ETHIK UND MILITÄR

KONTROVERSEN
IN MILITÄRETHIK UND
SICHERHEITSPOLITIK

AUSGABE 01/2019

Konfliktzone Cyberspace: Perspektiven für Sicherheit und Frieden

SPECIAL

Der Cyberraum als Domäne militärischen Handelns

zebis

KONFLIKTZONE CYBERSPACE: PERSPEKTIVEN FÜR SICHERHEIT UND FRIEDEN

SPECIAL: DER CYBERRAUM ALS DOMÄNE MILITÄRISCHEN HANDELNS

Editorial
Veronika Bock Seite 03

Mehr Verantwortung im Cyberspace – aber wie?
Götz Neuneck Seite 04

„Cyberkrieg": Geschichte und Gegenwart eines umkämpften Begriffs
Philipp von Wussow Seite 11

Die Aussicht auf Frieden im Cyberspace
George R. Lucas Seite 18

Über Cyber, Krieg und Cyberkrieg
Eneken Tikk und Mika Kerttunen Seite 26

Riskante Kriegsspiele: Warum wir im Cyberwar nur verlieren können
Anke Domscheit-Berg Seite 32

Cybersicherheit und Cyberverteidigung – besserer Schutz durch behördliche Zusammenarbeit
Andreas Könen Seite 40

Der Organisationsbereich Cyber- und Informationsraum als wichtiger Teil einer gesamtstaatlichen Sicherheitsvorsorge
Generalleutnant Ludwig Leinhos Seite 46

„Es gibt heute keine militärische Operation, keinen militärischen Konflikt ohne Cyberdimension"
Interview mit Generalmajor José Luis Triguero de la Torre Seite 51

„Erste Erfolge in der Cyberdiplomatie sind bereits sichtbar"
Interview mit Kapitän zur See Matthias Friese Seite 54

Glossar Seite 57

Impressum/Alle Ausgaben Seite 59

EDITORIAL

„Sechs von zehn Internetnutzern haben Angst vor Cyberkriegen“, meldete der IT-Branchenverband Bitkom Anfang des Jahres 2019. Womöglich hat die Umfrage bei vielen eine Gefahr heraufbeschworen, über die sie sich vorher gar keine Gedanken gemacht haben. Dennoch bietet die Nachricht einige Ansatzpunkte zur Reflexion.

Was ist überhaupt ein Cyberkrieg, was stellen wir uns darunter vor? Und findet er jenseits faszinierender hollywoodesker Science-Fiction-Szenarien überhaupt statt? Angesichts aufsehenerregender Attacken und der alltäglichen kriminellen und infiltratorischen Aktivität im Cyberspace – so waren laut dem Bundesamt für Sicherheit in der Informationstechnik 2018 rund 800 Millionen Schadprogramme im Umlauf, 25 Prozent mehr als im Vorjahr – mögen diese Fragen provokativ erscheinen. Die Redaktion von „Ethik und Militär“ hat sich dennoch entschieden, die (um auch sprachlich im Bild zu bleiben) Reset-Taste zu drücken.

Der einführende Beitrag widmet sich der Entwicklung der Bedrohungslage. Bei aller zunehmenden Austragung zwischenstaatlicher Konflikte im Cyberraum mittels teils spektakulärer DDoS-Attacken, disruptiver Software und „Waffen“ wie dem berühmten Stuxnet-Wurm ist noch kein einheitliches Verständnis von zentralen Kategorien wie Krieg und Frieden in der Cybersphäre vorhanden. Umso wichtiger erscheint ein Austausch, eine Verständigung über wesentliche Konzepte und eine Orientierung an bereits existierenden Abrüstungsprozessen und -regimen, um die Eskalationsgefahr einzudämmen.

Im Folgenden untersuchen mehrere Autoren, inwiefern es überhaupt angemessen ist, von einem Krieg im Cyberspace zu sprechen. Dass es sich dabei nicht um eine abstrakte definitorische Problemstellung handelt, wird schnell klar. Versuche, die Cyberdomäne mit einer völkerrechtlichen Herangehensweise zu befrieden, waren offensichtlich bisher nur eingeschränkt tauglich. Warum ist es trotzdem noch nicht zu einer Eskalation gekommen? Warum sollten wir uns dennoch mit den realen politischen Risiken der Entwicklung befassen?

Die Frage, ob unsere Unterscheidung zwischen innerer und äußerer Sicherheit in einem „umkämpften Raum“ wie dem Cyberspace noch anwendbar ist, rückt so ebenfalls in den Vordergrund. Wie kann beziehungsweise muss der Staat die Domäne des Internets regulieren, um Sicherheit zu gewährleisten? Eine Netzaktivistin und Vertreterin der Opposition im Bundestag sowie ein Verantwortlicher des Bundesinnenministeriums stellen ihre Standpunkte dar.

Die zunehmende Digitalisierung von Kommunikations- und Waffentechnik sowie die Furcht vor Cyberattacken, beispielsweise gegen kritische Infrastrukturen, haben dazu geführt, dass sich das Militär überall auf der Welt – in Deutschland mit dem Aufbau des Kommandos Cyber- und Informationsraum – darauf vorbereitet, in der digitalen Sphäre zu operieren. Aus den Beiträgen hochrangiger Vertreter von Bundeswehr und NATO im Special dieser Ausgabe wird deutlich, wie sie Bedrohungen einschätzen und mit welchen Strategien sie darauf reagieren.

Die Redaktion bedankt sich wie immer herzlich bei allen, die ihren Anteil an der Fertigstellung dieser Ausgabe von „Ethik und Militär“ haben. Angesichts der facettenreichen Diskussion haben wir im Gesamttitel dieser Ausgabe bewusst auf den Begriff „Cyberwar“ verzichtet. Wir sind der Ansicht, dass es für Sie, liebe Leserinnen und Leser, solcher Reizwörter nicht bedarf, um über die vielfältigen ethischen und sicherheitspolitischen Implikationen der digitalisierten Konfliktaustragung nachzudenken.

Dr. Veronika Bock
Direktorin des zebis

MEHR VERANTWORTUNG FÜR DEN CYBERSPACE – ABER WIE?

