Universitätsverlag Potsdam

Valentin Protze

Zur völkerstrafrechtlichen Bewertung rein störender Cyberoperationen

Staat, Recht und Politik – Forschungs- und Diskussionspapiere
State, Law, and Politics – Research and Discussion Papers
12

Staat, Recht und Politik – Forschungs- und Diskussionspapiere
State, Law, and Politics – Research and Discussion Papers
12

Valentin Protze

Zur völkerstrafrechtlichen Bewertung rein störender Cyberoperationen

Universitätsverlag Potsdam

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Informationen zum Autor:
Valentin Protze studiert Rechtswissenschaften an der Juristischen Fakultät der Universität Potsdam. Das Papier basiert auf seiner Schwerpunkthausarbeit im Bereich des Internationalen Rechts.

Universitätsverlag Potsdam 2022
http://verlag.ub.uni-potsdam.de/

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 2533 / Fax: 2292
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Staat, Recht und Politik – Forschungs- und Diskussionspapiere = State, Law, and Politics – Research and Discussion Papers** wird herausgegeben von apl. Prof. Dr. iur. Norman Weiß, Universität Potsdam.

ISSN (online) 2509-6974

Kontakt:
norman.weiss@uni-potsdam.de

Online veröffentlicht auf dem Publikationsserver der Universität Potsdam
https://doi.org/10.25932/publishup-54331

Zur völkerstrafrechtlichen Bewertung rein störender Cyberoperationen

Valentin Protze

A Einleitung

B Die völkerstrafrechtliche Bewertung störender Cyberoperationen

I. Definition störender Cyberoperationen

1. Cyberoperationen

2. Abgrenzung störend / zerstörend

II. Völkerstrafrechtliche Aspekte störender Cyberoperationen

1. Anwendbarkeit völkerrechtlicher Normen auf Cyberoperationen

2. Die einzelnen Verbrechen

3. Individuelle Kriminelle Verantwortlichkeit

C Fazit

Anmerkungen

Abstract

This paper addresses the classification under international criminal law of purely disruptive, i.e. non-destructive, cyber operations. After the necessary clarification of terms, the individual questions of the applicability of international criminal law are discussed and it is examined which elements of crime can be realized by such actions.

Zusammenfassung

Dieses Papier thematisiert die völkerstrafrechtliche Einordnung rein störender, also nicht zerstörender Cyberoperationen. Nach der erforderlichen Begriffsklärung werden die einzelnen Fragen der Anwendbarkeit des Völkerstrafrechts erörtert und geprüft, welche Tatbestände durch solche Aktionen verwirklicht werden können.

A Einleitung

Das Internet und die damit verbundene Digitalisierung haben in den letzten Jahrzehnten immens zur Optimierung unseres täglichen Lebens beigetragen. In nahezu jedem Bereich des öffentlichen und des privaten Lebens ist jede Person und somit unsere gesamte Gesellschaft auf das Funktionieren digitaler Technik angewiesen. Der Ausfall oder die Ausspähung solcher computergesteuerten Systeme könnten fatale Folgen für einen gesamten Staat, wenn nicht sogar eine Staatengemeinschaft haben. Gerade deshalb ist diese Infrastruktur in den letzten Jahren zu einem beliebten Angriffsziel geworden.[1] Eingesetzte Mittel sind dabei häufig solche, deren heutige Bedeutung im Zeitpunkt der Entstehung von grundlegendem humanitärem Völkerrecht und Völkerstrafrecht noch nicht einzuschätzen war, nämlich digitale.

Wie Angriffe mittels rein störenden Cyberoperationen völkerstrafrechtlich zu werten sind, soll in der vorliegenden Untersuchung erörtert werden. Da der Internationale Strafgerichtshof (IStGH) das einzige weltweit agierende Strafgericht ist, liegt der Fokus dieser Untersuchung auf der Strafbarkeit nach dem Römischen Statut des IStGH (IStGH-Statut). Zunächst ist zu untersuchen, was Cyberoperationen, insbesondere rein störende, überhaupt sind. In einem nächsten Schritt soll untersucht werden, ob rein störende Cyberoperationen aufgrund ihrer Schwere überhaupt unter die Gerichtsbarkeit des IStGH fallen. Im Zentrum steht jedoch die Erörterung, ob und wie störende Cyberoperationen die einzelnen Verbrechenstatbestände erfüllen können. Da der Tatbestand des Kriegsverbrechens die Verletzung von humanitärem Völkerrecht voraussetzt, wird auch hierauf einzugehen sein.

B Die völkerstrafrechtliche Bewertung störender Cyberoperationen

I. Definition störender Cyberoperationen

1. Cyberoperationen

Bei der Suche nach Definitionen von Cyberoperationen fällt auf, dass der Begriff der Cyberoperation ein Oberbegriff ist, der nicht ganz einheitlich definiert, sondern von verschiedenen Stakeholdern unterschiedlich verwendet wird. So definiert das Verteidigungsministerium der USA Cyberoperationen einfach als Operationen, bei denen der Hauptzweck darin besteht, Ziele im oder durch den Cyberspace zu erreichen.[2] Ähnlich werden Cyberoperationen auch im Tallinn Manual[3] für Cyber Warfare definiert, nämlich als den Einsatz von Computerfähigkeiten mit dem primären Hintergrund Ziele im oder durch den Gebrauch von Cyberspace zu erreichen.[4] Cyberspace ist dabei eine Umgebung aus physikalischen und nicht-physikalischen Komponenten, die durch die Benutzung von Computern und anderen elektromagnetischen Komponenten, insbesondere durch voneinander abhängigen Netzwerken informationstechnischer Infrastruktur und die darin enthaltenen Daten charakterisiert wird.[5] Auch das Internationale Komitee vom Roten Kreuz (IKRK) definiert Cyberoperationen einfach als Operationen mittels Datenfluss gegen oder durch einen Computer oder ein Computersystem.[6]

Die Definition der Cyberoperationen wird in der Literatur teilweise konkretisiert, zum Beispiel als Aktionen, die durch die Nutzung von Computernetzwerken durchgeführt werden, um die in Computern und Computernetzwerken gespeicherten Informationen oder die Computer und Netzwerke selbst zu stören, zu beeinträchtigen oder zu zerstören.[7]

All diese Definitionen haben gemeinsam, dass Computer oder Computernetzwerke gleichzeitig Mittel und Ziel von Cyberoperationen sein können.[8] Jedoch sieht man schon anhand der Definition des IKRK, dass nicht jede Operation, die einen Computer oder ein Computernetzwerk zum Ziel hat, gleich eine Cyberoperation sein muss. Das Mittel muss viel mehr auch ein computer- oder netzwerkspezifisches sein, denn nur so lässt sich die Besonderheit von Cyberoperationen begründen.[9] Man kann also nicht von einer Cyberoperation sprechen, wenn der Erfolg der Operation am betreffenden Computer oder Computernetzwerk rein durch physische Kräfte, sei es durch Explosion oder mittels Magnetismus eintritt. Dies ist vergleichbar mit den Eigenheiten von ABC-Waffen. Auch hier ist das Besondere nicht der Erfolg des Einsatzes, also der Schaden und Tod von Menschen, sondern die Art und Weise des Erfolgs.[10]

Darüber hinaus sagen die Definitionen nichts darüber aus, ob die Operationen von der Ferne geschehen müssen. Cyberoperationen umfassen daher auch das lokale Anbringen von Viren durch Agenten.[11]

Zusammenfassend lassen sich Cyberoperationen also wie folgt definieren: Cyberoperationen sind ein unbefugter informationstechnologischer Zugriff auf ein Netzwerk, einen Computer oder ein Computersystem, um Informationen zu erlangen, Daten zu manipulieren oder physischen Schaden auch mittelbar anzurichten. Diese Definition scheint sehr weit gefasst. Dies ist aber notwendig um die vielen verschiedenen Formen von Cyberoperationen zu umfassen.

2. Abgrenzung störend / zerstörend

Im Folgenden soll nun eine Definition für störende Cyberoperationen gefunden werden. Grundsätzlich werden Cyberoperationen nach ihren Auswirkungen in Cyberangriffe und Cyberausnutzung untergliedert.[12] Die Grenze wird so gezogen, dass Cyberangriffe stets Auswirkungen in der realen Welt, also außerhalb des Cyberspace, entfalten müssen,[13] während Cyberausnutzung rein systeminterne Auswirkungen entfaltet.[14] Der Ort, wo sich die Auswirkungen niederschlagen, hat aber nichts damit zu tun, ob eine Cyberoperation lediglich störend oder physisch zerstörend wirkt. Zu beachten ist auch, dass bei Cyberoperationen die Zweit-

und Drittfolgen meist verzögert auftreten.[15] Primär wird nur ein Computer, ein Computersystem oder ein Netzwerk gestört. Sekundär kann eine solche Störung aber gravierende Folgen für physische Objekte und die Bevölkerung mit sich bringen.[16] Sollten solche primären und sekundären Folgen die physischen Zerstörung von Objekten bewirken, so ist von einer physisch zerstörenden Cyberoperation die Rede. Tritt kein physischer Schaden auf, so liegt eine rein störende Cyberoperation vor, soweit die Funktionalität des angegriffenen Objekts eingeschränkt wird.

Verdeutlicht wird dies an dem Beispiel einer gegen ein Krankenhaus geführten Cyberoperation. In einer ersten Variante führt diese dazu, dass lebenserhaltende Geräte überhitzen und dadurch zerstört werden. Hierdurch sterben Menschen, die auf diese Geräte angewiesen sind. Infolge der physischen Zerstörung der Geräte handelt es sich um eine physisch zerstörende Cyberoperation. In einer zweiten Variante werden durch die Cyberoperation Patientendaten derart verändert, dass sie durch die Ärzte falsch behandelt werden und dadurch sterben. Mangels physischen Schadens an Objekten handelt es sich hier lediglich um eine rein störende Cyberoperation. Das Beispiel verdeutlicht zugleich, dass die Folgen beider Arten von Cyberoperationen sich ähneln können. Nur weil die eine physischen Schaden mit sich bringt, heißt das nicht, dass sie automatisch schwerere Konsequenzen nach sich zieht.

