Perkovich/Hoffman 2019).

⇨ 4.1.4 Gültigkeit völkerrechtlicher Regeln

Übereinstimmend kann anhand von zwei Berichten von UN-Expert*innengruppen (UN-Dok. A/68/98 vom 24.06.2013, para 20 und A/70/174 vom 22.07.2015, para 28c), Ausführungen der Bundesregierung (2015) und in den Tallinn Manuals (2013, 2017) sowie anhand der Einschätzungen von Expert*innen wie von Heinegg (2020), Kreuzer (2019) oder Schmahl (2020) gesehen werden, dass das Völkerrecht und die dort festgehaltenen Regeln auch im Cyberbereich Geltung beanspruchen. Entsprechend »ist auch die Geltung des Gewaltverbots (Art 2 Abs 4 UN-Charta), des Interventionsverbots, des Souveränitätsprinzips sowie des Rechts auf Selbstverteidigung (Art 51 UN-Charta) im Cyberspace« (Kreuzer 2019, 65) bestätigt.[23] Sich

(23) Dabei sind nach Kreuzer die Berichte der UN-Expert*innen zwar »nicht rechtsverbindlich, haben aber aufgrund ihrer Anerkennung durch die Generalversammlung

daraus ergebende Implikationen liegen unter anderem darin, dass die USA (vgl. Finlay 2018, 358) wie auch Deutschland konventionelle Reaktionen auf Cyberangriffe als Möglichkeit festgelegt haben: In einer Antwort auf eine Kleine Anfrage der FDP-Fraktion 2018 verlautbart die Bundesregierung, dass im Fall der Einstufung eines Cyberangriffs als bewaffneter Angriff »die Bundesrepublik Deutschland mit allen zulässigen militärischen Mitteln reagieren« würde (Die Bundesregierung 2018a, 6).

⇨ 4.2 Herausforderungen von (g)CNA

⇨ 4.2.1 (Un-)Möglichkeit zu unterscheiden und kollaterale Effekte

Die für gCNA geschriebenen Programme werden häufig als digitale Präzisionswaffen bezeichnet.[24] Dabei muss jedoch beachtet werden, dass die als »Kollateralschäden« benannten Folgen in den meisten Fällen einzig »accidental harm to non-military targets« beinhalten und entsprechend »in their description of both harm (considering only physical or property), and the object of any potential harm (non-military targets only)« (Romanosky/Goldman 2016, 12) begrenzt sind. Der aus dem Bereich kinetischer Waffen abgeleitete Begriff greift, mit Romanosky und Goldman, zu kurz, da es schwierig sei »to estimate the second and third-order effects of cyber attacks on related systems, and in particular on civilian systems« (ebd.). Dies gilt insbesondere für ein enges Verständnis von »harm«: »By all accounts of military actions (…) harm would not include: inconvenience, irritation, stress, or fear, because they do not amount to ›loss of life,‹ ›injury,‹ or ›damage‹« (ebd., 14).

Aussagen, dass Cyberwaffen generell nur auf ein Angriffsziel zugeschnitten und etwaige Kollateralschäden auszuschließen seien, müssen daher präzisiert werden. Um dies auch sprachlich zu verankern, eignet sich der Begriff der »Kaskaden-Effekte« bzw. »Cybereffekte«, die Zimmermann (in Meister/Biselli 2019) in einem Gutachten für die

der Vereinten Nationen erhebliches Gewicht für den völkerrechtlichen Diskurs zum Cyberspace« (2019, 65).

(24) S. u.a. die interne Einschätzung des BMVg von 2015, wonach »[o]ffensive Cyber-Fähigkeiten (…) in der Regel nicht-letal und mit hoher Präzision auf gegnerische Ziele (…) wirken, zum Anderen [sic!] kann diese Wirkung im Gegensatz zu kinetischen Wirkmitteln unter Umständen sogar reversibel sein« (in Meister 2015).

Wissenschaftlichen Dienste des Deutschen Bundestages benennt,[25] da »[i]n technischer Hinsicht (…) beim Einsatz digitaler Waffen das anvisierte Ziel grundsätzlich nicht so ausgeschaltet werden [kann], dass unintendierte Schäden ausgeschlossen werden können« (ebd.).[26] Außerdem ließen sich »militärische, öffentliche oder private Ziele (…) kaum voneinander unterscheiden« (ebd.).

Schulze stellt die möglichen Folgen in einen noch größeren Kontext: Sollte man

> Einsatzbedingungen, operative Beschränkungen und etwaige Folgeeffekte eigener Cyber-Operationen falsch einschätzen, ergeben sich (…) enorme Risiken für Kollateralschäden, etwa in Form einer ungewollten Beeinträchtigung der zivilen kritischen Infrastruktur in Drittländern. Hieraus können sich ungünstige Eskalationsdynamiken ergeben (2020b, 8).[27]

Reinhold betont zusätzlich, dass durch das Fehlen internationaler Übereinkommen im Cyberbereich ein erhöhtes »Risiko von Fehlinterpretationen und Fehlreaktionen« bestehe (2020, 7).[28] Schließlich warnen Perkovich/Hoffman (2019) davor, dass die Verwundbarkeit von Akteur*innen sehr unterschiedlich sei und entsprechend gelte, dass Staaten wie Iran, Nordkorea, Russland und auch China bei Konflikten im Cyberraum wenig zu verlieren hätten.

Hieran anschließend muss auch die Frage der tatsächlichen Möglichkeit einer Reversibilität gestellt werden.[29] Während in der Regel Daten

(25) Da das Gutachten zwar in Meister/Biselli (2019) geleakt, aber von Zimmermann, Oberstleutnant der Bundeswehr, verfasst wurde, soll fortan bei Bezug auf das Gutachten Zimmermann als Autorenverweis dienen.
(26) Ein Beispiel hierfür ist das versehentliche Ausschalten des Internets in Syrien durch die NSA (vgl. Ackermann 2014).
(27) Vgl. auch die Ausführungen von Zimmermann (2019).
(28) Für andere Einschätzungen zum Eskalationspotential s. Borghard/Lonergan (2019) sowie Lin (2016). Auch Maness und Valeriano machen darauf aufmerksam, dass »[m]ost cyber incidents are allowed to occur without any significant response from the victim« (2016, 318). Zu untersuchen wäre hierbei, ob (Kaskaden-)Effekte wie ein mittelfristiges Steigern der Rüstungsausgaben im Cyberbereich als »significant response« eingeordnet würden oder, wenn sie als ein »second or third order effect« gezählt werden, dort entsprechend nicht auftauchen.
(29) Vgl. Fußnote 24.

durch Backups gesichert sind, stellt sich dies bei gCNA (s. 3.3.2) anders dar. Deutlich weitgehender sind auch Folgen durch Kollateraleffekte, die entsprechend keine bzw. wenig Reversibilität zulassen: Verlorenes Vertrauen in staatliche Infrastruktur ist beispielsweise schwerlich wieder aufzubauen (vgl. Altmann 2019, 90).

Abschließend kann festgehalten werden, dass Kollateralschäden, insbesondere im umfassenden Sinne von Kollateraleffekten, beim Einsatz von Cyberoperationen nicht ausgeschlossen werden können.

⇨ 4.2.2 Die (Un-)Möglichkeit der Proportionalität bei Gegenangriffen

Ein weiterer Aspekt ist die Frage nach der Proportionalität bei Cyberoperationen. Wie dargelegt, ist nicht nur das Erkennen von Cyberangriffen problematisch (vgl. u.a. 4.1.2), sondern auch die Identifizierung der betroffenen Netzwerke und das Ausmaß der Schäden. Da zu treffende »Gegenmaßnahmen (…) notwendig und verhältnismäßig sein [müssen]« und gleichzeitig »Cyberangriffe nur gegen unmittelbar ablaufende Cyberangriffe zulässig sind« (Kreuzer 2019, 79), stellt sich hier die besondere Herausforderung in der Bewertung solcher Maßnahmen und der damit einhergehenden Folgen. Umso mehr, da gilt: Wenn »der Cyberangriff beendet oder unterbunden [ist], müssen Gegenmaßnahmen eingestellt werden« (ebd.).

⇨ 4.2.3 Langfristigkeit der Vorbereitungen

Zwei weitere Aspekte sollen durch ein Zitat von Oeter beleuchtet werden:

> Um im Ernstfall auch offensiv operieren zu können, bedarf es jedoch weit im Vorhinein des Aufbaus entsprechender Kapazitäten – und des Entwickelns von Handlungsroutinen für derartige Operationen, des Austastens der Sicherheitsstandards potenzieller Gegner, letztlich auch des Anlegens und der Pflege möglicher Zugänge zu geschützten gegnerischen Netzen (etwa über ›backdoors‹ und ›exploits‹) (2020b, 107).

Oeter beschreibt, dass Cyberoperationen und die dafür eingesetzten Programme langfristig geplant und vorbereitet werden müssen. Mit Schulze ergibt der notwendige Zeitraum von »Monaten bis Jahren« eine »Vorfeldverlagerung« (2020b, 29). Dies zeigt, dass die Vorberei-

tungen für gCNA frühzeitig, also »bereits in Friedenszeiten entwickelt [werden], um im Konfliktfall einsatzbereit zu sein« (ebd.).

Die Notwendigkeit »des Anlegens und der Pflege möglicher Zugänge« zeigt noch einen zweiten, oftmals vernachlässigten Aspekt: Das unabdingbare und systematische Beschaffen und Vorhalten von »Kenntnisse[n] über Zielsysteme, deren Erreichbarkeit und Schwächen« (Reinhold 2020, 6).[30] Dies erfolgt beispielsweise durch den Kauf von sog. Zero-Day-Exploits: Hier werden Sicherheitslücken u.a. in Betriebssystemen als Zugänge für einen eigenen Angriff geheim gehalten.[31] Als Beispiel möglicher Folgen kann der Cyberangriff NotPetya im Jahr 2017 angeführt werden: Obwohl der NSA die Sicherheitslücke EternalBlue im Windows-Betriebssystem bekannt war, wurde diese zurückgehalten und nicht an den Hersteller gemeldet (vgl. ebd.). Durch einen Hackerangriff auf die NSA wurden jedoch Informationen hierüber erbeutet und ein großflächiger Angriff gestartet, der weltweit einen Schaden von mehreren Milliarden Dollar verursachte (vgl. Reinhold 2017). Als weiterer Aspekt kann auch »Reverse-Engineering«, i.e. das Nutzen einer Angriffssoftware durch den Angegriffenen, eine mögliche Folge einer CNA sein, wie dies im Fall der Wiper Malware durch den Iran zu sehen war (vgl. Perkovich/Hoffman 2019). Damit potenziert sich gleichzeitig die Suche nach Exploits: »Der steigende Bedarf durch staatliche Stellen für derartige Informationen fördert deren Marktwert und schafft Anreize für Unternehmen zum Aufkauf und Handel mit diesen Informationen« (Reinhold 2020, 5). Entsprechend können, im Anschluss an die Ausführungen in 4.2.1, auch durch das Offenhalten oder den Einbau von Sicherheitslücken kollaterale Effekte entstehen – noch vor einer gCNA.