Abstract

Die Rezepte und Mechanismen des etablierten internationalen Rüstungskontrollrechts lassen sich kaum auf die augenblicklichen Militarisierungstendenzen im Cyberspace eins zu eins übertragen, meint der Autor des hier abgedruckten Beitrages. Dass jedoch die Erfahrungen aus dem Entwicklungsprozess der internationalen Rüstungskontrolle inspirierend für die Schaffung vertrauensbildender Maßnahmen im Cyberspace sein können, zeigt Götz Neuneck als ein führender deutscher Experte für Rüstungskontrollpolitik glaubwürdig auf.

Nicht nur die immer tiefer gehende Vernetzung verursacht eine steigende Verwundbarkeit und Bedrohung der internationalen Sicherheit. Auch diverse Maßnahmen zur Cybersicherheit, die eigentlich diesen Phänomenen Rechnung tragen sollen, beinhalten immer aggressivere Operationsmöglichkeiten im Cyberspace und bergen eine enorme Eskalationsgefahr.

Zwar ist der Begriff „Cyberwar" nicht hinreichend definiert, sodass jeder internationale Akteur etwas anderes darunter verstehen mag. Gerade daraus jedoch ergibt sich eine immense Unsicherheit, da die Staaten in ihren jeweiligen Militärdoktrinen unterschiedliche Kriterien setzen, nach welchen Cyberattacken die Kriegsschwelle überschritten sei. So bezeichneten die USA nordkoreanische Hackeraktivitäten in Vergangenheit bereits als „kriegerische Handlungen". Zeitgleich scheint es Neuneck zufolge, als schreite durch die sich verschärfende Staatenkonkurrenz auch die Militarisierung des Cyberspace unaufhaltsam voran.

Gibt es also überhaupt Möglichkeiten für eine Friedenskonsolidierung im Cyberspace? An Initiativen hierfür – national wie international – mangelt es nicht, und auch positive Beispiele für zwischenstaatliche Entspannungspolitik im Cyberspace existieren bereits. Letztlich gilt es aber auch dort, verantwortungsvolles Handeln vom Ende her zu denken. Dazu müsse eine konsensfähige Vorstellung her, was bei allen Vorstellungen von Cyberkrieg eigentlich einen Cyberfrieden ausmache.

Autor: ***Götz Neuneck***

Der öffentliche und internationale Diskurs über Sicherheit und Frieden im Cyberraum und die künftigen Gefahren katastrophaler Cyberkonflikte haben sich in den letzten Jahren verschärft und zugespitzt. Einerseits wird insbesondere vom Westen der Erhalt eines „offenen, sicheren und friedlichen" Cyberspace vertreten, andererseits treffen Staaten nicht nur Vorbereitungen für eine effektive Cyberverteidigung, sondern sie sind schon seit Längerem aktiv in Form von nachrichtlichen Operationen im Cyberraum tätig. Das Risiko von Cyberangriffen mit fatalen Folgen steigt, da die moderne Welt immer stärker vernetzt und „computerisiert" wird. Diese Entwicklung wird sich mit der forcierten Digitalisierung weiter fortsetzen. Stichworte sind hier das „Internet of Things" (IoT) und das „Advanced Manufacturing" (zum Beispiel mithilfe von 3-D-Druckern), aber auch die Debatte um künstliche Intelligenz.

Zudem werden zunehmend aggressive Formen von Cyberoperationen wie Hack-back, Cyberoffensiven et cetera diskutiert, vorbereitet und teilweise sogar schon durchgeführt.[1] Rund 30 Staaten sollen laut der letzten Bedrohungsanalyse der USA über offensive Cyberfähigkeiten verfügen, also das Vermögen, in die Computer anderer Staaten einzudringen, sensible Informationen zu stehlen, zu manipulieren oder automatisierte Prozesse zu unterbrechen. Die USA selbst sind hier technologisch ein wesentlicher Trendsetter.

Auch Organisationen wie die NATO, die OSZE und die Europäische Union haben die Cybersicherheit zu einer neuen Aufgabe erhoben. Maßnahmen zur Vertrauensbildung werden ebenso diskutiert wie offensive Strategien, Abschreckung oder Rüstungskontrollvorschläge.

Die Bundeswehr legt sich eine Teilstreitkraft zur „Cyberverteidigung" mit insgesamt 13 500 Dienstposten im neu gegründeten Kommando Cyber- und Informationsraum zu. Zum einen soll sowohl im Inland als auch im Einsatzland im Rahmen einer nationalen Gefahrenabwehr der Einsatz, Schutz und Betrieb des IT-Systems der Bundeswehr zusammengeführt und gestärkt werden. Zum anderen sollen die Fähigkeiten zur Aufklärung und Wirkung im

Cyber- und Informationsraum verbessert und weiterentwickelt werden.

Was bedeutet das nun aber in einer zunehmend vernetzten und von digitalen Technologien bestimmten Welt? In welchem internationalen Umfeld findet diese Entwicklung statt, und welche Beschränkungsmaßnahmen können national, EU-weit oder international ergriffen werden? Angesichts des schnellen technologischen und sicherheitspolitischen Wandels gibt es darauf keine einfachen Antworten. Die Schaffung von Institutionen wie dem Cyber-Abwehrzentrum oder einer schnellen Eingreiftruppe seitens des BSI beantwortet diese Fragen allein nicht. Wenn Soldaten auch „im Cyberraum operieren" sollen, müssen klare Definitionen, Maßstäbe und Verhaltensregeln geschaffen werden, um die Verpflichtungen des internationalen Völkerrechts einzuhalten und ein digitales Wettrüsten zu verhindern. Darüber hinaus müssen Staaten geeignete Normen und Prinzipien festlegen, damit zum Beispiel das Internet nicht weiter militarisiert wird. Umso mehr kommt der Außen- und Friedenspolitik die Aufgabe zu, sich um eine konsistente Strategie für die Gefahrenvorsorge, eine sinnvolle Ressourcenverteilung und belastbare Defensivkonzepte zu kümmern. Auch international müssen die EU und Deutschland sich angesichts eines verschärften Wettbewerbs zwischen den USA, China und Russland stärker positionieren.