Rein störende Cyberoperationen sind also ein informationstechnologischer Zugriff auf einen Computer, ein Computersystem oder ein Netzwerk, um das angegriffene Ziel in seiner Funktionalität zu beschränken, ohne es dabei unmittelbar physisch zu beschädigen.

II. Völkerstrafrechtliche Aspekte störender Cyberoperationen

1. Anwendbarkeit völkerrechtlicher Normen auf Cyberoperationen

a) Allgemeine Aspekte

Bei der völkerstrafrechtlichen Bewertung störender Cyberoperationen stellt sich zunächst die Frage, ob der Cyberspace und somit auch Cyberoperationen überhaupt völkerrechtlichen Normen unterfallen oder ob er ein Rechtsraum sui generis ist. Diese Ansicht wurde vor allem früher mit der Begründung vertreten, dass es keine greifbare Manifestation von physisch genau lokalisierbaren Standorten gebe. Dadurch wären die Konzepte, auf denen völkerrechtliche Regelungen fußen, nämlich das Territorialitätsprinzip und das Souveränitätsprinzip, hinfällig, sodass Völkerrecht im Cyberspace nicht angewandt werden kann.[17] Dem ist aber entgegenzuhalten, dass der Cyberspace sich sehr wohl physisch manifestiert und zwar in der aus physischen Elementen bestehenden Technik, die sich auf staatlichen Territorien befindet.[18] So unterliegt Cyberspace ganz klar staatlicher Souveränität.[19] Dasselbe lässt sich auch aus der Staatenpraxis herleiten, wonach Cyberspace seit jeher den jeweiligen nationalen Gerichtsbarkeiten unterworfen ist.[20] Daher ist auch Völkerstrafrecht als Völkerrecht im Cyberspace anwendbar.

b) Gerichtsbarkeit des IStGH

Grundsätzlich kann der IStGH seine Gerichtsbarkeit gemäß Art. 12 IStGH-Statut über Völkerrechtsverbrechen ausüben, die durch Cyberoperationen verübt worden sind, wenn die weiteren Voraussetzungen erfüllt sind.

aa) Territoriale Gerichtsbarkeit des IStGH

Nach Art. 12 II IStGH-Statut ist das der Fall, wenn entweder der Staat, dessen Staatsangehörigkeit der Täter besitzt, oder der Staat, in dessen Hoheitsgebiet das fragliche Verhalten stattgefunden hat, Vertragspartei des Statuts ist.

Neben dem rein praktischen Problem, dass der Täter aufgrund der Anonymität im Internet nur selten ausfindig gemacht werden kann, bereitet hier die Formulierung „fragliches Verhalten“[21] Probleme. Die Wortwahl deutet darauf hin, dass bei der Formulierung der Norm davon ausgegangen wurde, dass der Ort, an dem die Schädigungshandlung vorgenommen wurde identisch ist mit dem, an dem der Schaden eintritt. Der Cyberspace ist aber ein entgrenzter Raum.[22] So kann ein Hacker in Russland mittels Cyberoperation innerhalb weniger Sekunden auf einen Computer in Südamerika zugreifen, der wiederum ein Ziel in Australien angreift. Die Frage hierbei ist, in welchem Staat das fragliche Verhalten begangen wurde.[23] Wäre dies lediglich der Ursprungsstaat, so könnten Personen, die nicht die Staatsangehörigkeit einer Vertragspartei des Statuts besitzen, die Gerichtsbarkeit des IStGH leicht umgehen, indem sie Cyberoperationen von Ländern aus starten, die ebenfalls keine Vertragsparteien des Statuts sind. Für Cyberoperationen würde so der Schutz vor Völkerrechtsverbrechen erheblich gemindert. Ein anderer Ansatz wäre es zu sagen, dass das fragliche Verhalten in der Souveränität aller betroffenen Staaten liegt.[24] Das würde bedeuten, dass lediglich einer dieser Staaten Vertragspartei des Statuts sein muss. Dies würde aber dazu führen, dass – wenn weder der Ursprungsstaat der Cyberoperation noch deren endgültiger Zielstaat Vertragspartei des Statuts sind – das Verhalten trotzdem in die Gerichtsbarkeit des IStGH fiele. Dies ist nicht nur mit Art. 30 WVK, wonach völkerrechtliche Verträge keine Wirkung gegenüber Dritten entfalten, unvereinbar, sondern auch mit dem Sinn und Zweck der Norm, nach dem Völkerrechtsverbrechen in oder durch Vertragsstaaten verhindert werden sollen. Dementsprechend ist der Begriff „fragliches Verhalten“ so auszulegen, dass er sich lediglich auf die Konsequenzen der Cyberoperation im Zielstaat bezieht.[25]

Der IStGH kann über Cyberoperationen seine Gerichtsbarkeit also ausüben, soweit diese den Tatbestand eines Völkerrechtsverbrechens in einem Vertragsstaat des Statuts erfüllen.

bb) Schwere störender Cyberoperationen

Die Präambel des IStGH-Statuts legt fest, dass der IStGH nur bei schwersten Verbrechen tätig wird, die die internationale Gemeinschaft als Ganzes betreffen. So soll sichergestellt werden, dass der IStGH nicht durch eine Flut von geringeren Verbrechen bei der Verfolgung großer, schwerwiegender Verbrechen behindert wird.[26] Folglich befasst sich der IStGH nach Art. 17 I lit. d IStGH-Statut nicht mit Sachen, die nicht schwer genug sind, um weitere Maßnahmen des Gerichts zu rechtfertigen. Fraglich ist, ob durch rein störende Cyberoperationen Verbrechen einer solchen Schwere begangen werden können.

Aufgrund der massiven Eingriffe in die Souveränität von Staaten, die mit der Strafverfolgung durch ein internationales Strafgericht einhergehen,[27] könnte man annehmen, dass das IStGH-Statut die Schwelle, ab wann ein Verbrechen aufgrund seiner Schwere vom IStGH verfolgt werden kann, genau definiert hat. Doch trotz der vehementen Kritik, insbesondere von afrikanischen Staaten, der IStGH entscheide häufig aus politischen Gründen, wann ein Verbrechen diese Schwelle überschreitet,[28] ist keine eindeutige Definition festgelegt worden.

Bei der Prüfung der Schwere von Verbrechen durch die Vorverfahrenskammer (PTC) des IStGH und den Ankläger (OTP) kommt es auf das Ausmaß, die Art der Begehung sowie die Auswirkungen des Verbrechens an.[29]

Das Ausmaß von Taten bestimmt sich aus der Anzahl direkt und indirekt physisch oder psychisch geschädigter Opfer.[30] Die geografischen und zeitlichen Ausdehnungen der Taten sind Faktoren, die die Schwere der Tat heben oder senken können.[31] Daneben werden die Taten in

Kategorien eingeordnet, nach denen sie die Schwelle der Schwere regelmäßig über- oder unterschreiten. Als schwerwiegend genug werden häufig Taten gegen Personen angesehen, insbesondere die vorsätzliche Tötung, Sexualdelikte, Delikte gegen Minderjährige sowie physische und psychische Folter.[32] Delikte, die sich allein gegen Gegenstände richten, sind dagegen häufig nicht schwerwiegend genug, um eine Zuständigkeit des IStGH zu begründen.[33]

Es ist dennoch durchaus denkbar, dass eine störende Cyberoperation ein hinreichendes Ausmaß annimmt. Wird zum Beispiel durch eine störende Cyberoperation in einem strengen Winter die Stromversorgung eines ganzen Landes unterbrochen, kann ein Großteil der Bevölkerung nicht heizen und so unzweifelhaft erhebliche physische und psychische Schäden davontragen. In einem solchen Fall ist zweifellos von einem hinreichenden Ausmaß auszugehen. Anders gestaltet sich die Lage, wenn von dem Stromausfall nur wenige Menschen betroffen sind oder der Stromausfall nur kurze Zeit andauert.

Zu den Merkmalen, die laut OTP für die Beurteilung der Schwere von Verbrechen relevant sind, zählt die Art der Begehung. Diese wird insbesondere anhand des Grads der Beteiligung und des Vorsatzes der Täter beurteilt sowie danach, ob die Tat systematisch oder mittels Machtmissbrauchs begangen wurde.[34] Auch eine besondere Grausamkeit der Taten, etwa durch Diskriminierung, sexuellen Missbrauch oder Ausnutzung besonderer Schwäche der Opfer, verschärft deren Schwere.[35] Bei Cyberoperationen ist bezüglich des Vorsatzes zu beachten, dass seine Folgen häufig aufgrund der Komplexität der angegriffenen Ziele nicht endgültig abzusehen sind.[36] Es ist hier also nicht selten anzunehmen, dass Angreifer bezüglich der Folgen nur bedingt vorsätzlich handeln.

Schlussendlich sind auch die Auswirkungen zu beachten, die eine Tat mit sich bringt. Hierunter fallen neben dem Leid und Schrecken der Opfer vor allem längerfristige Auswirkungen, wie gesellschaftliche, wirtschaftliche oder Umweltschäden.[37] Wichtig ist, dass das Vorliegen solcher qualitativen Merkmale das Fehlen anderer quantitativer Merkmale ausgleichen kann, das Fehlen von solchen qualitativen Merkmalen die Schwere der Taten aber nicht automatisch entfallen lässt.[38] Ein Beispiel hierfür sind Angriffe auf humanitäre Hilfstruppen oder Angriffe unter deren Emblemen. Solche Angriffe lassen Helfende vor humanitären Einsätzen zurückschrecken, beziehungsweise erschüttern das Vertrauen in humanitäre Hilfstruppen nachhaltig, was die Wirkung solcher Einsätze gravierend hemmt.[39] Auch hier ist es durchaus denkbar, dass störende Cyberoperationen solche qualitativen Merkmale erfüllen. Zum Beispiel können Viren in Dokumenten oder Websites getarnt sein, die aufgrund der Verwendung des Emblems des Roten Kreuzes oder einer UN-Hilfsorganisation vertrauenswürdig erscheinen. Daneben ist es mittels störender Cyberoperationen möglich Wahlen zu manipulieren, wodurch Unruhen und Aufstände entstehen können, in denen Menschen getötet werden und die das Vertrauen in die Demokratie nachhaltig erschüttern.