⇨ 4.2.4 Von der (Un-)Möglichkeit einer wirksamen Abschreckung

Nach Schulze (2019, 1) müssen für eine wirksame Abschreckung drei Voraussetzungen erfüllt sein: Die*der potentielle Angreifer*in muss identifiziert sein, es müssen entsprechende Wirkmittel für einen kontrollierten Einsatz zur Verfügung stehen und die Drohung eines Gegenschlags muss als glaubwürdig erachtet werden. Dass die Voraussetzungen im Cyberbereich grundsätzlich schwierig zu erfüllen sind,

(30) Vgl. die Dreiteilung bei von Heinegg in 3.1.

(31) Koch, R. (2020, 6) benennt dies mit dem als »Pflegeaufwand« beschriebenen »Nachteil eines Cyberwirkmittels (…), wenn bspw. zu nutzende Schwachstellen aktualisiert werden müssen«.

zeigte die Analyse in 4.1.1.[32] Für die zweite Bedingung kann auf 4.2.1 und 4.2.3 verwiesen werden. Die Frage der Glaubwürdigkeit als dritte Bedingung stellt sich bei Cyberoperationen, die im Geheimen vorbereitet werden müssen und eine Zurschaustellung verhindern, ebenfalls. Entsprechend wird von einem »Abschreckungsdilemma« (vgl. Libicki in Reinhold/Schulze 2017, 11) gesprochen, über das Mielke ausführt, dass »noch weitgehend offen« sei, »[w]ie eine ›tailored deterrence‹ für Cyberkonflikte aussehen kann« (2020, 84). Auch empirisch zeigt sich an den großflächigen Angriffen auf die USA, sowohl im Rahmen des US-Wahlkampfs 2016 als auch auf Ministerien 2020, dass keine wirksame Abschreckung erreicht wurde.[33]

⇨ 4.2.5 Von der Möglichkeit des Absinkens der Schwelle zum Einsatz

Die teils vorhandene Einschätzung von Cyberoperationen als präzise (vgl. 4.2.1) deutet bereits an, dass Cyberoperationen »für westliche Demokratien prima facie (…) außerordentlich attraktiv« sind (Schörnig 2019a, 40). Dies wird bestärkt durch die Annahme, dass diese günstiger seien als konventionelle Rüstungsprojekte, nicht zuletzt weil sie »gezielt unterhalb bewaffneter Konflikte durchgeführt werden (…) und keinen Einsatz menschlicher Kräfte mit boots on the ground« (Reuter u.a. 2019, 27) notwendig machen. Im Umkehrschluss wird darauf aufbauend vor einem Absinken der »Hemmschwelle zum Einsatz offensiver Cyberkapazitäten« (Schörnig 2019a, 55) gewarnt. Die Frage nach der Kostspieligkeit von Cyberoperationen wird mitunter aber auch anders eingeschätzt: So halten Reinhold/Schulze (2017, 12) neben den notwendigen Personalkosten auch »das Aufstellen von Arsenalen mit einsatzbereiter digitaler Gegenschlags-Software [für, mw] enorm kostspielig. Komplexe Sicherheitslücken, sofern man sie nicht durch eigenen Personalaufwand entdeckt, kosten je nach Zielsystem Hunderttausende oder gar Millionen von Euro« und haben »[l]aut einer Studie der RAND Corporation (…) eine durchschnittliche Lebenszeit von 6,9 Jahren« (ebd.), was die Notwendigkeit einer regelmäßigen Aktualisierung mit sich bringt.

(32) Vgl. für die Verbindung der Voraussetzungen auch Huth (1999, 26).

(33) Vgl. für weitere Ausführungen Schulze (2019), Perkovich/Hoffman (2019) sowie Zimmermann (2019). Zimmermann spricht bezogen auf das Erreichen einer Cyberabschreckung von einem »Scheitern« der USA und schätzt den Erfolg für Deutschland als »eher unwahrscheinlich« ein (ebd.).

⇨ 4.3 Zwischenfazit Kapitel 4

Die Ausführungen geben einen Überblick über Herausforderungen für die friedensethische Bewertung von Cyberoperationen. Während diese Übersicht aufgrund des begrenzten Umfangs dieses Artikels keinen Anspruch auf Vollständigkeit erhebt, bieten die aufgeführten Punkte gleichwohl eine ausreichende Grundlage für die nachfolgende Analyse.

⇨ 5. Gerechter Frieden und Cyberoperationen – Synthese

Das nachfolgende Kapitel führt die Inhalte der Kapitel 2 bis 4 zusammen. Als Struktur der Analyse dienen die sieben Kriterien aus dem Leitbild des Gerechten Friedens.

⇨ 5.1 To Hack Back or Not? Eine Kriterienanalyse

Aktuell wird die Frage nach dem Einsatz von Hackbacks in Deutschland diskutiert (vgl. Zimmermann 2019). Hackbacks sollen eingesetzt werden, um einen Cyberangriff auf eigene Netze in »Echtzeit zu stoppen, Daten zu löschen oder Rechner zu deaktivieren« (Schulze 2019). Während u.a. Leinhos hierfür einen »digitalen Verteidigungsfall« (in Becker 2019) schaffen will, ist verfassungsrechtlich noch unklar, inwiefern diese überhaupt legitim sind (vgl. Kipker 2019). Dazu stellt sich die Frage, welche Institution hierfür infrage käme. Während die Bundeswehr qua des obig ausgeführten Profils bereits in diesem Bereich operiert, gehen andere Überlegungen in Richtung des BSI oder des Bundesnachrichtendienstes (vgl. Biselli 2020; Mascolo/Steinke 2019).[34] Da die Debatte um Hackbacks eine friedensethische Antwort durch die Überprüfung der Kriterien des Leitbilds des Gerechten Friedens bisher entbehrt, soll die nachfolgende Analyse durch ein einfaches, fiktives Szenario[35] begleitet werden.

> *Das Szenario besteht aus einem weitreichenden Hackerangriff, von dem u.a. KRITIS wie Regierungs-, Krankenhaus- und Bundeswehrserver in Deutschland betroffen sind. Nachdem dieser detektiert wurde, stellt sich die Fra-*

(34) Vgl. die Ausführungen in 3.2.
(35) Vgl. auch die Vorgehensweise in Hering/Schubert (2012).

ge nach einer unmittelbaren Reaktion durch einen Hack-back.

Es ist klar, dass die Herausforderungen und Implikationen, die in einem realen Fall hieraus folgen würden, weitaus vielschichtiger sind. Gleichwohl können bereits hier Hürden und Eckpunkte für die ethische Bewertung identifiziert werden.

⇨ 5.1.1 Kriterium 1: Erlaubnisgrund

Durch die in der Denkschrift angelegte grundsätzliche Möglichkeit einer legitimen Anwendung von Gewalt besteht diese auch für Hackbacks, i.e. als Anwendung von Gewalt (s. 3.3.2). Für diese müssen das im Kriterium benannte, notwendige »Maß« erfüllt und ein Angriff als »schwersten, menschliches Leben und gemeinsam anerkanntes Recht bedrohenden Übergriff« (Zi. 102) zu kategorisieren sein. Während letale Cyberangriffe bisher non-existent waren, könnte durch einen großflächigen Angriff auf KRITIS, beispielsweise Krankenhäuser, eine solche Schwelle überschritten werden. Dabei besteht jedoch das Risiko einer falschen Einordung eines Cyberangriffs (vgl. 4.1.2): Weil regelmäßig Spionageoperationen (CNE) in externen Netzwerken stattfinden, besteht die Schwierigkeit, diese »nur« als solche und nicht als »Vorbereitung« bzw. CNA einzuordnen oder einen Zusammenhang mit dem aktuellen Angriff herzustellen.[36] Hierbei stellt sich auch die Frage, inwiefern bei einem Angriff überhaupt von einem Gewaltakt (s. 3.3.2) gesprochen werden kann: Da es für die Einordnung als Gewaltakt notwendig ist, die Motivation der angreifenden Partei zu kennen, ist weitreichendes Vorwissen unabdingbar. Wie in 4.1.2 beschrieben liegt eine exakte Bestimmung des Ausmaßes schwerlich innerhalb kurzer Zeit vor. Damit unmittelbar verknüpft sind auch die in Kriterium 2 benannte Autorität und der Verweis auf das Selbstverteidigungsrecht: In der Regel kann, gerade bei über einen längeren Zeitraum durchgeführten Angriffen, kaum von einer unmittelbar stattfindenden Selbstverteidigung und damit einem legitimen Grund für eine militärische Gegenreaktion gesprochen werden (vgl. Reinhold/ Schulze 2017, 9). Die Frage ist also, ob im Regelfall überhaupt von

(36) S. Schmahl, derzufolge »Computer Network Exploitation oder Cyberspionage (…) im rein zwischenstaatlichen Verhältnis zu keinen nennenswerten völkerrechtlichen Problemen [führt]. Werden lediglich Mobiltelefone, Computer oder sonstige internetbasierte Daten von Staatsorganen durch hoheitlich eingeschleuste Spyware ausspioniert, liegt grundsätzlich kein Verstoß gegen das völkerrechtliche Interventionsverbot vor« (2020, 90).

einem »Gegen« der Gewalt gesprochen werden kann.[37] Dass beim vorliegenden Szenario menschliches Leben unmittelbar bedroht sein kann, ist nicht von der Hand zu weisen. Damit kann dieser Aspekt des Kriteriums durchaus erfüllt sein. Gleichwohl zeigen die weiteren Ausführungen, dass insbesondere die Detektion gravierende Hürden darstellt.