Grundlegendes zu Konflikten im Cyberraum

Heute werden die zeitlichen und räumlichen Grenzen von Kriegen aufgeweicht. Das Internet selbst kennt keine territorialen Grenzen. Geheime Operationen, hybride Kriegführung oder Propagandakriege sind übliche Schlagworte in diesem Kontext. Treffend stellt die ressortübergreifende „Cyber-Sicherheitsstrategie für Deutschland 2016" dazu unter anderem fest: „Innere und äußere Sicherheit im Cyberraum sind nicht mehr trennscharf voneinander abzugrenzen."[2] Diese Erkenntnis ist weder neu noch besonders zielführend. Sie stellt aber neue Fragen an die Zuständigkeit, Verantwortungsbereiche und mögliche Effizienzmaßnahmen der beteiligten Ressorts (Bundesinnen- und Verteidigungsministerium und Auswärtiges Amt). Eine einfache Antwort gibt es darauf sicher nicht, denn viele Faktoren in der „schönen neuen" Cyberwelt bleiben vage. Dies beginnt bei der Einschätzung der Bedrohungslage und reicht über Definitionsfragen bis hin zur effektiven und personell kompetenten Vorbereitung geeigneter und wirkungsvoller aktiver und passiver Gegenmaßnahmen. Dabei steht auch die internationale Debatte vor mehreren kaum zu umgehenden Hindernissen.

Wenn Soldaten auch „im Cyberraum operieren" sollen, müssen klare Definitionen, Maßstäbe und Verhaltensregeln geschaffen werden

Cyberwar ist ein Begriff, der oft verwendet wird, aber kaum eindeutig bestimmbar ist. Eine international akzeptierte Definition existiert bisher nicht. Das aktuelle Einsatzspektrum von Cyberangriffen ist breit und fluid.[3] Es reicht von DDoS-Angriffen, Datendiebstahl, Aufklärung und Spionage über Sabotage (Stuxnet) bis hin zu potenziell aktiven Kriegshandlungen.

Militär und Nachrichtendienste überwinden technische Barrieren und dringen bereits heute in die Computersysteme anderer Staaten ein. Die Gründe sind vielfältig: Sie können psychologischer Natur sein oder der Vorbereitung weiterer Angriffshandlungen *(„preparing the battlefield")* dienen, aber auch die Schwächung eines Opponenten zum Ziel haben. Ziele solcher Angriffe sind nicht nur militärische Einrichtungen, sondern auch industrielle Anlagen (Ölproduktion, Energieversorgung, Finanzsystem), also im weitesten Sinne zivile kritische Infrastrukturen. Dabei können die Motivationen und Fähigkeiten der Akteure sehr unterschiedlich sein. Entscheidend ist, dass die heutige Software- und auch Hardwareentwicklung viele Verwundbarkeiten offenlässt und die Überwindung von Sicherheitsbarrieren möglich macht.

Cyberangriffe können Teil einer umfassenden Operation sein und auch eine militärische Komponente beinhalten. So bombardierte Israel ei-

nen noch nicht betriebsbereiten Nuklearreaktor in Syrien, nachdem die Luftabwehr, das heißt Radar und Abwehrraketen, elektronisch ausgeschaltet worden war. 2007 wurden estnische Regierungs-, Banken- und Medienseiten blockiert; zu dem Angriff bekannte sich später eine kremltreue russische Jugendorganisation. 2008 führte wahrscheinlich Russland koordinierte Cyberoperationen und konventionelle Angriffe gegen Georgien aus. Präsident Obama gab 2016 bekannt, dass Cyberoperationen bei der Offensive gegen den IS genutzt wurden. Weitere Beispiele lassen sich finden. Nicht nur der Stuxnet-Wurm, der gegen die iranischen Zentrifugen eingesetzt wurde, zeigt die Charakteristika einer Cyberwaffe. Dazu gehört ein Träger mit einer „Nutzlast", die modular aufgebaut gegen unterschiedliche Ziele eingesetzt werden kann. Auch die Wirkungen von solcher disruptiven Malware sind schwer einzuschätzen. Die Malware NotPetya wurde durch eine russische Hackergruppe gegen die Ukraine eingesetzt, traf aber wohl unbeabsichtigt auch die Spedition Maersk, deren Betrieb kurzzeitig eingestellt werden musste. Weitere Bespiele sind die Erpressungssoftware WannaCry und Bad Rabbit. Diese Aktionen richten erheblichen ökonomischen oder psychologischen Schaden an, gelten aber nicht als unmittelbare Kriegshandlung.

Bei Cyberangriffen wird letztlich jeder Staat für sich entscheiden, ob eine kriegerische Handlung vorliegt oder nicht

Heute treten aber auch vermehrt Cyberangriffe in aktuellen Konfliktkonstellationen auf: So gelang es 2016 wahrscheinlich russischen Hackern, eine Hochspannungsanlage nahe Kiew auszuschalten (Operation Crash Override). Die Angriffe gegen Sony Pictures im Jahr 2014 wurden von der Obama-Administration als „kriegerische Handlungen" Nordkoreas eingeschätzt, aber militärische Aktionen blieben aus. Typische Gegenreaktionen sind bis heute öffentliche Anklagen, Sanktionen oder das Ausweisen von Diplomaten, nicht jedoch aktive „kinetische" Kriegshandlungen. Daran wird aber auch deutlich, dass letztlich jeder Staat für sich entscheiden wird, ob eine kriegerische Handlung vorliegt oder nicht.

Weiterführend wäre es, wenn der UN-Sicherheitsrat hier eine klare Regelung basierend auf den Prinzipien des humanitären Völkerrechts erarbeiten würde. Bisher ist der Cyberraum eine Domäne asymmetrischer politischer Kriegführung, verbunden mit einer Diplomatie von Zwangsmaßnahmen (also beispielsweise Sanktionen oder Embargos). Auch finden im Internet viele geheime Operationen statt, die eskalieren können, aber die bisher nicht eine klassische Kriegsschwelle erreicht haben. Dies kann sich jedoch in Zukunft ändern. Festzuhalten ist zudem, dass Cyberwaffen proliferieren oder von anderen Staaten gestohlen (Beispiel Eternal Blue) werden können.