Störende Cyberoperationen können also durchaus eine Schwere annehmen, die vom IStGH verfolgt werden kann. Durch das Fehlen klarer Kriterien ist eine Einzelfallprüfung jedoch stets unentbehrlich.

2. *Die einzelnen Verbrechen*

Im folgenden Abschnitt wird nun erörtert, welche völkerrechtlichen Verbrechen störende Cyberoperationen verwirklichen können.

a) Völkermord nach Art. 6 IStGH-Statut

Die Begehung von Völkermord nach Art. 6 IStGH-Statut mittels störender Cyberoperationen scheint äußerst unwahrscheinlich. Der Grund dafür ist, dass die Auswirkungen von Cyberoperationen wie bereits erwähnt selten eindeutig abzusehen sind. Gezielte Angriffe auf bestimmte Gruppen im Sinne des Art. 6 IStGH-Statut scheinen nur selten möglich, aber durchaus denkbar.[40] Von dem Beispiel der Verursachung eines winterlichen Stromausfalls ausgehend, wäre ein Völkermord denkbar, wenn der Stromausfall nur Ortsteile beträfe, in denen sich lediglich die Gruppe befindet, die teilweise oder ganz zerstört werden soll.[41] Denkbar wäre auch das Abgreifen und Registrieren von Daten über eine Gruppe des Art. 6 IStGH-Statuts, um diese dann in einem Völkermord zu verwenden.[42] Dies wäre mangels Funktionalitätseinschränkung des Ziels keine störende Cyberoperation. Außerdem begründet eine solche Handlung höchstens eine Verantwortlichkeit nach Art. 25 III lit. a / lit. c IStGH-Statut und stellt an sich noch keinen Völkermord dar.[43]

b) Das Verbrechen der Aggression nach Art. 8bis IStGH-Statut

Möglich erscheint hingegen die Verwirklichung des Verbrechens der Aggression nach Art. 8bis IStGH-Statut.

aa) Persönliche Voraussetzungen des Täters

Das Besondere am Verbrechen der Aggression nach Art. 8bis IStGH-Statut ist, dass es nicht von jedermann begangen werden kann, sondern gem. Art. 8bis I IStGH-Staut nur von Personen oder Personengruppen,[44] die in der Lage sind das politische oder militärische Handeln eines Staates zu kontrollieren oder zu lenken. Im Falle von Cyberoperationen heißt das aber nicht, dass diese Personen die Cyberoperation selbst durchführen müssen, was regelmäßig wohl ihre Fähigkeiten übersteigen dürfte. Es muss vielmehr reichen, dass diese Personen die Cyberoperation anordnen, sie also verantwortlich für die betreffende Cyberoperation sind.[45] Zu vergleichen ist dies mit herkömmlichen Angriffen, in denen sich die Verantwortlichen häufig ebenfalls nicht selbst die Hände schmutzig machen.

bb) Fall des Art. 8bis II?

Die Frage, ob eine störende Cyberoperation überhaupt ein Fall von Art. 8bis II sein kann, ist in zwei Schritten zu klären. Zunächst ist festzustellen, ob es sich bei der störenden Cyberoperation um Waffengewalt handelt. Anschließend ist zu prüfen, ob sie einem Tatbestandsmerkmal des Art. 8bis II lit. a - g IStGH-Statut unterfällt.

(1) Störende Cyberoperationen als Waffengewalt?

Der Begriff der bewaffneten Gewalt ist im Völkerrecht unter anderem in der UN-Charta immer wieder zu finden. Allerdings ist die Definition des Begriffs uneinheitlich, wobei an drei Stellen angesetzt werden kann.[46]

(a) Instrument-based-Ansatz

Zunächst erscheint es logisch im Sinne des Instrument-based-Ansatzes die Definition vom Wort Waffe abzuleiten. Demnach ist ein bewaffneter Angriff das Anwenden kinetischer Gewalt durch traditionelle Waffen.[47] Das Problem dieses Ansatzes ist, dass er sehr einengt, da er lediglich die physischen Merkmale des Angriffs in den Fokus nimmt.[48] Dieser Ansicht zufolge könnten Cyberoperationen niemals Waffengewalt darstellen, was sich jedoch nur schwer erklären lässt. Denn wie bereits ausgeführt, können auch störende Cyberoperationen den Tod und die Verletzung von Menschen verursachen. Es leuchtet daher nicht ein, warum die Tötung von Menschen mittels herkömmlichen Waffen anders zu bewerten sei als die mit modernen Waffen.[49] Dazu kommt, dass der Instrument-based-Ansatz schon Schwierigkeiten hatte,

zu erklären, warum Bio- und Chemiewaffen, die ja gerade keine kinetische Wirkung entfalten, als Waffen gelten.[50] Dieser Ansatz muss ständig prüfen, ob neuartige Waffen wie herkömmliche Waffen eingeordnet werden können,[51] was ihn darüber hinaus äußerst unpraktikabel erscheinen lässt. Gegen diese Ansicht spricht weiterhin die Staatenpraxis, wonach Grenzgefechte mit herkömmlichen Waffen lediglich als „Grenzscharmützel" abgetan wurden.[52] Zudem gilt laut dem Internationalen Gerichtshof (IGH) jede Gewaltanwendung als Waffengewalt, unabhängig von den eingesetzten Waffen.[53] Es kann also nicht allein darauf ankommen, ob herkömmliche Waffen für einen Angriff verwendet wurden.

(b) Target-based-Ansatz

Der Target-based-Ansatz nimmt bei der Bestimmung, wann es sich um Waffengewalt handelt, das Ziel des Angriffs in den Fokus. Nach diesem Ansatz handelt es sich um bewaffnete Gewalt, sobald eine Operation gegen national kritische Infrastruktur durchgeführt wird.[54] Der Vorteil dieses Ansatzes liegt darin, dass er komplett vom Begriff der Waffe losgelöst ist, es hier also nicht auf die Art der Waffe ankommt. Gleichzeitig hat er aber zwei eklatante Schwächen. Zum einen ist er zu offen,[55] sogar das Ausspähen von Daten, das anerkannter Weise nicht verboten ist,[56] würde sofort als ein bewaffneter Angriff gesehen werden. Dies entspricht auch nicht der Staatenpraxis, nach der Staaten bisher recht tolerant mit Angriffen auf ihre nationale kritische Infrastruktur umgingen und sich nicht darauf beriefen Ziel eines bewaffneten Angriffs geworden zu sein.[57] Zum anderen verlagert dieser Ansatz das Definitionsproblem der Waffe lediglich in den Bereich der nationalen kritischen Infrastruktur, wo schnell Abgrenzungsprobleme entstehen können,[58] da jedes Land eigene Kriterien bei der Bestimmung seiner nationalen kritischen Infrastruktur heranzieht.[59]

(c) Effect-based-Ansatz

Als dritter Ansatzpunkt ist der Effect-based-Ansatz zu sehen, der auf die Wirkung der Operationen abstellt. Demnach stellt jede Operation, deren Auswirkungen auch durch kinetisch wirkende Waffen hätten erreicht werden können, einen bewaffneten Angriff dar.[60] Dies ergibt vor allem Sinn, wenn man bedenkt, dass das humanitäre Völkerrecht und damit auch das Völkerstrafrecht auf die internationale Eingrenzung von Gewalt und deren Auswirkungen abzielt.[61] Zudem ist auch die Beurteilung der Rechtswidrigkeit von Taten meist an deren Folgen geknüpft.[62] Der Effect-based-Ansatz überzeugt also zunächst. Auch Vertreter des Instrument-based-Ansatzes stimmen dem Effect-based-Ansatz im Prinzip zu, wenn sie die Definition von Waffen auf deren Wirkung stützen.[63]

Doch auch dieser Ansatz orientiert sich zu nah an den Auswirkungen herkömmlicher Waffen. Dadurch liegt es nah, einen bewaffneten Angriff erst dann zu sehen, wenn das betroffene Teil physisch ausgewechselt werden muss.[64] Dabei ist es doch gerade das Besondere an Cyberoperationen, dass sie – im Übrigen wie Bio- und Chemiewaffen auch – physisch nicht zerstören müssen, um großen Schaden anzurichten.[65] Es kann folglich nicht darauf ankommen, ob der angerichtete Schaden physisch oder elektronisch behoben wird. Eine derart konservative Auslegung des Wirkungsbegriffs hinterließe eine klaffende Schutzlücke, nicht nur in Art. 8bis IStGH-Statut, sondern zum Beispiel auch in Art. 51 UN-Charta und würde somit das Selbstverteidigungsrecht der Staaten untergraben.

(d) Effect-on-target-based-Ansatz

Bei Betrachtung der einzelnen Ansätze liegt es nahe, ähnlich wie bei der Bestimmung der Schwere von Taten, nicht nur eine Komponente der Operation in den Fokus zu nehmen.[66] Indem man die Auswirkungen auf das Ziel betrachtet, können sowohl reine Funktionsbeeinträchtigungen, als auch physischer Schaden unter den Begriff der Waffengewalt subsumiert werden,[67] sodass der Target-based-Ansatz eingeengt und der Effect-based-Ansatz geweitet

werden. Konkret heißt das, je wichtiger die betreffende nationale Infrastruktur gesehen wird, desto geringer müssen die Auswirkungen auf sie sein, um als Waffengewalt zu gelten.[68] Dies erlaubt zwar keine klare Definition der Waffengewalt – dies ist vielmehr im Einzelfall zu prüfen – was aber aufgrund der Vielzahl der unterschiedlichen heutigen und zukünftigen Angriffsmethoden auch nicht möglich ist. Der Effect-on-target-based-Ansatz garantiert dabei eine nachvollziehbare Leitlinie dafür, wann eine Operation als Waffengewalt anzusehen ist.