⇨ 5.1.2 Kriterium 2: Autorisierung

Das zweite Kriterium bezieht sich in den Ausführungen explizit auf die Ebene der UN als der einzigen Institution, die einen Einsatz von Gewalt legitimieren kann. Dies hat für Cyberoperationen zur Folge, dass, abgesehen von einem Einsatz zur Selbstverteidigung, das Gewaltverbot und somit ein Verbot von gCNA generelle Gültigkeit hat. Wenn diese als selbstverteidigende Maßnahmen ergriffen werden, sind sie nur so lange legitim, bis sich der UN-Sicherheitsrat damit befasst hat. Ob dies jedoch auch für Hackbacks gilt, ist offen: Im Gutachten von Zimmermann heißt es, dass die »völkerrechtliche Zulässigkeit grenzüberschreitender Abwehrmaßnahmen (…) zweifelhaft« sei (2019). Dabei wirft auch die Notwendigkeit der Geheimhaltung von Cyberoperationen, deren Vorbereitungen sowie konkreter Einsätze die Frage auf, inwiefern eine sachlich fundierte Entscheidung öffentlicher Gremien möglich ist. Dies gilt insbesondere, da eine Zustimmung des Bundestags für »bewaffnete Unternehmungen« ein »Kernkriterium« (Schulze 2020b, 8) ist. Entsprechend müssen Politiker*innen ausreichend Kenntnis besitzen, um die Reichweite und den Rahmen eines Einsatzes zu bestimmen. Diese Frage wird bei Hackbacks umso dringlicher, da diese als unmittelbare Reaktion vorgesehen sind. Es lässt sich jedoch bisher feststellen, dass der (öffentliche) Diskurs auch innerhalb des Bundestags nur in Ansätzen geführt und vonseiten der Bundesregierung stark eingeschränkt wird.[38] Überlegungen, dass die Entscheidungen zu einem Hackback nicht vom Bundestag, sondern von Behördenleitungen getroffen werden sollen (vgl. Koch, W. 2020,

(37) Wenn mittels Cyberoperationen unmittelbar auf einen konventionellen Angriff reagiert würde, stellte sich diese Frage entsprechend nicht.

(38) S. u.a. die Antworten auf Anfragen von Parteien, die meist die Aussage enthalten: »Die Fragestellung berührt derart schutzbedürftige Geheimhaltungsinteressen, dass auch ein geringfügiges Risiko des Bekanntwerdens, wie es auch bei einer Übermittlung an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In diesem Fall überwiegt daher das Staatswohlinteresse gegenüber dem parlamentarischen Informationsrecht« (Die Bundesregierung 2019).

29), sind vor dem Hintergrund der Denkschrift kritisch zu bewerten. Auch die NATO scheidet nach der Denkschrift, sofern sie unabhängig von einem UN-Mandat agiert, als Akteurin explizit aus (Zi. 122). Die Ausführungen zeigen, dass diesem Kriterium derart hohe Hürden zugrunde liegen, dass eine Erfüllung unwahrscheinlich ist.

⇨ 5.1.3 Kriterium 3: Richtige Absicht

Das Abwehren »eines evidenten, gegenwärtigen Angriffs« ist mit weitreichenden Herausforderungen versehen: Den Ausführungen der Denkschrift liegt eine strikte Ablehnung von präemptiven und präventiven Angriffen zugrunde, solange diese nicht »evident« sind. Eine »Früherkennung« von Planungen und selbst unmittelbar bevorstehenden Cyberangriffen ist aber kaum möglich (s. 4.1.2).[39] Entsprechend scheinen einzig Reaktionen denkbar, was Hackbacks durchaus entsprechen würde. Dass zwar Cyberoperationen im Sinne von Selbstverteidigung grundsätzlich als völkerrechtlich legitim eingeordnet wurden, wurde gezeigt – inwiefern jedoch die völkerrechtliche sowie grundgesetzliche Zustimmung bei Hackbacks gegeben ist, ist noch zu klären (vgl. Krit. 2). Grundvoraussetzungen dafür sind jedoch die Attribution sowie eine geeignete Konzeption (s. 4.1.1). Dass ersteres in aller Regel unklar bleibt, stellt daher für jegliche Reaktion eine Herausforderung und mithin eine gravierende Einschränkung für die Erfüllung dieses Kriteriums dar. Ein bisher in der Forschungslandschaft wenig beleuchteter Aspekt im Rahmen der Konzeption ist die Frage nach einem Ende des Einsatzes bzw. der Operation. Kurz/Rieger (2018, 168) sehen darin eines der grundlegenden Probleme, da Elemente jeder militärischen Strategie in Form eines klaren Ziels verloren gehen: »In der Regel gibt es kein definiertes Ende, keinen Friedensschluss, keine Nachkriegsordnung, keine Kodifizierung der entstandenen Machtverschiebungen.« Auch wenn Hackbacks als »Gewaltgebrauch (…) zur Abwehr eines (…) Angriffs« verstanden werden können, stellen die Adjektive »evident« und »gegenwärtig« weitreichende Herausforderungen dar. Darüber hinaus werden durch die bestehende Asymmetrie konzeptionelle Fragen aufgeworfen, welche die Komplexität weiter erhöhen[40] und die Möglichkeit einer Ge-

(39) Wie obig beschrieben gilt dies sogar für gerade stattfindende Angriffe.

(40) Beispielhaft sei hier an Hering/Schubert erinnert: Die dortig vorgenommene Einordnung des Beispiels als »legitim«, obwohl das im Rahmen der Operation durchgeführte »Lynchen« (!) von Gaddafi »nicht hätte passieren dürfen« (2012, 214), zeugt davon. Aus der Sicht des Autors dieser Arbeit würde für das konkrete Beispiel u.a. anhand dieses Kriteriums ein

samtkonzeption erschweren: Wenn innerhalb von »Minuten« (Leinhos in Lilienström 2020) ein Gegenangriff vorbereitet, erstellt, abgestimmt (s.o. 5.1.2) und durchgeführt werden soll, scheint eine Erfüllung dieses Kriteriums insbesondere durch die kaum mit Sicherheit zu treffende Attribution nahezu unmöglich.

⇨ 5.1.4 Kriterien 4 bis 6: Eine Frage der Folgen und Mittel

Aufgrund der inhaltlichen Nähe sollen die Kriterien 4 bis 6 gemeinsam betrachtet werden. Dabei bietet sich ein chronologischer Zugang an. Der erste bei einem Angriff auf eigene Systeme notwendige Schritt ist die Detektion. Hierbei stellt sich unmittelbar die Frage sowohl nach der Art, dem Ziel sowie dem Ausmaß des Angriffs. Jeder dieser Punkte für sich ist hochkomplex und meist bereits ein Ergebnis von Interpretationen. Um zu bestimmen, wie ein Gegenangriff aussehen soll, müssen diese Ergebnisse jedoch vorliegen. Erst daran kann sich die Frage, welche Mittel »aller Voraussicht nach hinreichend wirksam« sind und gleichzeitig »Leid und Schaden auf das notwendige Mindestmaß (…) begrenzen«, anschließen (s. 4.2.2). Wenn eine Reaktion auf einen Angriff via Hackback erfolgen soll, ist das Ziel, diesen mit möglichst wenig Zeitverzögerung durchzuführen. Neben den Fragen, die sich bereits in Kriterium 1 stellten, müssen hier auch Attributionen sowie mögliche Folgen dieser Gegenangriffe thematisiert werden. Für Attributionen ist wie beschrieben im Regelfall eine komplexe Untersuchung vonnöten. Dazu können Hackbacks weitreichende kollaterale Effekte hervorrufen (s. 4.2.1). Da Angriffe im Regelfall über zwischengeschaltete Server stattfinden, sind ein Hackback und mithin das Ausschalten dieser Server auch insofern relevant, da diese in (unbeteiligten) Drittstaaten liegen können. Zusätzlich besteht die Gefahr von Kaskadeneffekten, nicht zuletzt durch *False Flags*. Wenn entsprechend ein Hackback andere Adressat*innen trifft, bei denen ein Abschalten des Servers als Angriff aufgefasst wird, kann ein Selbstverteidigungsfall und eine sich anschließende Eskalation provoziert werden. Dabei ist auch ein versehentliches Abschalten von *KRITIS* möglich.[41] Entsprechend ist der in Kriterium 5 explizierten Forderung,

Nichterfüllen aller Kriterien konstatiert und ein solcher Einsatz entsprechend nicht in Übereinstimmung mit den Kriterien der Ethik rechtserhaltender Gewalt gesehen werden.

(41) Dass dies sogar ein direktes Ziel sein kann, führt die Konzeption der Bundeswehr explizit aus: »Technische Entwicklungen im kinetischen Spektrum in Verbindung mit dem Cyberraum verschaffen neue Möglichkeiten des Handelns, etwa durch die zeitlich

keine größeren Schäden als die hervorgerufenen zu verursachen, *per se* schwerlich nachzukommen, da die entsprechenden Ausmaße kaum bestimmbar sind.

Ein weiterer Aspekt liegt in der Notwendigkeit, Sicherheitslücken zu erlangen oder sogar in Systeme einzufügen (s. 4.2.3). Durch das Zurückhalten oder sogar den bewussten Einbau von Exploits besteht sowohl die Gefahr, dass das Wissen darüber bei einem Hack der eigenen Systeme entwendet und gegen diese verwendet,[42] als auch, dass die Lücken von anderen Akteur*innen gefunden und genutzt werden. Der potentiell verursachte Schaden kann deutlich höher wiegen als die *Möglichkeit* der Nutzung.[43] Dieser Aspekt (s. 4.2.3) zeigt, dass notwendige langfristige Vorbereitungen von (g)CNA mit einer Vielzahl von Risiken einhergehen. Auch die Annahme niedrigerer Kosten muss in Frage gestellt werden (s. 4.2.5). Dies gilt nicht zuletzt auch vor dem Hintergrund einer finanziellen wie auch personellen Begrenztheit von Ressourcen. Die in der Denkschrift getroffene Formulierung legt dabei eine strenge Auslegung nahe (»…*alle* wirksamen Mittel…«), wobei durch die gegenwärtige Ressourcenverteilung zwischen ministerialen Ressorts grundsätzlich ein Ungleichgewicht bereits im Vorlauf möglicher Eskalationen zu konstatieren ist.

Ebenfalls der Frage nach der Verhältnismäßigkeit der Mittel wie auch der Folgen kann der Ansatz der Abschreckungsstrategie zugeordnet werden (s. 4.2.4).[44] Wie dargestellt, stellen das »Attributionsproblem« sowie die Gefahr kollateraler Effekte bereits große Herausforderungen zur Erfüllung des Kriteriums dar. Auch wenn Atomwaffen und Cyberoperationen hier nicht direkt verglichen werden sollen, gilt das zugrundeliegende Argument zur Abschreckung (Zi. 109) durchaus: Dass eine »Cyber-Abschreckung (…) multipolar und zwischen asymmetrischen Opponenten« (Schulze 2019, 2) angelegt sein müsste,

koordinierte Beeinflussung gegnerischer Systeme und kritischer Infrastrukturen« (BMVg 2018, 47).

(42) Zum Nachweis, dass dies nicht fiktiv ist, vgl. das obige Beispiel EternalBlue.

(43) Hierbei muss betont werden, dass Sicherheitslücken auch von Geheimdiensten genutzt werden, wobei das Risiko hier wie dort identisch ist. Dabei ergibt sich generell die Frage, wie das Leitbild des Gerechten Friedens Spionage und geheimdienstliche Aktivitäten einstuft und inwiefern in dieser Praxis eine Problematik gesehen wird.