„Militarisierung des Cyberraums" durch Staatenkonkurrenz?

Das Worldwide Threat Assessment der US-Regierung setzt „Cyberbedrohungen" auf Seite eins der globalen Bedrohungen und nennt als Akteure Russland, China, Nordkorea, Terroristen und Kriminelle. Weiter formuliert die US-Analyse: „Viele Länder betrachten Cyberfähigkeiten als ein geeignetes Instrument zur Projektion ihres Einflusses und werden die Cyberfähigkeiten weiterentwickeln."[4] Cyberoperationen gegen das nordkoreanische Raketenprogramm im Sommer 2017 unterstreichen den Anspruch und die Bereitschaft der USA, im Cyberspace militärisch aktiv zu werden – auch wenn die Maßnahmen in diesem Fall nicht zu dem gewünschten Ergebnis geführt haben. Zu einer Eskalation ist es bisher nicht gekommen, und auch die Wirkung war eher begrenzt. Das muss aber nicht immer so bleiben. Ein künftiger Krieg, verbunden mit massiven Cyberangriffen, liegt im Bereich des Möglichen.

Die strategischen Dokumente der Trump-Administration haben den „Machtwettbewerb zwischen den USA, Russland und China" als Paradigma für das 21. Jahrhundert ausgerufen, und dementsprechend spricht die Cy-

berpolitik der USA eine aggressivere Sprache als noch unter Obama. Sie wird unterstützt durch die Interviews des Sicherheitsberaters John Bolton und die Sprache des Vision Statement des U. S. Cyber Command mit dem Titel „Achieve and Maintain Cyberspace Superiority“.[5] Darin wird zu „persistenten Aktionen“ aufgerufen, um die „Cyberüberlegenheit der USA“ zu bewahren. Offensive präventive Aktionen werden damit also zum Normalfall erklärt. Dies findet sich vor dem Hintergrund des wiederauflebenden Wettbewerbs wieder in der National Defense Strategy (2018) und der National Security Strategy (2017). Laut der gemeinsamen Publikation „Cyberspace Operations“ der US-Stabschefs vom 8. Juni 2018 zielen offensive Cyberoperationen darauf ab, „Macht in und durch den ausländischen Cyberraum zu projizieren“.[6] In der neuen Cyber Strategy 2018 und der Cyber Posture Review wird als zentrales Thema unter anderem „die Nutzung des Cyberraums zur Stärkung der militärischen Letalität und Effektivität“[7] angegeben. Eine Studie des CATO-Instituts folgert daraus: „Der Cyberraum wird eine Domäne für Soldaten, nicht nur ein Netzwerk für Spione.“[8]

Russland benutzt statt des Präfix „Cyber“ den Begriff „Information“ und hat selbst 2016 eine Doktrin für „Information Security“ vorgestellt.[9] Zum einen fürchtet man besonders die „Destabilisierung“ seitens fremder Staaten durch „Informations- und psychologischen Einfluss“. Zum anderen bezieht hier der Begriff „Informationssphäre“ viel stärker den Inhalt der Information selbst ein, die im Internet verbreitet wird. Damit werden im Verbotsfall die Möglichkeiten verstärkter Zensur im Land geschaffen. Zusätzlich möchte Russland eine eigene, gut kontrollierbare Version des Internets aufbauen. Es kann als sicher gelten, dass eine neue Cyberdoktrin als Reaktion auf die aktuelle US-Doktrin ebenfalls aggressivere Elemente beinhalten wird. Nicht zuletzt wird Russland von den USA massiv verdächtigt, mit Cyberoperationen in die US-Präsidentschaftswahlen 2016 eingegriffen zu haben.

Auch China verwendet nicht den Cyberbegriff, sondern spricht stets von „Informationsbedrohungen“. Das Land führt seit Jahrzehnten Cyberspionage-Operationen insbesondere gegen die USA durch.[10] Ein Element ist der Diebstahl von geheimen militärischen Informationen, aber auch von solchen aus der Wirtschaft (Patente et cetera). Beim Treffen der Präsidenten Obama und Xi Jinping 2015 vereinbarte man eine Art Stillhalteabkommen. In der Tat gingen die chinesischen Angriffe zurück. Dies zeigt, dass bilaterale Abkommen durchaus Wirkung zeigen können. Die digitale Aufrüstung der Zukunft verhindern können sie jedoch kaum, zumal diverse andere Staaten sich auf defensive und offensive Operationen im Cyberraum vorbereiten.

Mögliche friedenskonsolidierende Maßnahmen für den Cyberraum – national und international

Die internationale Gemeinschaft diskutiert, insbesondere seit den Stuxnet-Fällen 2010, internationale Aktionen, Regeln und Instrumente, um ein ausuferndes digitales Wettrüsten zu verhindern und eine schrittweise Militarisierung des Internets zu dämpfen. Hierbei stellen sich viele neue Fragen: Ist sichergestellt, dass Cyberoperationen nicht zu einer realen Eskalation und sogar zu kriegerischen Handlungen führen werden? Wie können die verschiedenen Akteure, das heißt Staaten, Industrie und Zivilgesellschaft, zusammenarbeiten, damit ein „einheitliches, sicheres und friedliches“ Internet erhalten bleibt? Können angesichts der Unübersichtlichkeit, Größe und der Gesetze des Cyberraums Prinzipien und Regeln effizient und überprüfbar aufgestellt werden, um katastrophale Cyberaktionen zu verhindern? Im Gegensatz zum klassischen Rüstungskontrollacquis ist der Cyberraum für jedermann offen, schnell wachsend, sich technologisch schnell verändernd und wird zudem hauptsächlich von privatwirtschaftlichen Akteuren betrieben. Die

Die Einbeziehung von Zivilgesellschaft, Wirtschaft und Industrie ist bei künftigen Regelungen für den Cyberraum unbedingt notwendig

Einbeziehung von Zivilgesellschaft, Wirtschaft und Industrie ist bei künftigen Regelungen also unbedingt notwendig.