(2) Alternativen des Art. 8bis II IStGH-Statut

Bei der Prüfung, ob störende Cyberoperationen einem Fall von Art. 8bis II lit. a - g IStGH-Statut unterfallen können, kommen im Prinzip nur lit. b[69] und lit. d[70] in Betracht.[71] Bei Art. 8bis II lit. a IStGH-Statut ist das Wort „Waffe" keinesfalls eng im Sinne von herkömmlicher, durch kinetische Energie wirkende Waffe zu verstehen.[72] Dem steht der Wortlaut der Norm „Waffe jeder Art"[73], wonach der Begriff der Waffe weit zu fassen ist, entgegen.[74] Auch nach Ansicht des IGH ist der Begriff der Waffe weit auszulegen, wonach auch Cyberoperationen als Waffe gelten können, soweit sie ähnliche Auswirkungen wie konventionelle Waffen haben.[75]

Auch eine Erfüllung des Tatbestandes von lit. d stellt kein Problem dar. Wie bereits erläutert, können störende Cyberoperationen einen Angriff darstellen. Wird dieser von Streitkräften eines Staates gegen Streitkräfte eines anderen Staates durchgeführt, ist lit. d also erfüllt.[76]

Darüber hinaus ist es aufgrund des Analogieverbots aus Art. 22 II IStGH-Statut nicht möglich störende Cyberoperationen analog unter andere Fälle von Art. 8bis II lit. a - g IStGH-Statut zu subsumieren.[77]

(3) Schwellenklausel aus Art. 8bis I IStGH-Statut

Auch wenn Cyberoperationen Angriffshandlungen sein können, ist weiterhin fraglich, ob Cyberoperationen überhaupt offensichtliche Verstöße gegen die UN-Charta darstellen, also die Schwellenklausel des Art. 8bis I IStGH-Statut überschreiten. Das Problem hierbei ist die Unbestimmtheit der Schwellenklausel, die sich wiederum aus der Unbestimmtheit der Angriffshandlung in Art. 8bis II IStGH-Statut ergibt.[78] Dadurch ergeben sich Grauzonen, in denen jederzeit erklärt werden kann, dass die Verletzung der UN-Charta im vorliegenden Fall nicht offenkundig gewesen sei.[79] Das Gegenteil ist hier schwer beweisbar, sodass die Gefahr besteht, dass Art. 8bis IStGH-Statut lediglich zu einer Symbolnorm degradiert wird.[80] Klar ist, dass es aufgrund der Formulierung in Art. 8bis IStGH-Statut einen Unterschied zwischen einer Angriffshandlung und dem Verbrechen der Aggression geben muss.[81] Dies hat die UN-Generalversammlung konkretisiert, indem nur die gefährlichste Form der Angriffshandlung die Schwellenklausel erfüllen soll.[82] Die Angriffshandlung muss demnach ihrer Art, ihrer Schwere und ihres Umfangs nach eine offenkundige Verletzung der UN-Charta darstellen.[83] Eine solch hohe Schwelle legitimiert dabei aber bei weiten nicht Gewaltanwendungen, da diese zwar nicht zwangsweise unter das Verbrechen der Aggression fallen, aber weiterhin verboten sind.[84] Die Anforderungen, die eine störende Cyberoperation erfüllen muss, um ein Verbrechen der Aggression darzustellen, sind also hoch, aber nicht unüberwindbar.[85] Hat eine störende Cyberoperation zur Folge, dass eine Vielzahl an Menschen sterben sowie physischen und psychischen Schaden erleide,[86] überschreitet sie zweifellos die Schwellenklausel des Art. 8bis I IStGH-Statut.[87] Trotz alledem ist es nicht möglich, hier generelle Aussagen zu treffen; eine Einzelfallprüfung ist stets unentbehrlich.[88]

(4) Zwischenfazit

Eine Verwirklichung des Verbrechens der Aggression nach Art. 8bis IStGH-Statut ist also möglich.

c) Kriegsverbrechen nach Art. 8 IStGH-Statut

Störende Cyberoperationen könnten in einem bewaffneten Konflikt auch Kriegsverbrechen darstellen. Damit eine Handlung ein Kriegsverbrechen darstellt, muss es eine konkrete Verbindung zwischen der Handlung und dem bewaffneten Konflikt geben.[89] So ist ein Kriegsverbrechen nach dem bewaffneten Konflikt, in dem es geschieht, geformt oder davon abhängig.[90] Dabei muss der bewaffnete Konflikt zwar nicht unbedingt kausal für die Tat geworden sein, aber eine essentielle Rolle für den Täter gespielt haben, sei es, dass die Tat dem Täter so erst möglich geworden ist, dem Täter dadurch der Tatentschluss gekommen ist, oder dass er die Tat durch den bewaffneten Konflikt auf eine gewisse Art und Weise ausführen konnte.[91] In einem bewaffneten Konflikt können störende Cyberoperationen also nur Kriegsverbrechen darstellen, soweit eine solche konkrete Verbindung zu dem jeweiligen bewaffneten Konflikt besteht. In der Regel dürfte es sich hierbei um das Hervorrufen des Tatentschlusses handeln, da gerade durch die territoriale Entgrenzung des Cyberspace Cyberoperationen immer möglich sind und im Gegensatz zu herkömmlichen Angriffen nicht erst durch den bewaffneten Konflikt möglich gemacht werden.

In einem bewaffneten Konflikt liegt es nahe, dass störende Cyberoperationen dazu verwendet werden, geschützte Objekte oder Personen anzugreifen. Hier kann in drei Fallgruppen unterschieden werden.[92]

aa) Angriff direkt gegen geschützte Personen oder Objekte

Die offensichtlichste Art ein solches Kriegsverbrechen zu begehen, ist der direkte Angriff auf geschützte Objekte. Angriff ist dabei gemäß Art. 49 I des 1. Zusatzprotokolls zur Genfer Konvention (ZP I) jede offensive wie defensive Gewaltanwendung gegen den Gegner. Diese Definition des Angriffs setzt schon vom Wortlaut her eine deutlich geringere Intensität voraus als der des bewaffneten Angriffs des Art. 8bis II IStGH-Statut. Eine Einbeziehung jeder Gewalt ist auch unter dem Aspekt sinnvoll, dass es hier in erster Linie um den Schutz bestimmter Gruppen in einem bewaffneten Konflikt – in dem durch die Anwendung des Ius in bello Menschenrechte arg beschnitten werden – geht.[93] Eine störende Cyberoperation kann also unbestritten einen Angriff im Sinne des Art. 49 I ZP I darstellen.[94] Wenn ein Staat in einem internationalen bewaffneten Konflikt online Patientendaten in einem Krankenhaus derart verändert, dass Patienten falsch behandelt werden und deswegen sterben, so begeht die ausführende Person zweifellos ein Kriegsverbrechen nach Art. 8 II lit. b i) IStGH-Statut.

bb) Angriff auf Dual-use-Objekte

Komplizierter gestaltet sich die Lage hingegen, wenn sich der Angriff gegen sogenannte Dual-use-Objekte richtet, also gegen solche, die nicht rein zivil, sondern auch militärisch genutzt werden. Nach Art. 52 II ZP I sind militärische Objekte solche, die aufgrund ihrer Beschaffenheit, ihres Standortes, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den in dem betreffenden Zeitpunkt gegebenen Umständen einen eindeutigen militärischen Vorteil darstellen. Diese Definition wirft eine entscheidende Frage auf:

Sind der Cyberspace und die in ihm enthaltenen elektronischen Daten überhaupt Objekte im Sinne des Art. 52 ZP I? Klar ist, dass – wenn überhaupt – nur die physische Infrastruktur des Cyberspace ein Objekt im herkömmlichen physischen Sinne darstellt.[95] Die Nichteinbeziehung von virtuellen Objekten des Cyberspace würde allerdings zu nicht nachvollziehbaren Abgrenzungen führen.[96] So wäre die auf einem elektronischen Chip gespeicherte Datei kein Objekt, der Chip an sich schon. Die Zerstörung eines günstigen Computerchips würde dann mehr wiegen, als die alleinige Beschädigung einer bedeutsamen Datei. Zudem hinterließe in

der heutigen Zeit die Reduzierung des Wortes Objekt auf rein physische Objekte eine gewaltige Schutzlücke, da so der zivile Cyberspace kein ziviles Objekt und somit nicht geschützt wäre. Auch der authentische Wortlaut des Art. 52 ZP I steht der Erfassung rein elektronischer Daten als Objekt nicht entgegen.[97] Der Cyberspace und die in ihm enthaltenen elektronischen Daten können somit Objekte im Sinne des Art. 52 ZP I sein.

(1) Unterscheidungsgebot

Eine Besonderheit des Cyberspace ist, dass die militärische und zivile Infrastruktur so eng wie in keinem anderen Bereich verwoben sind. Militärische Cyberoperationen sind auf zivile Server angewiesen und nutzen diese, ohne dass das Militär dies beabsichtigen würde.[98] Daraus und aus dem Fakt, dass Verlauf und Folgen von Cyberoperationen derzeit nie ganz absehbar sind,[99] folgt, dass von jeder gegen das Militär geführten Cyberoperation Zivilisten und andere geschützte Objekte betroffen sein können.[100] Dem IKRK zufolge verstieße folglich jede Cyberoperation gegen das in Art. 51 IV ZP I normierte Unterscheidungsgebot, da jeder Angriff auf militärische Cyber-Infrastruktur gleichzeitig einen Angriff auf die zivile darstellt.[101]

Andere meinen, dass gerade durch die Verwobenheit militärischer und ziviler Cyber-Infrastrukturen diese als einheitliches Objekt zu sehen sind.[102] Da zivile Objekte in Art. 52 I ZP I negativ als alle nicht militärische Objekte definiert sind und grundsätzlich jede noch so geringe elektronische Speicherkapazität militärisch genutzt werden kann,[103] soll der Cyberspace ein militärisches Objekt sein und somit angegriffen werden können.[104]

Obwohl der gesamte Cyberspace militärisch genutzt werden kann, unterfällt ein Großteil davon vermutlich rein ziviler Nutzung. Objekte, die militärisch und zivil genutzt werden, heißen Dual-use-Objekte.[105] Die Legitimität für Angriffe auf Dual-use-Objekte ist auf der Ebene der Verhältnismäßigkeit von Angriffen zu prüfen.[106]

(2) Verhältnismäßigkeitsgrundsatz Art. 51 V lit. b ZP I

Der Verhältnismäßigkeitsgrundsatz ist in Art. 51 V lit. b ZP I derart definiert, dass ein Angriff als unterschiedslos gilt, bei dem damit zu rechnen ist, dass er den Tod oder die Verwundung von Zivilpersonen oder die Beschädigung ziviler Objekte verursacht, die in keinem Verhältnis zum erwarteten konkreten militärischen Vorteil stehen. Es ist also der konkrete zu erwartende militärische Vorteil gegen den voraussichtlichen Schaden der Zivilbevölkerung abzuwägen.