(44) Dieser Ansatz steht zum Szenario in einem wechselseitigen Verhältnis: Einerseits könnten Hackbacks (nach herkömmlichen Theorien, s.o.) zum Entstehen einer Abschreckung beitragen, wenn klar wäre, dass diese eingesetzt würden. Nach dieser Einschätzung wäre ein tatsächlicher Einsatz durch die entsprechende Abschreckung gleichzeitig unwahrscheinlich.

führt vielfach zur Einschätzung, dass ein »Zurückgreifen auf eine Abschreckungslogik und der Aufbau von Bedrohungspotenzial (…) nicht [funktionieren], da der Gegner auch an anderer Stelle zuschlagen könne« (Brüßler 2019).[45] Auch die empirische Studie von Valeriano/Jensen deutet darauf hin: »Attacks do not beget attacks, nor do they deter them« (2019, 1). Entsprechend unwahrscheinlich ist es, dass sich Cyberoperateur*innen von einer staatlichen Abschreckungspolitik abhalten lassen. Damit zusammen hängt schließlich auch die Frage nach der Wirksamkeit und Effektivität von Hackbacks: Wie Reinhold (2020, 8; s. 4.2.4) verdeutlicht, kann das Ausschalten eines Servers zwar möglicherweise eine temporäre Unterbrechung bewirken, Hacker*innen werden hierfür jedoch »geeignete Redundanzmaßnahmen, auf die gegebenenfalls ausgewichen werden kann, in die Angriffsstruktur einbauen«. Auch die Effektivität von Hackbacks ist demzufolge sehr begrenzt.

⇨ 5.1.5 Kriterium 7: Unterscheidungsprinzip/Diskriminierung

Dass kollaterale Effekte bei Cyberoperationen nicht ausgeschlossen werden können (s. 4.2.1), gilt auch bei Hackbacks (s. 5.1.4). Dabei zeigt sich im Besonderen die Herausforderung, inwiefern angreifende Cyberoperateur*innen als Kombattant*innen eingeordnet werden.[46] Personen und Einrichtungen zu schonen, wie im Kriterium benannt, kann hierbei explizit auch auf Server bezogen werden, die selbst gekapert und zwischengeschaltet für einen Cyberangriff genutzt wurden, deren Betreiber*innen damit jedoch selbst Betroffene und somit Nicht-Kombattant*innen sind. Gerade hierfür besteht die Gefahr unkontrollierter Kaskadeneffekte. Auch die zunehmende Vermischung zwischen Zivilem und Militärischem kann hier eingeordnet werden, die durch COTS, die Abhängigkeit von Unternehmen sowie die Vielzahl von Akteur*innen eine trennscharfe Unterscheidung erschwert (s. 4.1.3). Dies gilt auch und gerade vor dem Hintergrund, dass »IT-gesteuerte Waffensysteme, militärische Kommunikationsnetzwerke, Hauptquartiere und weltweit verteilte Kommunikationsleitstellen« (Schulze 2020b, 23) Teil nahezu jeder militärischen Operation sind

(45) Dabei kann eine Parallele zum sog. »War on Terror« gesehen werden (vgl. Münkler 2018, 579).

(46) Dass »gewohnheitsrechtlich mittlerweile viele Regelungen aus dem Recht der internationalen bewaffneten Konflikte analog auf das Recht nicht-internationaler bewaffneter Konflikte übertragen« (Koch, R. 2019, 89) werden, zeugt von einem zunehmend inklusiven Verständnis des Unterscheidungsgebots.

und viele digitale Schnittstellen aufweisen, die potentielle Ziele darstellen können (vgl. Koch, R. 2020, 6). Im Lichte der Ausführungen muss hinsichtlich des Unterscheidungsprinzips bei Hackbacks festgehalten werden, dass eine Erfüllung kaum möglich ist.[47]

⇨ 5.2 Zwischenfazit Kapitel 5

Mit den Ausführungen wurde eine Vielzahl an Herausforderungen und Hürden aufgezeigt, die aus der Perspektive einer Ethik rechtserhaltender Gewalt beim Einsatz von Hackbacks bestehen. Als Zwischenfazit kann festgehalten werden, dass Hackbacks die Kriterien bei strikter Anwendung in der Regel nicht in ihrer Gesamtheit erfüllen können. Dies gilt insbesondere für Fragen der Attribution, von kollateralen Effekten sowie der damit zusammenhängenden (Nicht-)Unterscheidbarkeit von Kombattant*innen. Den Ausführungen folgend ist auch ein Aufbau zu Abschreckungszwecken abzulehnen.

⇨ 6 Alternative zu Kriterien oder Alternative zu gCNA?

Mit dem Ergebnis der Analyse können unterschiedliche Schlüsse gezogen werden. Eine Perspektive ist die Ablehnung von Hackbacks und damit einhergehend die Frage nach einem alternativen Vorgehen. Ein zweiter Ansatz besteht darin, die Bewertungskriterien für Cyberoperationen anzupassen. Im Kapitel 6.1 soll mit letzterem Ansatz begonnen, ehe in 6.2 alternative Ansätze innerhalb des Frameworks des Gerechten Friedens ausgeführt werden.

⇨ 6.1 Aus dem Rahmen (ge)fallen?

⇨ 6.1.1 Eine Frage der Auslegung?

Explizit stellt beispielsweise Oeter die Frage, inwiefern alle Kriterien bei Cyberoperationen gelten müssen:

> Insgesamt wird man hier – jedenfalls im Kontext des bewaffneten Konfliktes – die Maßstäbe der Beweisbarkeit

(47) Inwiefern die Herausforderung, dass die Folgen eines Cyberangriffs nicht abschätzbar sind, Soldat*innen im Bereich der »Inneren Führung« zu einer Befehlsverweigerung bringen kann, könnte als separater Forschungsbereich weiterbearbeitet werden. Grundsätzlich wird auch in der Denkschrift der EKD die individuelle Verantwortung von Soldat*innen betont (Zi. 65).

> erheblich absenken müssen und hinreichende Sicherheit in der Zuweisung der Autorenschaft ausreichen lassen müssen (2020b, 99).

Dieser Ansatz findet sich auch im Tallinn Manual wieder (vgl. Kreuzer 2019, 71).

Darüber hinaus wird häufig angeführt, dass der explizite Bezug auf den UN-Sicherheitsrat insbesondere bei Cyberoperationen keinen sinnvollen Rahmen darstelle (vgl. Oeter 2020a, 129).

⇨ 6.1.2 Besser konventional als digital?

Dass bestimmte Charakteristika wie obig aufgezeigt nur für digitale und nicht für kinetische Angriffe gelten, zeigte zwar deren Unterschiedlichkeit. Übergeordnet jedoch gilt durch die angewendete Definition, dass beide als Einsatz von Gewalt zu beurteilen sind. Dies böte entsprechend die Möglichkeit, auf einen Cyberangriff mit konventionellen Mitteln reagieren zu dürfen (vgl. Finlay 2018, 374). Bezogen auf das obige Szenario ist die Einschätzung in der Konsequenz jedoch gleich: Die Attributionsproblematik stellt jede Art von Reaktion vor kaum zu lösende Aufgaben. Es bleibt also festzuhalten, dass in der Theorie eine gewaltsame, konventionelle Reaktion möglich wäre, die jedoch, bei Betrachtung des konkreten Beispiels, vor ähnlichen Problemen steht.

⇨ 6.1.3 Zwischenfazit Kapitel 6.1

Während eine kritische Auseinandersetzung mit den Kriterien legitim ist, birgt eine Ablehnung bereits einzelner Kriterien weitreichende Risiken, die zu einer Umkehrung der Beweisstandards führen können. Darüber hinaus spräche die Analyse, selbst wenn ein Kriterium ausgeklammert würde, für eine Ablehnung von Hackbacks. Nicht zuletzt ist vor dem Entstehen eines parallelen Sets von Kriterien für Einsätze im Cyberraum zu warnen, da hiermit Abgrenzungsprobleme zwischen Kriterienkatalogen entstehen könnten. Cyberoperationen und insbesondere gCNA können zwar als neue Ausprägungsformen von Gewalt angesehen werden. Dass die im Framework enthaltenen Kriterien deshalb zwangsläufig geändert bzw. abgesenkt werden müssten, heißt dies aber mitnichten, insbesondere, da es durchaus Alternativen zu Hackbacks gibt, die innerhalb des Leitbilds und ohne Anwendung

von Gewalt umsetzbar sind. Überlegungen hierzu sollen im nachfolgenden Kapitel erörtert werden.

⇨ 6.2 Alternativen zu gCNA

Die Zielperspektive der Denkschrift, die über eine Überprüfung der Kriterien hinausgeht, stellt »eine kooperativ verfasste Ordnung ohne Weltregierung [dar, mw]. Die Mittel einer solchen kooperativen Weltordnung sind Institutionen auf globaler und regionaler Ebene, insbesondere internationale Organisationen und Regelwerke« (Zi. 86). Dabei zeigt sich auch im Cyberbereich, dass vor allem auf der Ebene der UN, aber auch im Bereich von Unternehmen und der Zivilgesellschaft bereits Ansätze bestehen, die auf eine Stärkung der eigenen System-Resilienz sowie internationaler Normen hinwirken.

⇨ 6.2.1 Cyber Diplomacy

Die Hauptansätze hierbei sind staatlich-diplomatischer Natur und liegen u.a. im Aufbau einer »international community of diplomats within cyberspace« (Riordan 2019, 111). Beispielhaft kann der im Auswärtigen Amt angesiedelte Bereich der zivilen Cyberaußen- und Cybersicherheitspolitik benannt werden, über den Deutschland auch auf Ebene der UN wie auch in Regionalorganisationen (u.a. der OSZE) aktiv ist.[48] Dabei können die Ansätze zumeist als »vertrauensbildende Maßnahmen« kategorisiert werden, wenn auch auf unterschiedlichen Ebenen (vgl. Neuneck 2017, 812). Dazu wird beispielsweise die »Einführung einer unabhängigen Institution im Rahmen der Vereinten Nationen für Attribution« (Reuter u.a. 2019, 31) angeregt, unter deren Dach bei Angriffen staatenübergreifende Möglichkeiten zur Nachverfolgung entwickelt werden könnten.[49] Die mit einem solchen Ansatz verbundene Internationalisierung auf der UN-Ebene ließe sich in die Ausführungen der EKD-Denkschrift integrieren, die – wie im Zuge der Terrorismusbekämpfung – »eine wirksame Strafverfolgung (…) und eine internationale Strafgerichtsbarkeit« fordert (Zi. 106). Dabei könnte beispielsweise das Instrument der Sanktionierung zum Einsatz

(48) Auch wenn Treffen mitunter ohne Einigung verliefen (vgl. Schulze 2020a), stellen sie trotzdem einen wichtigen Austauschrahmen dar, besonders in Zeiten schwindender Multilateralität.