Im Cyberraum gilt: „Die beste Defensive ist eine gute Defensive."[11] In den letzten zehn Jahren wurden auf verschiedenen Ebenen erhebliche Bemühungen unternommen, um international gemeinsame Regeln aufzustellen und zu implementieren. Im Rahmen der *Tallinn Manuals* (Vol. I und Vol. II) wurden im NATO-Kontext völkerrechtliche Regeln erarbeitet, die in Bezug auf die Anwendbarkeit des Völkerrechts viele rechtliche Fragen angesprochen haben. Zunächst sind auf nationaler Ebene Regierungen im Rahmen der Katastrophen- und Kriegsvorsorge herausgefordert, ihre eigenen digitalen Strukturen zu schützen oder resilient auszugestalten. Dazu gehören die Steigerung der Awareness bei den Nutzern, eine gute Frühwarnung und Verwundbarkeitsanalyse, ein „Attribution Scanning" sowie resilientere Netzstrukturen. Auch die Rüstungsexportkontrolle muss einbezogen werden, denn nur so kann verhindert werden, dass gefährliche Malware in die Hand von feindlichen Staaten gelangt.[12]

Stärkerer Schutz und Zurückhaltung bei offensiven Aktionen wären wesentliche Voraussetzungen für den Erhalt des frei zugänglichen Cyberraums

Zudem müssen Entscheidungsträger die nötige technologische Expertise haben, um in Krisen die richtigen Urteile zu fällen. Da Cybersicherheit im Friedens- und Kriegsfall eine ressortübergreifende Aufgabe ist, sollten ein verstärkter personeller Austausch zwischen den Bundesbehörden und abgestimmte Fortbildungsmaßnahmen die „ressortübergreifende Resilienz" stärken. Ebenso braucht es zwingend ein besseres Verständnis neuer technologischer Entwicklungen wie künstlicher Intelligenz. Eine enge Zusammenarbeit der Behörden mit Industrie und Wissenschaft ist hier unabdingbar. Eine standardmäßige „Ende-zu-Ende-Verschlüsselung" für die Kommunikation wäre ein wichtiger Schritt.

Stärkerer Schutz und Zurückhaltung bei offensiven Aktionen wären wesentliche Voraussetzungen für den Erhalt des frei zugänglichen Cyberraums. Analysen zeigen, dass diese Ziele von der jeweiligen Sicherheitspolitik der Staaten abhängig sind. Der aggressivere Wettbewerb zwischen den USA, China und Russland fordert von der Europäischen Union eine klare Positionierung. Mittelmächte wie Australien, Deutschland oder Kanada hätten hier die Aufgabe, entsprechende Cyberregeln für eine „friedliche und stabile Cybersphäre" gegenüber Staaten wie USA, Russland oder China voranzutreiben. International sind sowohl auf UN-Ebene (UN Group of Governmental Experts) als auch bei regionalen Organisationen wie der OSZE und ASEAN in Arbeitsgruppen wichtige Schlussfolgerungen und konkrete Vorschläge für vertrauensbildende Maßnahmen im Cyberraum erarbeitet worden. Diese beinhalten zum Beispiel gegenseitige Informationspflichten bei Cyberangriffen beziehungsweise bei der Aufstellung von Cyberdoktrinen oder das Verbot von Angriffen auf kritische Infrastrukturen.[13] In erster Linie mangelt es aber bisher an der Bereitschaft führender Staaten, diese Vorschläge auch aufzugreifen, glaubwürdig zu implementieren oder im internationalen Diskurs weiterzuentwickeln. Echte Transparenz in Bezug auf offensive Operationspotenziale, Cyberdoktrinen und die Funktion damit befasster Institutionen wäre ein Schritt vorwärts. Voraussetzung dafür ist dabei das gemeinsame Verständnis zentraler Begriffe wie Cyberangriff oder Cyberwaffe sowie deren Schadensdimension. Dies ist jedoch nur schwach ausgebildet und damit für jegliche Interpretation und künftige Anwendung offen. Staaten müssen hier eine gemeinsame Grundlage entwickeln. Ein von der UN gesponsertes

Der Autor

Götz Neuneck *ist Physiker und promovierte an der Universität Hamburg im Fachbereich Mathematik zum Dr. rer. nat. Von 1984 bis 1987 arbeitete er über Strategiefragen, Militärtechnologien und Rüstungskontrolle bei der Arbeitsgruppe Afheldt in der Max Planck Gesellschaft in Starnberg. Er ist stellvertretender Wissenschaftlicher Direktor des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH) und Leiter der Forschungsgruppe Rüstungskontrolle und neue Technologien. Er ist Vorsitzender der Arbeitsgruppe Physik und Abrüstung der DPG sowie Mitglied des Council der Pugwash Conferences on Science and World Affairs.*

gemeinsames Glossar als erster Schritt wäre hier hilfreich.

Das Problem der Attribution im Cyberraum erscheint kaum lösbar, dennoch müssen forensische Standards und Einrichtungen entwickelt werden, die mögliche Untersuchungen von Cyberzwischenfällen vornehmen können.[14] Aus den Transparenz- und Verifikationsregeln der etablierten Rüstungskontrolle (zum Beispiel Internationale Atomenergiebehörde, Organisation für das Verbot chemischer Waffen, Organisation des Vertrags über das umfassende Verbot von Kernwaffen) kann hier einiges gelernt werden.

Soldaten müssen dazu ausgebildet werden, im Einsatz die Prinzipien des humanitären Völkerrechts (vor allem Verhältnismäßigkeit, Diskriminierungsgebot, militärische Notwendigkeit) auch bei Konflikten im Cyberraum anwenden zu können. Gemeinsame Übungen mit befreundeten Staaten können helfen, Erfahrungen zu sammeln und Krisen im Verbund zu bewältigen.

Firmen wie Microsoft („Digital Geneva Convention") oder Siemens („Charter of Trust") haben eigene Vorschläge und Prinzipien ausgearbeitet, die das Verhalten von Firmen und Einzelnutzern für ein „stabiles und friedliches" Internet positiv gestalten sollen. Die Non-Profit-Organisation Access Now setzt sich für den Schutz der digitalen Rechte der Nutzer weltweit ein und bietet Hilfe an, wenn Nutzer angegriffen oder ausspioniert werden. Der von Präsident Macron initiierte „Paris Call für Vertrauen und Sicherheit im Cyberraum" hat viele Unterstützer gefunden und setzt sich für die Einhaltung fundamentaler Prinzipien in dieser Sphäre ein.[15] Dies trägt sicher zur Bewusstseins- und Verantwortungsbildung der wichtigen Nutzerkreise bei, wird aber kaum entscheidend helfen, problematische staatliche Akteure bei den Nachrichtendiensten oder dem Militär mancher Länder zu erreichen.