Problematisch ist hier das Wort „Beschädigung".[107] Insbesondere störende Cyberoperationen zeichnen sich dadurch aus, dass sie keinen physischen Schaden an Objekten hervorrufen, sondern lediglich ihre Funktionalität hemmen. Doch kann man den Funktionsverlust mit Beschädigung gleichsetzen? Dafür spricht, dass Art. 51 V lit. b ZP I von Beschädigung spricht, während in Art. 52 II ZP I von vollständiger oder teilweiser Zerstörung und Neutralisierung die Rede ist.[108] Das lässt darauf schließen, dass Beschädigung ein Oberbegriff für die ganze oder teilweise Zerstörung sowie die reine Neutralisation eines Objekts ist.[109] Dafür spricht auch der Sinn und Zweck der Norm, der ja ziviles Eigentum schützen soll.[110] Für einen Zivilisten dürfte es kaum einen Unterschied darstellen, ob er seinen Computer nicht benutzen kann, weil er physisch kaputt ist oder weil ihm elektronisch der Zugang zu diesem verwehrt wurde. Auch der authentische Wortlaut der Norm spricht nicht dagegen, dass Beschädigung auch den reinen Funktionsverlust umfasst.[111] Dass dies richtig ist, sieht man daran, dass die Zerstörung eines zivilen Autos zwar einen geringen, aber immerhin einen Angriff auf die Zivilbevölkerung darstellen würde, die elektronische Lahmlegung des gesamten zivilen Kommunikationsnetzwerkes aber nicht.[112] Der reine Funktionsverlust gilt also auch als Beschädigung im Sinne des Art. 52 V lit. b ZP I. Dabei ist aber auch zu berücksichtigen, dass im Gegensatz zu physischen Beschädigungen weder Reparatur noch Wiederaufbau nötig ist. Der Angreifer muss die störende Cyberoperation meist einfach beenden, damit das Objekt seine vollständige Funktion wiedererlangt. Eine reine Funktionsunterbrechung ist also mit geringeren Langzeitfolgen als

eine physische Beschädigung verbunden, was auch in der Verhältnismäßigkeit zu beachten ist.[113]

Was den eindeutigen militärischen Vorteil angeht, so ist es auch möglich diesen auf die gesamte Operation zu sehen,[114] zeitlich sind davon jedoch keine reinen Langzeitvorteile umfasst.[115]

Wie bereits erwähnt ist bei Cyberoperationen problematisch, dass ihre Folgen meist nicht ganz abzusehen sind, der Schaden und der Nutzen in der Verhältnismäßigkeit aber aus einer Ex-ante-Sicht zu beurteilen ist.[116] Ein Kommandeur könnte sich somit darauf berufen, er habe weder gewusst, noch gewollt, dass der Angriff unter anderem die Zivilbevölkerung trifft.[117] Der dem Kommandeur zustehende Beurteilungsspielraum ist aus der Sicht einer gut informierten, vernünftigen Person in den Umständen des Verursachers zu beurteilen.[118] Da unvorhergesehene Zweit- und Drittfolgen bei Cyberoperationen immer auftreten können, ist hier auch verstärkt mit solchen zu rechnen.[119]

(3) Vorsichtsmaßnahmen

Das führt dazu, dass entsprechende Vorsichtsmaßnahmen gemäß Art. 57, 58 ZP I bei und gegen Cyberoperationen zu treffen sind. So ist der Angreifer bei Cyberoperationen verpflichtet, dass Angriffsziel so weit möglich genau zu untersuchen, um mögliche ungewollte Nebenfolgen für die Zivilbevölkerung auszuschließen.[120] Sollte eine ausreichende Informationsgewinnung nicht möglich sein, so ist der Angriff – abhängig von anderen Faktoren wie der Lage des Ziels – nicht durchzuführen.[121] Umgekehrt ist es aufgrund der potentiell weniger schwerwiegenden Auswirkungen möglich, dass Cyberoperationen als Angriffsmethode zu wählen sind.

Doch gemäß Art. 58 ZP I hat auch die angegriffene Partei Vorsichtsmaßnahmen zu treffen, wie die Trennung von ziviler und militärischer Infrastruktur vorzunehmen. Bezogen auf den Cyberspace könnte das bedeuten, dass das Militär nur eine eigene, von der zivilen getrennte Cyberinfrastruktur nutzen müsste.[122] Dazu bräuchte es aber unter anderem eigene Router und Satelliten, was vermutlich keine Konfliktpartei stemmen könnte.[123] Zudem hätte dann der zivile Cyberspace immer noch militärisches Potential, was Angriffe auf diesen nicht ausschließen würde.[124] Zumindest ist aber die Zivilbevölkerung ausreichend gegen Cyberoperationen zu schützen.[125]

(4) Zwischenfazit

Ist eine störende Cyberoperation auf Dual-use-Objekte unverhältnismäßig und liegen die übrigen Tatbestandsvoraussetzungen vor, so ist in der Regel ein Kriegsverbrechen nach Art. 8 II lit. b i), ii), iii) iv), lit. e i), ii), iii) oder iv) IStGH-Statut verwirklicht.

cc) Angriffe gegen Hacker

Zu guter Letzt stellt sich die Frage, ob und wann Gegenangriffe gegen Personen Kriegsverbrechen darstellen, die störende Cyberoperationen durchführen oder durchgeführt haben. Dies ist dann nicht der Fall, wenn sie entweder Kombattantenstatus innehaben, sie einer organisierten bewaffneten Gruppe angehören oder wenn sie Zivilisten sind, die direkt an bewaffneten Auseinandersetzungen teilnehmen.[126]

(1) Mitgliedschaft in einer organisierten bewaffneten Gruppe

Um festzustellen, wann eine Mitgliedschaft in einer organisierten bewaffneten Gruppe vorliegt, ist erst zu klären, wie eine solche Gruppe definiert ist. Dies ist der Fall, wenn die Gruppe ausreichend organisiert ist, also eine Hierarchie herrscht, die sich in hinreichenden Kommando-, Kontroll-, und Disziplinarstrukturen derart niederschlägt,

dass die Gruppe in der Lage ist die Handlungen der einzelnen Mitglieder zu kontrollieren.[127]

Dabei stellt sich die Frage, ob rein online organisierte Gruppen eine solche bewaffnete Gruppe bilden können. Dafür spricht, dass in der Definition der organisierten bewaffneten Gruppe physischer Kontakt kein Strukturelement ist.[128] Schon der Internationale Strafgerichtshof für das ehemalige Jugoslawien (englisches Akronym: ICTY) hat eine hinreichende Organisation bei Gruppen, deren Mitglieder verstreut sind bejaht.[129] Gerade durch die Anonymität im Cyberspace ist es aber schwer vorstellbar, wenn auch nicht unmöglich,[130] dass sich in rein online organisierten Gruppen eine Autorität herausbildet, die eine entsprechende Hierarchie entstehen lässt.[131] Die unzureichende Organisation einer bewaffneten Gruppe bedeutet aber nicht automatisch, dass Angehörige dieser Gruppe als Zivilisten und damit als vom humanitären Völkerrecht besonders geschützt gelten.[132]

(2) Zivilisten, die direkt an bewaffneten Feindseligkeiten teilnehmen

Sie würden vielmehr als Zivilisten gelten, die direkt an bewaffneten Feindseligkeiten teilnehmen, soweit die von ihnen ausgehende oder unterstützte störende Cyberoperation dazu geeignet ist, militärische Fähigkeiten zu beeinträchtigen oder geschützten Personen oder Objekten Schaden zuzufügen, zwischen der Cyberoperation und dem Schaden ein Kausalzusammenhang besteht und die Cyberoperation zur Unterstützung oder Schädigung einer Partei bestimmt ist.[133] Solange eine störende Cyberoperation unter diesen Voraussetzungen durchgeführt wird, ist die handelnde Person entsprechend Art. 51 III ZP I ein legitimes Angriffsziel.[134]

Das Problem ist hier, dass Cyberoperationen in der Regel nur wenige Sekunden dauern und die Folgen meist verzögert auftreten.[135] Eine Zivilperson würde mithin nur wenige Sekunden an der Feindseligkeit teilnehmen, sodass es unter humanitärem Völkerrecht praktisch unmöglich ist, solche Cyberoperationen zu kontern.[136] Das führt im Ergebnis aber dazu, dass Kombattanten als „rechtmäßige" Konfliktsteilnehmer jederzeit mit Gegenangriffen rechnen müssten, direkt an Feindseligkeiten teilnehmende Zivilisten als „unrechtmäßige" Konfliktsteilnehmer im Prinzip vollständig durch ihren Status als Zivilperson geschützt sind.[137] Das liegt daran, dass Kombattanten potentiell immer Angriffshandlungen vornehmen können. Dementsprechend ist es konsequent, den Begriff „solange"[138] für Zivilisten, die wiederholt an direkt an Feindseligkeiten beteiligt waren, so auszulegen, dass er die Zeit vom ersten bis zum letzten Angriff meint.[139] Um Angriffe auf die Zivilbevölkerung zu vermeiden, muss dies aber restriktiv geschehen.