(49) Dass hiermit eine generelle Rückverfolgbarkeit von Cyberoperationen einherginge (auch die der eigenen!), könnte wie beschrieben ein Grund für eine Ablehnung derselben sein (vgl. Kreuzer 2019, 84) – was aus normativer Sicht jedoch nicht dagegen spricht.

kommen (vgl. Zi. 130; Werthes 2019). Mit der *Cyber Diplomacy Toolbox* (vgl. Council of the European Union 2017) findet sich auch auf Ebene der EU ein Instrument »with the aim to influence the behaviour of potential aggressors, taking into account the necessity and proportionality of the response« (Moret/Pawlak 2017, 1).

Insgesamt zeigt sich ein zunehmendes Bewusstsein der Problematik und Lösungsversuche in akteur*innenübergreifenden, globalen Ansätzen, u.a. in der Digitalen Genfer Konvention sowie dem Paris Call (2018). Dabei können Unternehmen wie auch NGOs zentrale Rollen als »third type mediators« einnehmen:

> [E]ntrepreneurs – from think tanks, activist organizations, universities, transnational businesses – can offer non-national, nonprofit perspectives that often are necessary to identify the accommodations that all actors will need to make in order to minimally satisfy competing interests (Perkovich/Hoffman 2019).

⇨ 6.2.2 Deutschland als Norm-Entrepeneur?

Wie beschrieben sind auch Akteur*innen der Bundesregierung »erfolgreich in Gremien der Normen- und Regelsetzung für den Cyberraum, etwa in den Arbeitsgruppen für Informationssicherheit der Vereinten Nationen« (Zimmermann 2019). Entsprechend könnten diese bei der Etablierung neuer Normen im Cyberbereich eine Rolle als »norm entrepreneurs« (Wunderlich 2013, 32) einnehmen.[50] Japan könnte als Vorbild dienen (vgl. Schuetze 2020a), das vorrangig »Aufklärung und Überwachung im Innern« durchführt und für die »Cyber-Verteidigung und Cyberabwehr (…) nicht in die Netze anderer Staaten« eingreift (Schuetze 2020b, 4).[51] Eine solche Ausrichtung würde die Rolle Deutschlands als Norm Entrepreneur stärken. Hierauf könnte, auch vonseiten kirchlicher Akteur*innen, ein stärkerer Fokus gelegt werden, wie ihn der frühere Friedensbeauftragte des Rates der EKD, Renke Brahms, forderte (vgl. 2020, 3). Neben einer Stärkung wissen-

(50) Vgl. für den Prozess der Normbildung u.a. Finnemore/Sikkink (1998); Wunderlich (2013).

(51) Als Beispiel für eine solche Übung in Deutschland kann die »LÜKEX 21« (Länder- und Ressortübergreifende Krisenmanagementübung) gesehen werden, die im Mai 2021 hätte stattfinden sollen (vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2021).

schaftlicher Betrachtungen könnten diese noch mehr leisten: Nach Perkovich/Hoffmann (2019) ist

> cyber peacemaking (…) too important to be left to governments. Governments will ultimately determine whether peace is made, and conflict is avoided or contained, but others may need to set the stage and write the script for them.

Gerade hierbei könnten zivilgesellschaftliche Akteur*innen wie Kirchen einen Rahmen bieten.

⇨ 6.2.3 Zwischenfazit Kapitel 6.2

Die Ausführungen zeigen: Während einerseits der Ausbau der internationalen Zusammenarbeit aus der Perspektive des Gerechten Friedens eingefordert werden muss, sind Ansätze unter Einbezug von privatwirtschaftlichen und zivilgesellschaftlichen Akteur*innen voranzubringen. Ein besseres Verständnis über staatliche Aktivitäten, technische Möglichkeiten und eine konsequent öffentlich geführte Diskussion sind hierbei zu ergänzen, um zu einer dem Leitbild entsprechenden »kooperativen Weltordnung« (Zi. 195) zu kommen. Ein erster Schritt einer Normbildung könnte in Selbstverpflichtungen bestehen, wie sie auf staatlicher Ebene u.a. von Japan vorgenommen wurden. Eine Ächtung, wie mitunter vorgeschlagen,[52] könnte dabei als Korrektiv dienen, das einerseits die Zielperspektive wie auch einen Referenzra(h)men und Diskussionsraum darstellt.[53]

⇨ 7 Über die Kriterien hinaus – ein Mehr an Fragen

Aus der Analyse ergeben sich weitere Forschungsdesiderate. So könnte z.B. die Unterscheidung von CNA und CNE detaillierter analysiert werden, da strenggenommen auch bei CNE Veränderungen der Logdaten vorgenommen werden müssen, um nicht erkannt zu werden. Entsprechend besteht auch hierdurch die Möglichkeit einer De-

(52) S. u.a. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (2015).

(53) Ein analoges Beispiel ist der inzwischen in Kraft getretene Atomwaffenverbotsvertrag. Obwohl die sog. »Atomwaffenstaaten« bisher nicht beigetreten sind, ist mit dem Vertrag ein Korrektiv, eine Zielperspektive sowie ein Diskursraum geschaffen worden, womit die Entstehung einer Norm geschaffen werden soll (vgl. Nötzold 2018, 361).

tektion und damit einer (Gegen-)Reaktion auf diese (vgl. Herpig 2020b, 4; Schneier 2014). Dass auch für CNE Exploits verwendet werden müssen, zeigt zudem, dass die Trennung zwischen »Exploitation« und »Attack« zwar hinsichtlich des Vorgehens in Netzwerken besteht, sich daraus jedoch parallele Fragen ergeben, u.a. (ab) wann von einer Reaktion sowie (ab) wann vom »Beginn« eines Einsatzes von Gewalt gesprochen werden kann. Auch die Frage, wie CNE als Vorbereitung von CNA zu bewerten sind, fällt hierunter. Dazu stellen sich Fragen nach dem staatlichen Umgang mit Überwachungstechnologien, u.a. durch ein »Aufweichen von Verschlüsselung (…) und die Weiterentwicklungen von Internet-Protokollen« (Schulze 2020a, 6). Ein weiteres Forschungsfeld u.a. zum (Nicht-)Kombattant*innen-Status könnte auf den Revisited Just War Theories aufgebaut werden.

⇨ 8 Zusammenfassende Betrachtung: SI VIS PACEM, PARA …?

Ausgangspunkt dieses Artikels war die Frage, inwiefern sich (bestimmte) Cyberoperationen mit dem Framework des Gerechten Friedens erfassen und legitimieren lassen. Dabei wurde gezeigt, dass Hackbacks als Reaktionen auf vorangegangene Cyberangriffe mit großer Sicherheit *nicht alle* Kriterien erfüllen können. Das Resultat offenbarte friedensethisch gebotene Alternativen, insbesondere die Option, dass (außenpolitische) Akteur*innen der Bundesregierung als *Norm Entrepreneurs* agieren könnten. Die hierfür notwendige Glaubwürdigkeit kann durch eine konsequente zivile Ausrichtung erreicht werden.

Die aktuellen Planungen sowie die zunehmend militärische Aus- und Aufrüstung des Cyberbereichs auch in Deutschland vermittelt als Zielrichtung das Motto »Si vis pacem, para bellum« (»Wenn Du Frieden willst, bereite Krieg vor«). Dabei stellt das Leitbild des Gerechten Friedens dieses explizit als überholt dar: »Vom gerechten Frieden her denken heißt (…), dass die *para-bellum*-Maxime ersetzt werden muss durch den Grundsatz *si vis pacem para pacem* (›wenn du den Frieden willst, bereite den Frieden vor‹)« (Zi. 75).

Noch scheinen, das machten die Ausführungen aber auch deutlich, Weichenstellungen in Richtung einer Absage an gCNA, insbesondere Hackbacks, möglich. Es wird sich zeigen, wohin sich Deutschland bewegen wird. Wenn am Leitbild des Gerechten Friedens und dessen Kriterien festgehalten wird, scheint es nur einen Weg zu geben.

⇨ Abkürzungsverzeichnis und Glossar

APT(s)	Advanced Persistent Threats / hochentwickelte und andauernde Bedrohungen, meist komplexe Cyberangriffe
BMVg	Bundesministerium der Verteidigung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIR	Organisationsbereich Cyber- und Informationsraum der Bundeswehr
CNA	Computer Network Attacks / Computernetzwerkangriffe
gCNA	gewaltsame Computer Network Attacks / gewaltsame Computernetzwerkangriffe
CNE	Computer Network Exploitation / (Unbefugte) Ausnutzung von Computernetzwerken
COTS	Components-Off-The-Shelf / kommerzielle und standardisierte Software
DDoS	Distributed Denial of Service / Cyberangriff, der die Rechenleistung auslastet und (evtl.) zum Ausfall führen kann
EKD	Evangelische Kirche in Deutschland
Exploits	Softwarefehler, die Sicherheitslücken darstellen
False Flags	vermeintliche Indizien wie die Programmiersprache, die Angriffe falschen Akteur*innen zuordnen soll
KRITIS	Kritische Infrastrukturen
mw	Vom Autor in Zitate eingefügte Ergänzungen
Ransomware	Schadsoftware, die Daten in einem Computernetzwerk verschlüsselt und wodurch im Regelfall Geld erpresst wird
Spyware	Software, die Daten eines Computernetzwerks ausspioniert
Zero Days	Softwarefehler / Exploits, die Sicherheitslücken darstellen und öffentlich noch nicht bekannt sind

⇨ Literaturverzeichnis

Ackermann, Spencer (2014): Snowden: NSA accidentally caused Syria's internet blackout in 2012, in: The Guardian v. 13.8.2014, <https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war> (Zugriff am 21. Januar 2020).

Altmann, Jürgen (2019): Der Cyber-Rüstungswettlauf, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt, 2019, 87–103.

Arquilla, John; Ronfeldt, David (1993): Cyberwar is coming!, in: Comparative Strategy 12, 141–165.

Arquilla, John; Ronfeldt, David (2001): Networks and Netwars. The Future of Terror, Crime, and Militancy, Santa Monica, CA: Rand.

Becker, Matthias (2019): Der geheime Krieg im Netz: »Aktive Cyber-Abwehr« für Deutschland, <https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-krieg-im.724.de.html?dram:article_id=461140> (Zugriff am 17. April 2021).

Bedford-Strohm, Heinrich (2015): Öffentliche Theologie in der Zivilgesellschaft, in: Florian Höhne; Frederike van Oorschot (Hg.): Grundtexte Öffentliche Theologie, 211–216.