Mittelfristig sind Transparenz- und Rüstungskontrollregelungen notwendig, wenn es zu nachweislichen Kriegshandlungen unter Nutzung von disruptiven Cybertools kommen kann. Eine unmittelbare Übertragbarkeit der heutigen Rüstungskontrollarchitektur auf das Verbot von Cyberwaffen erscheint kaum möglich, da der Cyberraum nur extrem schwer zu kontrollieren ist, Cyberwaffen immateriell sind und unterschiedliche Schadenswirkungen haben.[16] Dennoch ist der Erhalt eines „offenen, friedlichen, frei zugänglichen, stabilen und sicheren" Cyberraums ein Ziel, das im Interesse der Staatenwelt liegt. In Bezug auf die Begrenzungen gefährlicher Angriffsvektoren, die Vermeidung von katastrophalen Schadenswirkungen und nicht zu kontrollierenden Eskalationspotenzialen kann man von dem jahrzehntelangen Entwicklungsprozess vertragsgebundener Rüstungskontrollregelungen einiges lernen.

Längerfristig stellt sich auch die Frage, was man unter einem dauerhaften Cyberfrieden verstehen kann, den ja viele Akteure immer wieder fordern. Scott J. Shackelford schreibt dazu: „Cyberfrieden ist nicht das Fehlen von Angriffen oder Ausnutzung, eine Idee, die man als negativen Cyberfrieden bezeichnen könnte. Vielmehr handelt es sich um ein Netzwerk von mehrstufigen Regimen, die zusammenarbeiten, um die globale, gerechte und nachhaltige Cybersicherheit zu fördern, indem sie Normen für Unternehmen und Länder klären, die dazu beitragen, das Risiko von Konflikten, Kriminalität und Spionage im Cyberspace auf ein Niveau zu senken, das mit anderen geschäftlichen und nationalen Sicherheitsrisiken vergleichbar ist."[17] Interessanterweise fehlt bei dieser hilfreichen Definition noch der Begriff des Krieges. Es bleibt also noch einige Arbeit zu tun.

Aus den Transparenz- und Verifikationsregeln der internationalen Rüstungskontrolle kann einiges gelernt werden

Ich danke Jantje Silomon, Oxford und Hamburg, für vertiefende Kommentare und Quellen.

1 Siehe z. B. den „Active Cyber Defense Certainty Act" des US-Kongresses, eingebracht im März von Tom Graves mit einer Ergänzung. https://www.congress.gov/bill/115th-congress/house-bill/4036 (Stand: 26.4.2019).
2 Bundesministerium des Innern (2016): *Cyber-Sicherheitsstrategie für Deutschland 2016.* Berlin, S. 5. https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Stand: 26.4.2019).
3 Zwischen 2000 und 2016 gab es nach Auswertung einer Analyse des CATO-Instituts 272 dokumentierte Cyberoperationen, von denen 32,7 % disruptiv waren, 54,4 % der Spionage zuzurechnen sind und 12,89 % der Zersetzung dienten. Siehe Maness, Ryan C./Valeriano, Brandon/Jensen, Benjamin (2017): „The Dyadic Cyber Incident Dataset, Version 1.1.".
4 Coats, Daniel R. (2017): „Worldwide Threat Assessment of the US Intelligence Community", Senate Select Committee on Intelligence, 11. Mai 2017, S. 1. https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf (Stand: 26.4.2019).
5 U. S. Cyber Command (2018): „Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command", April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 (Stand: 26.4.2019).
6 U. S. Joint Chiefs of Staff (2018): „Cyberspace Operations", Joint Publication 3-12, 8. Juni 2018, S. II-5. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf [Stand: 26.4.2019].
7 U. S. Department of Defense (2018): „Fact Sheet: 2018 DoD Cyber Strategy and Cyber Posture Review. Sharpening our Competitive Edge in Cyberspace". https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf (Stand: 26.4.2019).
8 Valeriano, Brandon/Jensen, Benjamin (2019): „The Myth of the Cyber Offense. The Case for Restraint", CATO Institute, Policy Analysis Nr. 862, 15. Januar 2019, S. 4. https://object.cato.org/sites/cato.org/files/pubs/pdf/pa862.pdf (Stand: 26.4.2019).
9 „Information Security Doctrine of the Russian Federation". https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (Stand: 26.4.2019).
10 Inkster, Nigel (2013): „Chinese Intelligence in the Cyber Age". In: *Survival* 55 (1), Februar/März 2013, S. 45–65.
11 Valeriano, Brandon/Jensen, Benjamin (2019): „The Myth of the Cyber Offense. The Case for Restraint", CATO Institute, Policy Analysis Nr. 862, 15. Januar 2019, S. 10. https://object.cato.org/sites/cato.org/files/pubs/pdf/pa862.pdf (Stand: 26.4.2019).
12 Granick, Jennifer (2014): „Changes to Export Control Arrangement Apply to Computer Exploits and More", The Center for Internet and Society, 15. Januar 2014. https://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more (Stand: 24.4.2019).
13 Siehe dazu Neuneck, Götz (2014): „Cyberwarfare – Hype oder Bedrohung?". In: *Ethik und Militär* 2014/2, S. 26–31. http://www.ethikundmilitaer.de/de/themenueberblick/20142-cyberwar/neuneck-cyberwarfare-hype-oder-bedrohung/ bzw. die gesamte Schwerpunktausgabe zum Thema „Cyberwar".
14 Von der NGO ICT4Peace wurde eine Netzwerkorganisation für eine „staatenlose Attribution" vorgeschlagen. Siehe: „Trust and Attribution in Cyberspace: An ICT4Peace proposal for an independent network of organisations engaging in attribution peer review", 6. Dezember 2018. https://ict4peace.org/activities/trust-and-attribution-in-cyberspace-an-ict4peace-proposal-for-an-independent-network-of-organisations-engaging-in-attribution-peer-review/ (Stand: 26.4.2019).
15 https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (Stand: 26.4.2019).
16 Siehe dazu zum Beispiel Tikk, Eneken (2017): „Cyber: Arms Control without Arms?". In: Koivula, Tommi/Simonen, Katariina (Hg.): *Arms Control in Europe: Regimes, Trends and Threats.* Helsinki, S. 151–187.
17 Shackelford, Scott J. (2014): *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyberpeace.* Cambridge, S. 365.