(3) Zwischenfazit

Erfüllt die hackende Person die oben genannten Kriterien, stellen Angriffe gegen diese Personen keine Kriegsverbrechen dar, solange die Angriffe im Einklang mit sonstigem humanitärem Völkerrecht stehen.

d) Verbrechen gegen die Menschlichkeit

Weiterhin erscheint es möglich, dass störende Cyberoperationen Verbrechen gegen die Menschlichkeit im Sinne des Art. 7 I IStGH-Statut darstellen. Voraussetzung dafür ist ein systematischer, groß angelegter Angriff auf die Zivilbevölkerung. Dies bedeutet laut Art. 7 II lit. a IStGH-Statut die mehrfache Begehung einer der in Art. 7 I IStGH-Statut aufgeführten Handlungen zur Ausführung oder Unterstützung der Politik eines Staates oder einer Organisation. Die Zurechnung einer störenden Cyberoperation gestaltet sich hier ebenso wie beim bewaffneten Konflikt über die Staatenverantwortlichkeit.[140]

Eine Organisation im Sinne des Art. 7 II lit. a IStGH-Statut zeichnet sich im Gegensatz zu der im bewaffneten Konflikt nicht durch ihre Kommandostruktur, sondern generelle Strukturen und Mechanismen aus, die hinreichend effizient sind, um eine Durchführung und Koordinierung eines solchen Angriffs zu gewährleisten.[141] Auch wenn die Kommandostruktur hier kein zwingendes Element mehr ist, so führt sie dennoch zu einer Effizienzsteigerung der Koordinierung und Durchführung des Angriffs, weswegen es auch hier unwahrscheinlich ist, dass eine reine Cyberorganisation diese Anforderungen erfüllt.

Bezüglich der Tatbestandsmerkmale ist zu sagen, dass hier allein die vorsätzliche Tötung nach Art. 7 I lit. a, sowie die Ausrottung nach lit. b IStGH-Statut möglich erscheinen.[142] Eine Lebensbedingung gemäß Art. 7 II lit. b IStGH-Statut die der Bevölkerung mittels störender Cyberoperation auferlegt wird und die zu deren Ausrottung führt, könnte hier der schon mehrmals angesprochene Stromausfall während eines strengen Winters sein.

Es können also auch Verbrechen gegen die Menschlichkeit durch störende Cyberoperationen begangen werden.

Es ist durchaus möglich, unter der alleinigen Anwendung störender Cyberoperationen den Tatbestand eines der vier völkerstrafrechtlichen Verbrechen des IStGH-Statuts zu verwirklichen.

Die Verbrechen der Aggression nach Art. 8bis IStGH-Statut, des Völkermords nach Art. 6 IStGH-Statut und die Verbrechen gegen die Menschlichkeit nach Art. 7 IStGH- Statut setzen jeweils heftige, groß angelegte oder präzise Angriffe voraus. Deshalb dürfte die Verwirklichung von Kriegsverbrechen nach Art. 8 IStGH-Statut derzeit am relevantesten sein.

3. Individuelle Kriminelle Verantwortlichkeit

Bezüglich der individuellen kriminellen Verantwortlichkeit unterscheiden sich störende Cyberoperationen nicht von anderen Tathandlungen. So sind die in Art. 25 IStGH-Statut niedergelegten Begehungsformen unproblematisch auch auf Cyberoperationen anwendbar. [143]

Bei störenden Cyberoperationen ist dabei insbesondere die Tatbegehung durch einen anderen relevant (Art. 25 III lit. a IStGH-Statut), bei der das Tatwerkzeug irrt.[144] So wird durch das reine Verändern von Patientendaten mittels Cyberoperation in einem Krankenhaus noch kein Mensch geschädigt. Dies geschieht erst mit der falschen Behandlung durch den aufgrund der veränderten Daten irrenden Arzt.

Bei teilnehmenden Begehungsformen, wie der Anstiftung nach Art. 25 III lit. b oder Unterstützung nach lit. c IStGH-Statut ist zu beachten, dass die unvorhersehbaren Folgen stets aus der Ex-ante-Sicht eines vernünftigen Menschen in einer vergleichbaren Situation zu beurteilen sind, sodass diese nie gänzlich unvorhergesehen sind.[145]

Eine besondere Form der Verantwortlichkeit stellt die Aufstachelung zum Völkermord nach Art. 25 III lit. e IStGH-Statut dar. Diese muss an einem öffentlichen Ort, worunter auch die Massenmedien wie das Internet zählen,[146] stattfinden. Aufgrund der Schwere der Schuld muss auch direkt zum Völkermord aufgestachelt werden, eine bloße Hassrede reicht hier nicht aus.[147] Bezogen auf Cyberoperationen wäre es beispielsweise denkbar, dass jemand die Socialmediakanäle der Tagesschau hackt und darüber zum Völkermord aufruft.

C Fazit

Die vorliegende Untersuchung beschäftigt sich mit der völkerstrafrechtlichen Bewertung von rein störenden Cyberoperationen.

Dabei konnte zunächst festgestellt werden, was rein störende Cyberoperationen überhaupt sind und dass sie, auch wenn sie nicht physisch zerstören, durch die aus ihnen resultierende Funktionalitätseinschränkung der Zielobjekte ähnliche Konsequenzen wie physisch zerstörende Cyberoperationen haben können. Soweit die Folgen schwerwiegend genug sind, kann auch der IStGH seine Gerichtsbarkeit über störende Cyberoperationen ausüben.

In der Folge wurde geprüft, ob die einzelnen Verbrechen des IStGH-Statuts von rein störenden Cyberoperationen erfüllt werden können. Dabei ist festgestellt worden, dass es bis auf den Völkermord nicht unwahrscheinlich ist, dass die Verbrechen des IStGH-Statuts auch von störenden Cyberoperationen verwirklicht werden.

Wichtig ist bei alledem jedoch, dass die Begriffe, die das Völkerrecht – insbesondere das humanitäre Völkerrecht und das Völkerstrafrecht – derzeit bereitstellt, offen für neue Begehungsformen interpretiert werden, da ansonsten erhebliche Strafbarkeitslücken entstehen. Gerade störende Cyberoperationen würden diese ausnutzen können und vor allem im bewaffneten Konflikt den Schutz geschützter Personen und Objekte untergraben. Bei einer offenen Interpretation aber zeigt sich, dass rein störende Cyberoperationen ohne große Probleme unter die Verbrechenstatbestände subsumiert werden können. Auch bei der individuellen völkerstrafrechtlichen Verantwortlichkeit treten keine besonderen Probleme auf. Durch die Besonderheit von störenden Cyberoperationen, so vielfältige Auswirkungen wie keine konventionelle Methode der Kriegsführung zu haben, ist eine Einzelfallprüfung jedoch stets unentbehrlich.

Wie die meisten völkerrechtlichen Themen ruft die völkerstrafrechtliche Diskussion rein störender Cyberoperationen nach mehr internationaler Zusammenarbeit, rechtlicher sowie tatsächlicher Natur. Denn zwei Faktoren machen Cyberoperationen so gefährlich: Erstens, die Unberechenbarkeit – auch für den Ausführenden – solcher Angriffe. Das heißt, Cyberoperationen können auch dort verheerende Auswirkungen haben, wo niemand diese für möglich gehalten hat. Zweitens, die geographische Entgrenzung im Cyberspace. Durch das Fehlen physischer Grenzen und Distanzen können Angriffe jedes Ziel jederzeit treffen. Zur Verhinderung von Völkerrechtsverbrechen folgen daraus zwei Konsequenzen: Zum einen müssen sich Staaten und die Weltgemeinschaft technisch rüsten, um Cyberoperationen stets von sich und ihren Bürgern abwehren zu können. Zum anderen müssen verbindliche Regeln über den Umgang mit Cyberoperationen geschaffen werden. Zwar können störende Cyberoperationen unter die bereits vorhandenen Verbrechenstatbestände des IStGH-Statuts subsumiert werden. Abgesehen davon gibt es keine verbindlichen Rechtsquellen, die sich speziell auf Cyberoperationen beziehen. Wie die Diskussion um die Angriffsqualität störender Cyberoperationen gezeigt hat, subsumieren viele Rechtsgelehrte störende Cyberoperationen in der Regel nicht unter die Angriffsdefinitionen der verschiedenen völkerrechtlichen Verträge. Schließt der IStGH sich solchen restriktiven Auslegungen an, wird ohne spezielle rechtsverbindliche Normen der Schutz des humanitären Völkerrechts sowie des Völkerstrafrechts unterlaufen.

Fakt ist aber auch, dass es noch keinen nachgewiesenen Fall eines mittels störender Cyberoperation begangenen Völkerrechtsverbrechens gab. Die Rechtsetzung hat hier also die Chance, der technischen Entwicklung vorauszugreifen und bereits so mittels Cyberoperation begangenen Völkerrechtsverbrechen vorzubeugen.

Neben den völkerrechtlichen Gesichtspunkten steht derweil das praktische Problem, dass eine Strafverfolgung von mittels Cyberoperation begangenen Völkerrechtsverbrechen aufgrund der Anonymität des Internets quasi unmöglich ist. Es besteht somit die Gefahr, dass störende

Cyberoperationen genutzt werden, um straffrei Völkerrechtsverbrechen zu begehen. Die Diskussion, ob es sinnvoll ist die Anonymität im Internet abzuschaffen, ist aber an anderer Stelle zu führen.

---

1 Vgl. *Johann-Christoph Woltag,* Military Cross-Border Computer Network Operations under International Law, 1. Auflage 2014, S. 41 ff.; *Heather Harrison Dinniss,* Cyber Warfare and the Laws of War, 2012, S. 6 ff.

2 "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace", US Department of Defense, Dictionary of Military and Associated Terms, 2010 S. 55.

3 Das Tallinn Manual ist ein akademisches Handbuch einer internationalen Expertengruppe, das beschreibt, wie insbesondere humanitäres Völkerrecht auf Konflikte im Cyberspace anzuwenden sind. Die aufgestellten Regeln sind nicht bindend.

4 "The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace", *Michael Schmitt*, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013, S. 258.

5 *Schmitt*, Tallinn Manual (Anm. 4), S. 258; vgl. US Department of Defense, Dictionary of Military and Associated Terms, 2010, S. 55.

6 "Cyber operations can be broadly described as operations against or via a computer or a computer system through a data stream", so das Internationale Komitee vom Roten Kreuz (IKRK), Bericht vom 31. Oktober 2011, 31IC/11/5.1.2., S. 36.

7 "Computer network attacks are 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", so *Harrison Dinniss* (Anm. 1), S. 4.