Biselli, Anna (2016): Der Bundestagshack – Eine Chronologie der Ereignisse, <https://netzpolitik.org/2016/der-bundestagshack-eine-chronologie-der-ereignisse/> (Zugriff am 07. Mai 2021).

Biselli, Anna (2020): Hackback im Bundespolizeigesetz. Seehofer wollte den digitalen Gegenangriff starten (Update), <https://netzpolitik.org/2020/hackback-bundespolizei-seehofer-will-den-digitalen-gegenangriff-starten/> (Zugriff am 17. April 2021).

BMVg, Bundesministerium der Verteidigung (2016): Abschlussbericht Aufbaustab Cyber- und Informationsraum. Empfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung, <https://www.bmvg.de/resource/blob/11412/868d0f8c03b84846f6bb959618a5518f/c-26-04-16-download-auftrag--cyber-verteidigung-data.pdf> (Zugriff am 07. Februar 2021).

BMVg (2018): Die Konzeption der Bundeswehr, <https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384> (Zugriff am 20. Januar 2021).

Bock, Andreas; Bock, Veronika; Elßner, Thomas; Frühbauer, Johannes J.; Iersel, Fred van; Merkl, Alexander (Hg.) (2019): Konfliktzone Cyberspace: Perspektiven für Sicherheit und Frieden, Hamburg: Zentrum für Ethische Bildung in den Streitkräften Zebis.

Bock, Veronika (Hg.) (2014): Cyberwar: die digitale Front – ein Angriff auf Freiheit und Demokratie?, Ethik und Militär 02.

Borghard, Erica D.; Lonergan, Shawn W. (2019): Cyber Operations as Imperfect Tools of Escalation, in: Strategic Studies Quarterly 13, 122–145.

Brahms, Renke (2015): Die Kriterien für einen Einsatz sind nicht erfüllt. Eine Stellungnahme des Friedensbeauftragten des Rates der Evangelischen Kirche in Deutschland zu einer militärischen Beteiligung Deutschlands am Kampfe gegen den sog. »Islamischen Staat« in Syrien, <https://www.evangelische-friedensarbeit.de/artikel/2015/brahms-die-kriterien-fuer-einen-einsatz-sind-nicht-erfuellt> (Zugriff am 14. Juli 2020).

Brahms, Renke (2020): Bericht des Friedensbeauftragten des Rates der EKD zur Weiterarbeit am Schwerpunktthema der Synode 2019 »Auf dem Weg zu einer Kirche der Gerechtigkeit und des Friedens«, <https://www.ekd.de/ekd_de/ds_doc/05-TOP-V-Bericht-des-Friedensbeauftragten.pdf> (Zugriff am 08. Februar 2021).

Brock, Lothar (2019): Rechtserhaltende Gewalt im Kontext einer komplexen Friedensagenda, in: Ines-Jacqueline Werkner/Torsten Meireis (Hg.): Rechtserhaltende Gewalt – eine ethische Verortung. Fragen zur Gewalt, 117–148.

Bruijne, Ad de; Hertog, Gerard Cornelis den (Hg.) (2018): The present »Just Peace/Just War« debate. Two discussions or one?, Leipzig: Evangelische Verlagsanstalt.

Brüßler, Lisa (2019): Autoren: Abhängigkeit von digitalen Systemen nimmt weltweit zu, <https://www.bundestag.de/dokumente/textarchiv/2019/kw12-buchvorstellung-cyberwar-630248> (Zugriff am 19. Dezember 2020).

BSI, Bundesamt für Sicherheit in der Informationstechnik (2019): Die Lage der IT-Sicherheit in Deutschland 2019, Schneckenlohe: Appel & Klinger Druck und Medien GmbH.

BSI (2020): Die Lage der IT-Sicherheit in Deutschland 2020, Schneckenlohe: Appel & Klinger Druck und Medien GmbH.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2021): LÜKEX 21. Cyberangriff auf Regierungshandeln, <https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/LUEKEX_21/LUEKEX_21_node.html> (Zugriff am 08. Mai 2021).

Busch, Carolin (2020): Von Firewall bis Hackback. Das Spektrum militärischer Cyberoperationen, in: Arbeitspapier Sicherheitspolitik, Bundesakademie für Sicherheitspolitik, <https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_2020_1.pdf> (Zugriff am 19. November 2020).

Clark, David; Landau, Susan (2011): Untangling Attribution, in: National Security Journal, 1–30, <https://harvardnsj.org/wp-content/uploads/sites/13/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf> (Zugriff am 15. Dezember 2020).

Coker, Christopher (2009): War in an Age of Risk, Cambridge: Polity Press.

Council of the European Union (2017): Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (»Cyber Diplomacy Toolbox«) – Adoption, <https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf> (Zugriff am 07. Februar 2021).

DefensiveCon (2020): DefensiveCon2020, <https://www.defensivecon.org/> (Zugriff am 07. Juni 2020).

Der Spiegel (2017): »WannaCry«-Attacke. Fakten zum globalen Cyber-Angriff, <https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html> (Zugriff am 27. Juni 2020).

Deutsche Welle (2021): Deutsche Firmen oft Opfer von Cyber-Attacken v. 23.4.2021, <https://www.dw.com/de/deutsche-firmen-oft-opfer-von-cyber-attacken/a-57250983> (Zugriff am 23. April 2021).

Die Bundesregierung (2015): Krieg im »Cyber-Raum« – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE, <https://

dipbt.bundestag.de/dip21/btd/18/069/1806989.pdf#page=4> (Zugriff am 21 Januar 2021).

Die Bundesregierung (2016): Weißbuch zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr, Berlin.

Die Bundesregierung (2018a): Cybersicherheit. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Jimmy Schulz, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP, <http://dipbt.bundestag.de/doc/btd/19/023/1902307.pdf> (Zugriff am 24. Februar 2021).

Die Bundesregierung (2018b): Hackbacks als aktive digitale Gegenwehr. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP, <http://dipbt.bundestag.de/doc/btd/19/054/1905472.pdf> (Zugriff am 30. Juni 2020).

Die Bundesregierung (2019): Fähigkeiten der »Cyber-Truppe« der Bundeswehr. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Heike Hänsel, Andrej Hunko, weiterer Abgeordneter und der Fraktion DIE LINKE, <http://dipbt.bundestag.de/doc/btd/19/103/1910336.pdf> (Zugriff am 06. Juli 2020).

Die Bundeswehr (2019a): Auftrag des Organisationsbereichs CIR, <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag> (Zugriff am 14. November 2020).

Die Bundesregierung (2019b): Wirken. Wie wirken die Angehörigen in der Bundeswehr?, <https://www.bundeswehr.de/de/organisation/cyber- und-informationsraum/auftrag/wirken> (Zugriff am 04. Januar 2021).

Die Bundesregierung (2020): Cyber- und Informationsraum, <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/> (Zugriff am 07. Juli 2020).

Die deutschen Bischöfe (2000): Gerechter Friede, 4. Aufl., Bonn: Sekretariat der Deutschen Bischofskonferenz.

Döge, Jenny (2010): Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime, in: AVR 48, 486–501.

Dörfler-Dierken, Angelika; Hofmann, Frank; Lohmann, Friedrich (Hg.) (2020): CYBER. Leben hinter der Firewall, Leipzig: Evangelische Verlagsanstalt.

Dörfler-Dierken, Angelika; Portugall, Gerd (Hg.) (2010): Friedensethik und Sicherheitspolitik. Weißbuch 2006 und EKD-Friedensdenkschrift 2007 in der Diskussion, Wiesbaden: VS Verlag für Sozialwissenschaften.

Ebeling, Klaus; Werkner, Ines-Jacqueline (Hg.) (2017): Handbuch Friedensethik, Wiesbaden: Springer VS.

EKD, Evangelische Kirche in Deutschland (2021): Freiheit digital: Die Zehn Gebote in Zeiten des digitalen Wandels. Eine Denkschrift der Evangelischen Kirche in Deutschland, Leipzig: Evangelische Verlagsanstalt.

Finlay, Christopher J. (2017): The concept of violence in international theory. A Double-Intent Account, in: International Theory 9, 67–100.

Finlay, Christopher J. (2018): Just War, Cyber War, and the Concept of Violence, in: Philos. Technol. 31, 357–377.

Finnemore, Martha; Sikkink, Kathryn (1998): International Norm Dynamics and Political Change, in: International Organization 52, 887–917.

Flade, Florian; Mascolo, Georg (2020): Cyberangriff auf Bundestag. Haftbefehl gegen russischen Hacker, in: tagesschau.de v. 5.5.2020, <https://www.tagesschau.de/investigativ/ndr-wdr/hacker-177.html> (Zugriff am 14. Dezember 2020).

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (2015): Cyberpeace. Keine militärischen Operationen im Internet!, <https://cyberpeace.fiff.de/Kampagne/WirFordern/> (Zugriff am 07 Februar 2021).

Gaycken, Sandro (2012): Die vielen Plagen des Cyberwar, in: Roman Schmidt-Radefeldt; Christine Meissler (Hg.): Automatisierung und Digitalisierung des Krieges. Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik, 89–116.

Hahn, Ullrich (2008): Aus Gottes Frieden leben – für gerechten Frieden sorgen. Anmerkungen zur neuen Friedensdenkschrift der Evangelischen Kirche in Deutschland (EKD), in: Forum Pazifismus. Zeitschrift für Theorie und Praxis der Gewaltfreiheit 17, 3–5, <http://

www.forum-pazifismus.de/Download-Archiv/FP17-0108.PDF> (Zugriff am 24. Oktober 2020).

Haspel, Michael (2009): Zwischen Internationalem Recht und partikularer Moral? Systematische Probleme der Kriteriendiskussion in der neueren Just War-Theorie, in: Ines-Jacqueline Werkner; Antonius Liedhegener (Hg.): Gerechter Krieg – Gerechter Frieden. Religionen und friedensethische Legitimationen in aktuellen militärischen Konflikten, 71–81.

Heintschel von Heinegg, Wolff (2020): Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen. Stellungnahme von Prof. Dr. iur. Wolff Heintschel von Heinegg, Europa-Universität Viadrina, Frankfurt (Oder), <https://www.bundestag.de/resource/blob/812388/802ed288657807fd771356094adcfe7f/stellungnahme-Wolff-Heintschel-von-Heinegg_14-12-2020-data.pdf> (Zugriff am 03. Januar 2021).

Hering, Norbert; Schubert, Hartwig von (2012): CyberAge: Mensch und Cybertechnologie in den Herausforderungen und Konflikten des 21. Jahrhunderts, Köln: Wolters Kluwer.

Herpig, Sven (2020a): Evaluation der Cyber-Sicherheitsstrategie für Deutschland 2016, <https://www.stiftung-nv.de/de/publikation/evaluation-der-cyber-sicherheitsstrategie-fuer-deutschland-2016> (Zugriff am 11. November 2020).