„CYBERKRIEG“: GESCHICHTE UND GEGENWART EINES UMKÄMPFTEN BEGRIFFS

Autor: ***Philipp von Wussow***

Ein weltweiter, katastrophaler Cyberkrieg hat trotz aller technischen Möglichkeiten bislang nicht stattgefunden und wird vermutlich in absehbarer Zeit nicht stattfinden – doch zugleich befinden wir uns mitten im Cyberkrieg, denn Angriffe im Internet sind geradezu ein fester Bestandteil des Alltags geworden. Wie hängt das zusammen, und welche Auswirkungen hat dieser paradoxe Befund auf unsere Vorstellungen von Krieg und Frieden? Schließlich: Ist es in dieser Situation eigentlich angebracht, von „Cyberkrieg“ zu sprechen? Und ist in dieser Situation das Militär überhaupt geeignet, Cybersicherheit zu gewährleisten?

Um sich zu vergewissern, ob die Bezeichnung „Cyberkrieg“ zutreffend ist, erscheint es ratsam, zunächst einmal die Geschichte des Begriffs und insbesondere der damit verbundenen Bedrohungsszenarien zu rekapitulieren. Von hier aus lässt sich die fragile strategische Situation besser verstehen, in der es trotz der Allgegenwart von Cyberangriffen keine realistische Aussicht auf große Cyberkriege gibt. Was sorgt für diese weitgehende Begrenzung des Cyberkriegs auf alltägliche Cyberangriffe? Diese Begrenzung wird in der einschlägigen Literatur gegenwärtig unter dem Aspekt der Normenbildung verhandelt – ein Sammelbegriff, unter dem sich so unterschiedliche Aspekte wie Diplomatie, strategische Abschreckung, ethische Begrenzungen und Haftungsfragen wiederfinden können.

Zwei Extrempositionen

Der Begriff „Cyberwar“ wurde 1993 von den Sicherheitsexperten John Arquilla und David Ronfeldt eingeführt, um „die Zukunft des Krieges“ im Zusammenhang mit der informationstechnischen Aufrüstung der Militärtechnologie und der daraus folgenden Neuorganisation der Kriegführung zu beschreiben.[1] Arquilla und Ronfeldt hatten dabei vor allem Terrorangriffe durch nicht staatliche Akteure im Sinn, wenngleich sie auch die zunehmende Integration von Cyberkomponenten in die militärische Gefahrenabwehr zu beschreiben suchten. Das Szenario des Cyberterrorismus ist kennzeichnend für eine erste Phase der Aufmerksam-

Abstract

Philipp von Wussow geht in seinem Artikel dem schillernden Begriff des „Cyberkriegs“ auf den Grund. Er identifiziert zwei Extrempositionen in der aktuellen Debatte – beide mit wenig Bezug zum tatsächlichen technischen Potenzial von Cyberangriffen, dagegen umso mehr zu Ängsten aus Zeiten des Kalten Kriegs. Laut der einen Seite drohen der Menschheit katastrophale Cyberkriegsszenarien bis hin zur Totalvernichtung („Cybergeddon“). Für die Vertreter der Gegenseite verbietet sich die Rede vom „Cyberkrieg“, weil dies vor allem einer militärisch-geheimdienstlichen Kontrolle des Internets Vorschub leiste und die Eskalationsgefahr erhöhe.

Der eigentliche Kern des Problems besteht dem Autor zufolge darin, dass die omnipräsente Cyberkriminalität und Cyberspionage „den permanenten Ausnahmezustand zum Normalzustand“ mache und mit der herkömmlichen Dichotomie von Krieg und Frieden nicht adäquat zu fassen sei. Dieser durch Hegemoniekämpfe und latente Bedrohung gekennzeichnete „Schwebezustand“ könne am besten mit dem Hobbes'schen Naturzustand – dem Kampf aller gegen alle – verglichen werden.

Zugleich lasse sich aber absehen, so von Wussow weiter, dass jener anarchische Status quo (dem Hobbes'schen Modell entsprechend) durch verschiedene Prozesse eingehegt werde, weil dies langfristig im Interesse der großen Akteure sei. Eine Normierung „von oben“, beispielsweise durch völkerrechtliche Instrumente, scheine hierfür allerdings weniger geeignet als eine Herausbildung von Verhaltensmaßstäben, die aus der Cyberpraxis selbst hervorgehen. Ebenso werde die Rechtsprechung zu Haftungsfragen oder das Setzen von Industriestandards eine große Rolle spielen.

Allein die Vielzahl der beteiligten Instanzen und die herrschende Arbeitsteilung zwischen Staat und Privatsektor widerlegt nach Auffassung des Autors die Rede von der „Militarisierung“ des Cyberspace. Genauso wenig solle man dem Militär angesichts der potenziellen Bedrohung durch einen möglichen Cyberangriff jegliche Befugnis bei der Cyberabwehr absprechen.

keit, die bis in die frühen 2000er-Jahre reicht. Sie wurde abgelöst durch eine zweite Phase, in der vor allem Staaten in den Fokus rückten. Die öffentliche Aufmerksamkeit erreichte um 2009/2010 ihren Höhepunkt, als mit den ersten staatlichen oder staatlich geförderten Cyberangriffen die Gefahren und Möglichkeiten der neuen Technologie erstmals großflächig demonstriert worden waren. Für einen Moment schienen „Cyberkriege" in der kollektiven Imagination westlicher Bevölkerungen die nächste große Bedrohung der Menschheit zu sein. Dabei wurden Vorstellungen aus der Zeit des Kalten Kriegs von einer bevorstehenden atomaren Auslöschung der Menschheit reaktiviert.