8 Ebda., S. 5.

9 Ebda.; *Luca Alexander Petersen,* Cyber Angriffe – Definition, Regulierung, Pönalisierung, in: GRZ 1/2020, S. 25 – 36 (S. 25, 26)

10 *Petersen* (Anm. 9), S. 25, 26.

11 *Tobias Keber/Przemyslaw Roguski*, Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und der aktuellen Staatenpraxis, in: AVR 2011, S. 399 – 435 (S. 405); *Marco Roscini,* Cyber Operations and the Use of Force in International Law, 2014, S. 12.

12 *Roscini* (Anm. 11), S. 16; *Michael Gervais,* Cyberattacks and the Laws of War, *in:* J.L. & CyberWarfare 2012, S. 8 – 98 (S. 20 f.); vgl. DoD Dictionary of Military and Associated Terms, 2021, S. 55.

13 „[A]ttacks are characterised by having effects in the real world beyond the cyber system itself." *Henning Lahmann*, Unilateral Remedies to Cyber Operations – Self Defense, Countermeasures, Necessity and the Question of Attribution, 2020, S. 20; *Schmitt*, Tallinn Manual (Anm. 4), S. 106.

14 S. *Gary Brown/Owen Tullos*, On the Spectrum of Cyberoperations, in: Small Wars Journal, 2012, verfügbar unter https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations, abgerufen am 11. Februar 2022; *Roscini* (Anm. 11), S. 16; *Lahmann* (Anm. 13), S. 20

15 *Louise Arimatsu,* Classifying Cyber Warfare in: Nicholas Tsagourias/Russell Buchan (Hrsg.) International Law and Cyberspace, 2015, S. 326 – 342 (S. 332); vgl. *Marco Roscini,* Gravity in the Statute of the International Criminal Court and Cyber Conduct that constitutes, Instigates or Facilitates International Crimes, CLF 2019, S. 247 – 272 (S. 261).

16 *Roscini* (Anm. 15), S. 261.

17 *Sean Kanuck*, Information Warfare: New Challenges for Public International Law, in: Havard Int'l Law Journal 1996 S. 272 – 292 (S. 287); *Rex Hughes,* A Treaty for Cyberspace, in: International Affairs 2010, S. 523 – 541 (S. 539).

18 *Nicholas Tsagourias,* The Legal Status of the Cyberspace, in: Tsagourias/Buchan (Anm. 15) S. 13 – 29 (S. 13); *Anne-Laure Chaumette*, International Criminal Responsibility of Individuals in Case of Cyberattacks, in: ICLRev. 2018, S. 1 – 35 (S. 10).

19 *Schmitt*, Tallinn Manual (Anm. 4), S. 16; s. *Harrison Dinniss* (Anm. 1), S. 29; *Petersen* (Anm. 9), S. 27; *Woltag* (Anm. 1), S. 57; *Tsagourias* (Anm. 18), S. 24.

20 Vgl. statt vieler *Harrison Dinniss* (Anm. 1), S. 29.

21 In der authentischen englischen Fassung "the conduct in question".

22 *Robin Geiss*, Implications for Non International Armed Conflicts, in: Int'lLStudies 2013, S. 627 – 645 (S. 637); *Harrison Dinniss* (Anm. 1), S. 29.
23 *Chaumette* (Anm. 18), S. 22; *Schmitt,* Tallinn Manual 2.0 on International Law Applicable to Cyber Operations, 2017, S. 55.
24 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 55.
25 Im Ergebnis ähnlich *William Schabas*, The Internation Criminal Court – A Commentary, 2010, S. 285.
26 *Crawford*, UN Doc a/cn.4/sr2330, Agenda item 4, Nr. 9; vgl. *Rachel López*, The Law of Gravity CLMJTL 2020, S. 565 - 622 (S. 586).
27 Etwa die Aufhebung nationaler Amnestien und Immunitäten, s. *Margaret de Guzman*, How Serious are International Crimes? The Gravity Problem in International Criminal Law, in: CLMJTL 2012, S.18 – 55, (S. 20).
28 So hat der Wirtschafts- Sozial- und Kulturrat der Afrikanischen Union dieser geraten, sich aufgrund der überdurchschnittlichen Anzahl von Verfahren des IStGH gegen afrikanische Staatsoberhäupter aus dem IStGH-Statut zurückzuziehen, s. https://www.jurist.org/news/2016/07/au-advisory-board-accuses-icc-of-bias-against-african-nations/ eingesehen am 11. Februar 2022; bekräftigt durch https://www.loc.gov/item/global-legal-monitor/2017-02-10/african-union-resolution-urges-states-to-leave-icc/ eingesehen am 11. Februar 2022.
29 Regulations of the Office of the Prosecutor, icc-bd/05-01-09, Nr. 29.
30 The Office of the Prosecutor, Policy Paper on Preliminary Examinations, 11/2013, Nr. 62.
31 *Margaret de Guzman*, Gravity and the Legitimacy of the International Criminal Court, FDMILJ 2009, S. 1400 - 1465 (S. 1451); *Roscini* (Anm.15), 261.
32 The Office of the Prosecutor (Anm. 30), Nr. 63; *De Guzman* (Anm. 31), S. 1452; *Roscini* (Anm.15), S. 261.
33 IStGH, *Prosecutor v. Ahmad Al Faqi Al Mahdi*, Entscheidung vom 27. September 2016, ICC-01/12-01/ 15-171, Nr. 77.
34 The Office of the Prosecutor (Anm. 30), Nr. 64.
35 Ebda.
36 *Roscini* (Anm. 15), S. 266.
37 S. The Office of the Prosecutor (Anm. 29), Nr. 65.
38 Vgl. *Roscini* (Anm. 15), S. 268.
39 Ebda.
40 *Chaumette* (Anm. 18), S. 9.
41 Ebda.
42 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 66.
43 *Chaumette* (Anm. 18), S. 9; *Schmitt*, Tallinn Manual 2.0, (Anm. 23), S. 66.
44 *Andreas Zimmermann/Elisa Freiburg* in: Otto Tiffterer/Kai Ambos (Hrsg.), The Rome Statute of the International Criminal Court, 2016, Art. 8bis IStGH-Statut, Rn. 35.
45 *Kai Ambos,* International Criminal Responsibility in Cyberspace, in: Tsagourias/Buchan (Anm. 15) S.118 – 146 (S. 138); *Zimmermann/Freiburg* (Anm. 44), Rn. 92.
46 Vgl. statt vieler: *Chaumette* (Anm. 18), S. 7.
47 *Ambos* (Anm. 45), S. 138.
48 *Marco Roscini*, Cyberoperations as a Use of Force in: Tsagourias/Buchan (Anm. 15), S. 233 – 254 (S. 236); *Matthew Waxman*, Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions, in: Int'l L. Studies, 2013, S. 109 – 122 (S. 111).
49 *Arimatsu* (Anm. 15), S. 329.
50 *Roscini* (Anm. 48), S. 239; *Chaumette* (Anm. 18), S. 7.
51 *Petersen* (Anm. 9), S. 28.
52 *Arimatsu* (Anm. 15), S. 330.
53 IGH-Gutachten vom 8. Juli 1996, Legality of the Threat or Use of Nuclear Weapons, Nr. 39.
54 *Christopher Joyner/Catherine Lotriont*e, Information Warfare as International Coercion – Elements of a Legal Framework, in: E.J.I.L., 2001, S. 825 – 865 (S. 855).
55 *Chaumette* (Anm. 18), S. 8; *Roscini* (Anm. 48), S. 236.
56 *James McGhee*, Hack, Attack or Whack - The Politics Impression on Cyberlaw, in: J.L. & CyberWarfare 2014, S. 13 – 41 (S. 17 f.); *Heike Krieger,* Krieg gegen Anonymous. Völkerrechtliche

Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, in: AVR, 2012, S. 1 – 20 (S. 8).

57 *Arimatsu* (Anm. 15), S. 332; vgl. *Gerhardt Walter*, Die größten Cyberattacken der vergangenen zwei, drei Jahre, in: Handelsblatt vom 23. September 2020, https://veranstaltungen.handelsblatt.com/cybersecurity/die-groessten-cyberattacken-der-vergangenen-zwei-drei-jahre/, eingesehen am 11. Februar 2022.

58 *Roscini* (Anm. 48), S. 236; *Chaumette* (Anm. 18), S. 8; *Petersen* (Anm. 9), S. 29.

59 S. UN-Generalversammlung, Resolution vom 23. Dezember 2002, GA Res 58/199.

60 *Chaumette* (Anm. 18), S. 8.

61 *Gervais* (Anm. 12), S. 29; *Julia Dornbusch*, Das Kampfführungsrecht im internationalen Cyberkrieg, 2018, S. 71.

62 So ist es egal, ob ein Mensch durch ein Messer oder Gift getötet oder verletzt wurde, *Dornbusch* (Anm. 61), S. 72.

63 So z.B. *Roscini* in Tsagourias/Buchan (Anm. 48), S. 236.

64 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 415; *Yoram Dinstein*, Computer Network Attacks and Self Defense, in: Int'l. L. Studies 2002, S. 99 – 119 (S. 103).

65 *Roscini,* in: Tsagourias/Buchan (Anm. 48), S. 237; *Ambos* in: Tsagourias/Buchan (Anm. 45), S. 124; *Reese Ngyuen*, Navigating Ius ad bellum in the Age of Cyber Warfare, in: CaliLRev 2013, S. 1097 – 1129 (S. 1103).

66 *Roscini* (Anm. 11), S. 55 ff.; s. *Dornbusch* (Anm. 61), S. 99 mit weiteren Nachweisen.

67 *Petersen* (Anm. 9), S. 30.

68 *Roscini* (Anm. 11), S. 59.

69 Der Einsatz von Waffen jeder Art durch einen Staat gegen das Hoheitsgebiet eines anderen Staates.

70 Der Angriff der Streitkräfte eines Staates gegen Streitkräfte eines anderen Staates.

71 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 139; *Chaumette* (Anm. 18), S. 8.

72 Ebda.

73 In der authentischen englischen Fassung "any weapon".

74 *Zimmermann/Freiburg* (Anm. 44), Rn. 126.

75 IGH-Gutachten (Anm. 53), Nr. 39; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 139.

76 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 139; *Chaumette* (Anm. 18), S. 8.