Herpig, Sven (2020b): Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen. Stellungnahme von Dr. Sven Herpig, Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, zur öffentlichen Anhörung am 14.12.2020 im Verteidigungsausschuss, <https://www.bundestag.de/resource/blob/812030/37cd9ce216d96f75760c79218bbf187b/stellungnahme-Dr-Sven-Herpig_14-12-2020-data.pdf> (Zugriff am 03. Januar 2021).

Hilz, Wolfram; Nötzold, Antje (Hg.) (2018): Die Zukunft Europas in einer Welt im Umbruch. Festschrift zum 65. Geburtstag von Prof. Dr. Beate Neuss, Wiesbaden: Springer Fachmedien Wiesbaden.

Hofstetter, Yvonne (2019): Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht, München: Droemer eBook.

Höhne, Florian; van Oorschot, Frederike (Hg.) (2015): Grundtexte Öffentliche Theologie, Leipzig: Evangelische Verlagsanstalt.

Hoppe, Thomas; Werkner, Ines-Jacqueline (2017): Der gerechte Frieden. Positionen in der katholischen und evangelischen Kirche in Deutschland, in*:* Klaus Ebeling; Ines-Jacqueline Werkner (Hg.): Handbuch Friedensethik, 343–359.

Huth, Paul K. (1999): Deterrence and International Conflict. Empirical Findings and Theoretical Debates, in: Annu. Rev. Polit. Sci. 2, 25–48.

Jäger, Sarah; Brock, Lothar (Hg.) (2020): Frieden durch Recht – Anfragen an das liberale Modell. Frieden und Recht, Wiesbaden: Springer Fachmedien Wiesbaden.

Kipker, Dennis-Kenji (2019): Hackback in Deutschland: Wer, was, wie und warum?, <https://verfassungsblog.de/hackback-in-deutschland-wer-was-wie-und-warum/> (Zugriff am 21. Januar 2021).

Kirchenamt der EKD (Hg.) (2019): Auf dem Weg zu einer Kirche der Gerechtigkeit und des Friedens. Ein friedenstheologisches Lesebuch, Leipzig: Evangelische Verlagsanstalt.

Klein, Paul; Kümmel, Gerhard (2012): Zwischen Rechtserhaltung und Nicht-Rechtserhaltung. Gewalt als Wesensmerkmal militärischer Organisationen, in: Torsten Meireis (Hg.): Gewalt und Gewalten. Zur Ausübung, Legitimität und Ambivalenz rechtserhaltender Gewalt, 49–68.

Koch, Bernhard (2019): Reflexionen zur ethischen Debatte um das ius in bello in der Gegenwart, in: Ines-Jacqueline Werkner; Peter Rudolf (Hg.): Rechtserhaltende Gewalt – zur Kriteriologie. Fragen zur Gewalt, 75–100.

Koch, Robert (2020): Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen: Stellungnahme von PD Dr. Dr. habil. Robert Koch, Bundesministerium der Verteidigung, zur öffentlichen Anhörung im Verteidigungsausschuss am 14. Dezember 2020, <https://www.bundestag.de/resource/blob/813126/

09f917a17e9d758fe282b1c53c97640f/stellungnahme-Robert-Koch-data.pdf> (Zugriff am 03. Januar 2021).

Koch, Wolfgang (2020): Zur Ethik der wehrtechnischen Digitalisierung: Informations- und ingenieurwissenschaftliche Aspekte, in: Rogg, Matthias; Scheidt, Sophie; Schubert, Hartwig von (Hg.): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, 17–54.

Kreuzer, Leonhard (2019): Hobbesscher Naturzustand im Cyberspace?, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt, 63–86.

Kurz, Constanze; Rieger, Frank (2018): Cyberwar – Die Gefahr aus dem Netz. Wer uns bedroht und wie wir uns wehren können, München: C. Bertelsmann.

Lemos, Rob (2018): Why the hack-back is still the worst idea in cybersecurity, in: TechBeacon v. 5.2.2018, <https://techbeacon.com/security/why-hack-back-still-worst-idea-cybersecurity> (Zugriff am 22. Januar 2021).

Lienemann, Wolfgang (2000): Frieden. Vom »gerechten Krieg« zum »gerechten Frieden«, Göttingen: Vandenhoeck & Ruprecht.

Lilienström, Sven (2020): Im Visier – Die Bedrohung aus dem Cyberraum, in: Gesichter des Friedens v. 22.6.2020, <https://www.faces-of-peace.org/cyberraum/> (Zugriff a, 22. April 2021).

Lin, Patrick (2016): Ethics of Hacking Back. Six arguments from armed conflict to zombies, <https://www.academia.edu/33317069/Ethics_of_Hacking_Back> (Zugriff am 04. Januar 2021).

Lindsay, Jon R. (2013): Stuxnet and the Limits of Cyber Warfare, in: Security Studies 22, 365–404.

Maness, Ryan C.; Valeriano, Brandon (2016): The Impact of Cyber Conflict on International Interactions, in: Armed Forces & Society 42, 301–323.

Mascolo, Georg; Steinke, Ronen (2019): Warum Deutschland im Netz so wehrlos ist, in: Süddeutsche Zeitung v. 10.5.2019, <https://www.sueddeutsche.de/digital/hack-back-cyber-angriff-militaer-1.4441488> (Zugriff am 17. April 2021).

Meireis, Torsten (Hg.) (2012): Gewalt und Gewalten. Zur Ausübung, Legitimität und Ambivalenz rechtserhaltender Gewalt, Tübingen: Mohr Siebeck.

Meireis, Torsten (2019a): Der gerechte Frieden und die Ambivalenz rechtswahrender Gewalt – eine Synthese, in: Ines-Jacqueline Werkner; Torsten Meireis (Hg.): Rechtserhaltende Gewalt – eine ethische Verortung. Fragen zur Gewalt, 149–160.

Meireis, Torsten (2019b): Gerechter Frieden und Cybersicherheit, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt, 105–120.

Meister, Andre (2015): Geheime Cyber-Leitlinie. Verteidigungsministerium erlaubt Bundeswehr »Cyberwar« und offensive digitale Angriffe, <https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/> (Zugriff am 14. Dezember 2020).

Meister, Andre (2020a): BND-Gesetz – Ausspähen unter Freunden wird legalisiert und ausgeweitet, <https://netzpolitik.org/2020/bnd-gesetz-ausspaehen-unter-freunden-wird-legalisiert-und-ausgeweitet/> (Zugriff am 29. Dezember 2020).

Meister, Andre (2020b): Bundesregierung beschließt Staatstrojaner für alle Geheimdienste, <https://netzpolitik.org/2020/bundesregierung-beschliesst-staatstrojaner-fuer-alle-geheimdienste/> (Zugriff am 21. Januar 2021).

Meister, Andre (2020c): Wir veröffentlichen den Gesetzentwurf, mit dem alle Geheimdienste Staatstrojaner bekommen, <https://netzpolitik.org/2020/mit-diesem-gesetz-bekommen-alle-geheimdienste-staatstrojaner/> (Zugriff am 21. Januar 2021).

Meister, Andre; Biselli, Anna (2019): Geheimes Bundestagsgutachten attackiert Hackback-Pläne der Bundesregierung, <https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/#2019-08-27_Bundestag-WD_Cyber-Abwehr-in-Deutschland> (Zugriff am 07. Juni 2020).

Mielke, Roger (2018): »Differenzierter Konsens?«, in: Ines-Jacqueline Werkner; Christina Schües (Hg.): Gerechter Frieden als Orientierungswissen: Grundsatzfragen, 27–48.

Mielke, Roger (2020): Digitalität und neue Projektionen von Macht. Ein Kommentar zu Niklas Schörnigs politikwissenschaftlichen Überlegungen, in: Matthias Rogg; Sophie Scheidt; Hartwig von Schubert (Hg.): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, 83–87.

Moret, Erica; Pawlak, Patryk (2017): The EU Cyber Diplomacy Toolbox. towards a cyber sanctions regime?, <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf> (Zugriff am 06. Februar 2021).

Müller, Harald; Wunderlich, Carmen (Hg.) (2013): Norm Dynamics in Multilateral Arms Control. Interests, Conflicts, and Justice (Studies in Security and International Affairs), Athens: University of Georgia.

Münkler, Herfried (2018): War on terror. Vom Kriminalitäts- zum Kriegsparadigma, in: ZfAS (Zeitschrift für Außen- und Sicherheitspolitik) 11, 573–580.

NATO (2020): Cyber Defence, <https://www.nato.int/cps/en/natohq/topics_78170.htm> (Zugriff am 21. Dezember 2020).

Neuneck, Götz (2017): Krieg im Internet? Cyberwar in ethischer Reflexion, in: Klaus Ebeling; Ines-Jacqueline Werkner (Hg.): Handbuch Friedensethik, 805–816.

Nötzold, Antje (2018): Der Atomwaffenverbotsvertrag, in: Wolfram Hilz; Antje Nötzold (Hg.): Die Zukunft Europas in einer Welt im Umbruch. Festschrift zum 65. Geburtstag von Prof. Dr. Beate Neuss, 353–375.

Oeter, Stefan (2020a): Chancen und Hindernisse der Herausbildung eines genuinen Friedensrechts neuer Qualität, in: Sarah Jäger; Lothar Brock (Hg.): Frieden durch Recht – Anfragen an das liberale Modell. Frieden und Recht, 121–146.

Oeter, Stefan (2020b): Plädoyer für die Normierung roter Linien des nicht mehr Hinnehmbaren. Rechtswissenschaftliche Perspektive – Kommentar zu Stefanie Schmahl, in: Matthias Rogg; Sophie Scheidt; Hartwig von Schubert (Hg.): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, 97–112.

Paris Call (2018): Paris Call for Trust and Security in Cyberspace, <https://pariscall.international/en/> (Zugriff am 07. Februar 2021).

Perkovich, George; Hoffman, Wyatt (2019): From Cyber Swords to Plowshares, in: Thomas de Waal (Hg.): Think Peace. Essays for an Age of Disorder.

Raiser, Konrad (2019): Eine Ethik rechtserhaltender Gewalt im ökumenischen Diskurs. Zwischen gerechtem Krieg und Pazifismus, in:

Ines-Jacqueline Werkner; Torsten Meireis (Hg.): Rechtserhaltende Gewalt – eine ethische Verortung. Fragen zur Gewalt, 95–115.

Rat der EKD (2007): Aus Gottes Frieden leben – für gerechten Frieden sorgen. Eine Denkschrift des Rates der Evangelischen Kirche in Deutschland, 2. Aufl., Gütersloh: Gütersloher Verlagshaus.

Rehage, Ruben (2019): Die digitale Front: So wappnet sich die Bundeswehr gegen Hacker-Angriffe, in: stern.de, <https://cyber-peace.org/wp-content/uploads/2019/08/Cyber-Crime_-Bundeswehr-Unternehmen-und-Versorger-wappnen-sich-_-STERN.de_.pdf> (Zugriff am 07. Januar 2021).

Reinhold, Thomas (2017): Petya / NotPetya / ExPetr / PetrWrap, <https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/petya_notpetya/> (Zugriff am 30. Dezember 2020).

Reinhold, Thomas (2019): Cyber-Einheiten der Bundeswehr lt. Interview »permanent im Krieg«?, <https://cyber-peace.org/2019/08/05/cyber-einheiten-der-bundeswehr-lt-interview-permanent-im-krieg/> (Zugriff am 15. Januar 2021).

Reinhold, Thomas (2020): Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen. Stellungnahme von Thomas Reinhold, TU Darmstadt, zur öffentlichen Anhörung am 14.12.2020 im Verteidigungsausschuss des deutschen Bundestages, <https://www.bundestag.de/resource/blob/812024/67fc9db4f856a8445355562500d2a134/stellungnahme-Thomas-Reinhold_14-12-2020-data.pdf> (Zugriff am 29. Dezember 2020).

Reinhold, Thomas; Schulze, Matthias (2017): Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von »hack backs«, <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf> (Zugriff am 04. Januar 2021).

Reuter, Christian; Riebe, Thea; Aldehoff, Larissa; Kaufhold, Marc-André; Reinhold, Thomas (2019): Cyberwar zwischen Fiktion und Realität. Technologische Möglichkeiten, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung: Fragen zur Gewalt, 15–38.

Reuter, Hans-Richard (2012): Terrorismus und rechtserhaltende Gewalt. Grenzen des Antiterrorismus aus ethischer Sicht, in: Torsten Meireis (Hg.): Gewalt und Gewalten. Zur Ausübung, Legitimität und Ambivalenz rechtserhaltender Gewalt, 11–29.

Rid, Thomas (2018): Mythos Cyberwar. Über digitale Spionage, Sabotage und andere Gefahren, Hamburg: Edition Körber.

Riordan, Shaun (2019): Cyberdiplomacy. Managing security and governance online, Cambridge, UK: Polity.

Rogg, Matthias; Scheidt, Sophie; Schubert, Hartwig von (Hg.) (2020): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, Hamburg: German Institute for Defence and Strategic Studies.

Romanosky, Sasha; Goldman, Zachary (2016): Cyber Collateral Damage, in: Procedia Computer Science 95, 10–17.

Rudolf, Peter (2017): Zur Legitimität militärischer Gewalt, Bonn: Bundeszentrale für Politische Bildung.

Rupp, Christina; Herpig, Sven (2021): Deutschlands staatliche Cybersicherheitsarchitektur, <https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur> (Zugriff am 07. Mai 2021).

Schmahl, Stefanie (2020): Computernetzwerkoperationen und Völkerrecht. Zuordnungsmodelle und Bewertungen im Überblick, in: Matthias Rogg; Sophie Scheidt; Hartwig von Schubert (Hg.): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, 87–96.

Schmidt-Radefeldt, Roman; Meissler, Christine (Hg.) (2012): Automatisierung und Digitalisierung des Krieges. Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik, Baden-Baden: Nomos.

Schmitt, Michael N. (Hg.) (2013): 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, New York: Cambridge University Press.

Schmitt, Michael N. (Hg.) (2017): Tallinn manual 2.0 on the international law applicable to cyber operations, New York, NY: Cambridge University Press.

Schneier, Bruce (2014): There's No Real Difference Between Online Espionage and Online Attack, <https://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/> (Zugriff am 07. Januar 2021).

Schörnig, Niklas (2019a): Gewalt im Cyberraum. Ein politikwissenschaftlicher Blick auf Begriff und Phänomen des Cyberkrieges, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung: Fragen zur Gewalt, 39–61.

Schörnig, Niklas (2019b): Resilienz stärken und Vertrauen bilden statt den Cyberwar herbeireden, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt, 121–133.

Schörnig, Niklas (2020): Implikationen eines Krieges at machine speed. Der digitale Wandel des bewaffneten Konflikts aus politikwissenschaftlicher Perspektive, in: Matthias Rogg; Sophie Scheidt; Hartwig von Schubert (Hg.): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, 67–82.

Schröfl, Josef; Rajaee, Bahram M.; Muhr, Dieter (Hg.) (2011): Hybrid and Cyber War as Consequences of the Asymmetry. A Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace; Political, Social and Military Responses, Frankfurt M.: Lang.

Schubert, Hartwig von (2013): Die Ethik rechtserhaltender Gewalt, Opladen: Budrich.

Schubert, Hartwig von (2018): Pflugscharen und Schwerter. Plädoyer für eine realistische Friedensethik, Leipzig: Evangelische Verlagsanstalt.

Schubert, Hartwig von (2020): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten. Einleitung, in: Matthias Rogg; Sophie Scheidt; Hartwig von Schubert (Hg.): Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten, 5–16.

Schuetze, Julia (2020a): Japan's cybersecurity policy. An introduction, <https://www.stiftung-nv.de/sites/default/files/rif-japan-schuetze-final.pdf> (Zugriff am 07. Februar 2021).

Schuetze, Julia (2020b): Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen. Stellungnahme von Julia Schuetze, Projektmana-

gerin im Bereich Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, <https://www.bundestag.de/resource/blob/812744/ea47db48d30b5aa32acd846b6ded1996/stellungnahme-Julia-Schuetze_14-12-2020-data.pdf> (Zugriff am 03. Januar 2021).

Schulze, Matthias (2018): From cyber-utopia to cyber-war. Normative change in cyberspace, <https://www.db- thueringen.de/receive/dbt_mods_00035107> (Zugriff am 21. Mai 2021)

Schulze, Matthias (2019): Überschätzte Cyber-Abschreckung, <https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A39_she.pdf> (Zugriff am 21. Mai 2021).

Schulze, Matthias (2020a): Konflikte im Cyberspace, in: UN-BASIS-INFORMATIONEN, <https://dgvn.de/fileadmin/publications/PDFs/Basis_Informationen/BI_61_Konflikte-im-Cyberspace.pdf> (Zugriff am 07. Februar 2021).

Schulze, Matthias (2020b): Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland, <https://www.swp-berlin.org/fileadmin/contents/products/studien/2020S15_she_CyberOperationen.pdf> (Zugriff am 16. November 2020).

Strub, Jean-Daniel; Grotefeld, Stefan (Hg.) (2007): Der gerechte Friede zwischen Pazifismus und gerechtem Krieg. Paradigmen der Friedensethik im Diskurs, Stuttgart: Kohlhammer.

Tödt, Heinz Eduard (1977): Versuch zu einer Theorie ethischer Urteilsfindung, in: Zeitschrift für Evangelische Ethik 21, 81–93.

Valeriano, Brandon; Jensen, Benjamin (2019): The Myth of the Cyber Offense: The Case for Restraint, in: Policy Analysis, <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint> (Zugriff am 26. Dezember 2020).

van Baarda, Ted (2018): Can Soldiers do »the decent thing« in War? The Just War tradition, the laws of war and Saving Private Ryan, in: Ad de Bruijne; Gerard Cornelis den Hertog (Hg.): The present »Just Peace/Just War« debate. Two discussions or one?, 13–34.

Waal, Thomas de (Hg.) (2019): Think Peace. Essays for an Age of Disorder, Washington, DC.

Werkner, Ines-Jacqueline (2010): Friedensethik und humanitäre Intervention. Konsequenzen aus der Friedensdenkschrift, in: Angelika Dörfler-Dierken; Gerd Portugall (Hg.): Friedensethik und Sicherheits-

politik: Weißbuch 2006 und EKD-Friedensdenkschrift 2007 in der Diskussion, 141–152.

Werkner, Ines-Jacqueline (2019): Cyberwar – die Digitalisierung der Kriegsführung?, in: Ines-Jacqueline Werkner; Niklas Schörnig (Hg.): Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt, 1–14.

Werkner, Ines-Jacqueline; Liedhegener, Antonius (Hg.) (2009): Gerechter Krieg – Gerechter Frieden. Religionen und friedensethische Legitimationen in aktuellen militärischen Konflikten, Wiesbaden: VS.

Werkner, Ines-Jacqueline; Meireis, Torsten (Hg.) (2019): Rechtserhaltende Gewalt – eine ethische Verortung. Fragen zur Gewalt, Wiesbaden: Springer Fachmedien.

Werkner, Ines-Jacqueline; Rudolf, Peter (Hg.) (2019): Rechtserhaltende Gewalt – zur Kriteriologie. Fragen zur Gewalt, Wiesbaden: Springer Fachmedien.

Werkner, Ines-Jacqueline; Schörnig, Niklas (Hg.) (2019): Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt, Wiesbaden: Springer Fachmedien.

Werkner, Ines-Jacqueline; Schües, Christina (Hg.) (2018): Gerechter Frieden als Orientierungswissen. Grundsatzfragen, Wiesbaden: Springer Fachmedien.

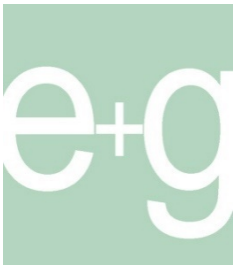
Werthes, Sascha (2019): Politische Sanktionen im Lichte rechtserhaltender Gewalt, in: Ines-Jacqueline Werkner; Peter Rudolf (Hg.): Rechtserhaltende Gewalt – zur Kriteriologie. Fragen zur Gewalt, 121–150.

Wheeler, David; Larsen, Gregory (2003): Techniques for Cyber Attack Attribution, in: Institute for Defense Analyses (IDA), 1–82.

Wissenschaftliche Dienste des Deutschen Bundestags (2015): Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare), <https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbee41d8d3d6898/WD-2-038-15-pdf-data.pdf> (Zugriff am 03. Januar 2021).

Wunderlich, Carmen (2013): Theoretical Approaches in Norm Dynamics, in: Harald Müller; Carmen Wunderlich (Hg.): Norm Dynamics in Multilateral Arms Control. Interests, Conflicts, and Justice (Studies in Security and International Affairs), 20–47.

Zitationsvorschlag:
Weber, Max (2021): To Hack Back or Not? Eine friedensethische Analyse von Cyberoperationen vor dem Hintergrund des Leitbilds des Gerechten Friedens. (Ethik und Gesellschaft 2/2021: Friedensethik und Geopolitik). Download unter: https://dx.doi.org/10.18156/eug-2-2021-art-5 (Zugriff am [Datum]).



ethikundgesellschaft
ökumenische zeitschrift für sozialethik

2/2021: Friedensethik und Geopolitik