77 z.B. DDoS als Blockade i.S.v. Art. 8bis II lit. c IStGH-Statut, s. *Noah Weisbord*, Judging Aggression, in: CLMJTL 2011, S. 82 – 168 (S. 154).

78 *Kai Ambos*, Das Verbrechen der Aggression nach Kampala, ZIS 11/2010, S. 649 – 668 (S. 656).

79 *Zimmermann/Freiburg* (Anm. 44), Rn. 67.

80 Ebda.

81 Ebda., Rn. 51; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 141; *Ambos* (Anm. 79), S. 654.

82 "The most dangerous form of the use of force", UN-Generalversammlung, Resolution vom 11. Juni 2010, RC/Res.6/2010 Annex III, Nr. 6.

83 Vgl. UN-Generalversammlung (Anm. 82) Annex III, Nr. 6; *Zimmermann/Freiburg* (Anm. 44), Rn. 57; *Chaumette* (Anm. 18), S. 9.

84 *Ambos* (Anm. 79), S. 656.

85 *Petersen* (Anm. 9), S. 35, der aber verkennt, dass störende und physisch zerstörende Cyberoperationen ähnliche Auswirkungen haben können.

86 Wie etwa im oben genannten Beispiel eines großflächigen Stromausfalls im Winter.

87 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 141.

88 Ebda.

89 *Michael Cottier*, in: Otto Triffterer/Kai Ambos, The Rome Statute of the International Criminal Court, 2016, Art. 8 IStGH-Statut, Rn. 37; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 127.

90 ICTY, *Prosecutor v. Kunarac et al*., Entscheidung vom 12. Juni 2002, it-96-23 und it-96-23/1-A Nr. 58.

91 Ebda.

92 *Chaumette* (Anm. 18), S. 14.

93 *Dornbusch* (Anm. 61), S. 140.

94 *Chaumette* (Anm. 18), S. 15; *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 392 f.

95 *Chaumette* (Anm. 18), S. 15; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 131.

96 *Harrison Dinniss* (Anm. 1) S. 184; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 131.

97 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 131.
98 *Robin Geiss/Henning Lahmann*, Cyber Warfare: Applying the Principle of Distinction in an interconnected Space, in: IsraelLawReview 2012, S. 381 – 399 (S. 389); *Dan Saxon,* Violations of International Humanitarian Law by Non State Actors during Cyberwar: Challenges for Investigators and Prosecutors, in: J.C. & SecurityLaw, 2016, S. 555 – 574 (S. 557); *Cordula Droege*, Get off my Cloud: Cyber Warfare, International Humanitarian Law and the Protection of the Civilians, in: International Review of the Red Cross (IRRC) 2013, S. 535 – 578 (S. 570).
99 Zu sehen ist das am Beispiel des Computerwurms Stuxnet. Dieser wurde konkret und ausschließlich auf die Zielgeräte übertragen. Unvorhergesehenerweise infizierte er aber auch hunderte andere Geräte, ohne dass dies vorher in Betracht gezogen wurde. vgl. *Droege* (Anm. 98), S. 571.
100 *Chaumette* (Anm. 18), S. 16; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 131.
101 S. IKRK (Anm. 6), S. 38.
102 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 131; vgl. *Schmitt*, Tallinn Manual 2.0 (Anm. 23), Regel 39.
103 *Geiss/Lahmann* (Anm. 98), S. 389.
104 Vgl. *Schmitt*, Tallinn Manual 2.0 (Anm. 23), Regel 39; *Ambos* (Anm. 45), S. 131; *Droege* (Anm. 98), S. 562.
105 Statt vieler *Droege* (Anm. 98), S. 562.
106 *Geiss/Lahmann* (Anm. 98), S. 395; *Chaumette* (Anm. 18), S. 17.
107 In der authentischen englischen Fassung „damage".
108 In der authentischen englischen Fassung „destruction" und „neutralization".
109 *Geiss/Lahmann* (Anm. 98), S. 397.
110 Ebda; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 124.
111 *Geiss/Lahmann* (Anm. 98), S. 397.
112 Ebda.; *Droege* (Anm. 98), S. 572.
113 *Dornbusch* (Anm. 61), S. 180 f.; *Droege* (Anm. 98), S. 573; *Harrison Dinniss* (Anm. 1), S. 207 f.
114 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 474; *Woltag* (Anm. 1), S. 227; *Dornbusch* (Anm. 61), S. 178.
115 *Dornbusch* (Anm. 61), S. 179, mit Verweis auf den IKRK Kommentar zum ZP I.
116 *William Boothby,* Methods and Means of Warfare: in: Int'lLStudies, 2013, S. 387 – 405 (S. 392); *Dornbusch* (Anm. 61), S. 176.
117 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 135.
118 *Dornbusch* (Anm. 61), S. 179; *Geiss/Lahmann* (Anm. 98), S. 396.
119 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 473; *Harrison Dinniss* (Anm. 1), S. 207.
120 *Droege* (Anm. 98), S. 574; *Ambos* (Anm. 45), S. 137.
121 *Schmitt,* Tallinn Manual (Anm. 4), S. 168.
122 *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 137; *Schmitt*, Tallinn Manual (Anm. 4), S. 176.
123 *Droege* (Anm. 98), S. 576.
124 *Geiss/Lahmann* (Anm. 98), S. 394.
125 *Droege* (Anm. 98), S. 575 f.
126 *Ambos*, in: Tsagourias/Buchan (Anm. 45), S. 128.
127 Vgl. ICTY, *Prosecutor v. Limaj et al.* it-03-66-t, Entscheidung vom 30. November 2005, Nr. 98 f.; *Michael Schmitt,* Cyberoperations and the ius in bello – Key Issues, in: Int'lLawStudies 2011, S. 89 – 110 (S. 98); *Ders.,* Classification of Cyberconflict, in: JConflictSecL 2012, S. 245 – 260 (S. 255); *Geiss* (Anm. 22), S. 634; *Chaumette* (Anm. 18), S. 14.
128 *Arimatsu,* in: Tsagourias/Buchan (Anm. 15), S. 340.
129 S. ICTY, *Prosecutor v. Boskoski & Tarculovski,* Entscheidung vom 10. Juli 2008, it-04-82, Nr. 202.
130 *Schmitt,* Key Issues (Anm. 127), S. 99.
131 *Geiss* (Anm. 22), S. 636.
132 So aber *Schmitt,* Key Issues (Anm. 127), S. 99.
133 *Harrison Dinniss* (Anm. 1), S. 140 f.; *Ambos,* in: Tsagourias/Buchan (Anm. 45), S. 128; *Schmitt,* Key Issues (Anm. 127), S. 100.
134 Ebda.; s. ICTY, *Prosecutor v. Galic,* Entscheidung vom 5. Dezember 2003, it-98-29, Nr. 48.
135 *Schmitt*, Key Issues (Anm. 127), S. 100.
136 Ebda.; *Chaumette* (Anm. 18), S. 19.
137 *Schmitt,* Key Issues (Anm. 127), S. 100.

138 Authentisch „for such time“.
139 *Schmitt,* Key Issues (Anm. 127), S. 100.
140 *Chaumette* (Anm. 18), S. 21.
141 S. IStGH, *Prosecutor v. Katanga*, Entscheidung vom 8. März 2014, icc-01/04-01/07, Nr. 1119; vgl. *Ambos,* in: Tsagourias/Buchan, (Anm. 45), S. 142.
142 Vgl. statt vieler: *Chaumette* (Anm. 18), S. 22.
143 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 395.
144 *Kai Ambos* in: Otto Triffterer/Kai Ambos (Hrsg.) The Rome Statute of the International Criminal Court, 2016, Art. 25 IStGH-Statut, Rn. 11.
145 *Schmitt*, Tallinn Manual 2.0 (Anm. 23), S. 399; bezüglich der unvorhergesehenen Folgen bei Cyberoperationen s. oben Punkt B) II.) 2.) c) aa) (2) (b).
146 S. ICTR, *Prosecutor v. Akayesu*, Entscheidung vom 2. Oktober 1998, ictr-96-4-t, Nr. 556; vgl. Völkerrechtskommission (ILC) Bericht vom 26. Juli 1996, U.N.Doc.A/51/10; *Chaumette* (Anm. 18), S. 32.
147 *Chaumette* (Anm. 18), S. 33; s. ICTR, *Prosecutor v. Nahimana et al*., Entscheidung vom 28. November 2007, ictr-99-52-a, Nr. 692.

Staat, Recht und Politik – Forschungs- und Diskussionspapiere
State, Law, and Politics – Research and Discussion Papers

ISSN (online) 1867-9528
https://nbn-resolving.org/urn:nbn:de:kobv:517-series-914

Herausgegeben von apl. Prof. Dr. iur. Norman Weiß, Universität Potsdam.

Zuletzt erschienene Ausgaben:

Nr. 11 Wogene Berhanu Mena
Civilizational Hexagon as a pathway to Conflict Management : Examining its application in Sub-Saharan Africa in the Post-Cold War Era
2021 | https://doi.org/10.25932/publishup-51669

Nr. 10 Itzik Aharon, Antonia Brill, Philip Fonseca, Azin Alizadeh Vandchali, Nina Wendel
The Protection of Women Human Rights Defenders and their Collective Actions
2020 | https://doi.org/10.25932/publishup-44427

Nr. 9 Alina-Camille Berdefy
Auftrag und Möglichkeiten der Kommission für Friedenskonsolidierung im System der Vereinten Nationen
2019 | https://doi.org/10.25932/publishup-43947

Nr. 8 Steven Kleemann
The Forgotten War: Yemen
2019 | https://doi.org/10.25932/publishup-43071

Nr. 7 Anna Letsiou Häusler, Nicolas Beckenkamp, Livia Röthlisberger
New Dimensions of an Old Dilemma – Hate Speech and Freedom of Expression
2019 | https://doi.org/10.25932/publishup-42486

Nr. 6 Stephanie Verlaan
Male victims of wartime sexual violence: an ignored phenomenon – An analysis of implications
2018 | https://nbn-resolving.org/urn:nbn:de:kobv:517-opus4-412632