Selbst wenn sich die Problemlage seitdem in vieler Hinsicht verändert hat, sind in der Debatte über Cyberkriege immer noch viele Ideen und Begriffe der 1990er-Jahre im Umlauf. Das Fortleben von gescheiterten Ideen – etwa dem Szenario des Cyberterrorismus, bei dem ideologisch motivierte Hacker von ihrem PC aus eine Katastrophe in der realen Welt auslösen – ist dabei lediglich Anzeichen einer grundsätzlicheren strategischen Unklarheit. Das ideologische Feld ließe sich grob in zwei Lager einteilen, in denen jeweils die extremsten Elemente den Ton angeben, während sich die vielen moderaten Stimmen in der Polemik gegen die Extrempositionen verfangen. Diesen Positionen zufolge drohen entweder große Cyberkatastrophen von bisher ungeahntem Ausmaß, oder die Bedrohung durch Cyberkriege ist nur vorgeschoben, und es droht in Wirklichkeit eine Militarisierung des Internets.

Das ideologische Feld ließe sich grob in zwei Lager einteilen, in denen jeweils die extremsten Elemente den Ton angeben, während sich die vielen moderaten Stimmen in der Polemik gegen die Extrempositionen verfangen

Die Aussicht auf globale „Cyberkriege" hat neue Bedrohungsszenarien eröffnet, die an die Stelle früherer Szenarien zur atomaren Auslöschung der Menschheit treten. Folgt man solchen Beschreibungen, so droht die Vernichtung der Zivilisation durch Zerstörung kritischer Infrastrukturen. Cyberkriege haben damit latente Vorstellungen von einem drohenden Atomkrieg reaktiviert – die reale Möglichkeit einer Auslöschung der Menschheit – und die vakante Stelle in der kollektiven Imagination eingenommen. Die entsprechenden Schlüsselbegriffe sind „Cyber 9/11", „Cyber Pearl Harbor", „Cyber Armageddon" (kurz „Cybergeddon"), in Ausnahmefällen auch „Cyber Holocaust".

In diesem Szenario kämpfen Terrorgruppen, Hackergruppen, *script kiddies* und andere Staaten gegen westliche Staaten, und zwar vornehmlich, indem sie großflächig sogenannte kritische Infrastrukturen lahmlegen.

Kritische Infrastrukturen sind Bereiche, die die moderne Zivilisation am Laufen halten, insbesondere Energie- und Wasserversorgung, Transport, Gesundheit, Banking und Agrar. Es handelt sich in der Regel um nicht staatliche Bereiche, die aber dennoch von vitalem Interesse für den Staat sind und deren potenzieller Ausfall eine Bedrohung der Souveränität darstellt. Insbesondere Kraftwerke, Krankenhäuser und Verkehrswege (einschließlich Häfen und Flughäfen), aber auch Kommunikationsnetze müssen unbedingt geschützt werden, denn die Zerstörung oder Unterbrechung dieser Infrastruktur würde das zivile Leben lahmlegen und potenziell viele Opfer nach sich ziehen. Solche Einrichtungen sind mit zunehmender Digitalisierung und Vernetzung verletzlich für Cyberangriffe geworden. Befürchtet wird, dass Hacker Staudämme öffnen und damit eine Flutwelle auslösen könnten; ebenso könnten sie Züge entgleisen lassen (vorzugsweise mit giftigen Chemikalien beladene Güterzüge) oder selbstfahrende Autos kapern und zu Waffen umfunktionieren; und durch Angriffe auf Kraftwerke könnte die Energieversorgung in urbanen Ballungszentren (wenn nicht gar landesweit) unterbrochen werden. Begleitet würden diese Angriffe von einer temporären Störung der Kommunikationsnetzwerke. Vielleicht die äußerste, noch geradezu futuristisch anmutende Idee ist, es könnte die „Smart City" der nahen Zukunft von Hackern gekapert werden und das Leben ihrer Bewohner zur Hölle auf Erden gemacht werden.

Trotz der prinzipiellen Möglichkeit hat es bis dato keine solchen großflächigen Cyber-

angriffe auf kritische Infrastrukturen gegeben. Bekannte Ransomware-Attacken gegen Krankenhäuser (so der Angriff auf das Neusser Lukas-Krankenhaus und zwei weitere Krankenhäuser in Nordrhein-Westfalen im Februar 2016) und Stadtverwaltungen haben bei Weitem nicht das imaginierte Maß an zivilem Schaden und strategischer Bedrohung erreicht. Die großen Dystopien der Zerstörung kritischer Infrastrukturen durch Hacker sind Cyberkriegs-Folklore geblieben. Entscheidend ist dabei, dass solche großflächigen Angriffe auf kritische Infrastrukturen für staatliche Akteure keinerlei strategischen Nutzen besitzen, während nicht staatliche Akteure, die sich auch ohne strategischen Grund dazu verleitet sehen könnten, dazu nicht in der Lage sind. Die operationellen Anforderungen sind hierfür zu hoch geworden, zudem fehlt es an strategischer Plausibilität für solche Angriffe.[2] Erst durch die Einbettung in eine größere Kriegsstrategie würden sie strategisch plausibel, wären dann aber zugleich in ihrer Reichweite beschränkt. Vermutlich würde das temporäre Ausschalten von Infrastrukturen im Krieg – etwa um die Stromversorgung des Feindes zu unterbrechen – hier eher zu einer Verringerung an physischer Zerstörung führen, wie dies von Anfang an zu den Szenarien von Cyberkriegen gehörte.

In der medialen Reaktion auf diese Katastrophenszenarien wurden viele der Argumente erprobt, die bis heute in immer neuen Kombinationen gegen den Begriff des „Cyberkriegs" angeführt werden. Kritiker stören sich dabei nicht nur an sensationalistischen Wortkombinationen wie Cyber 9/11, Cyber Armageddon oder Cyber Pearl Harbor. Im Kern bestreiten sie, dass es so etwas wie Cyberkriege überhaupt gibt. Sie glauben, dass der Begriff „Cyberkrieg" lediglich ein ideologisches Konstrukt ist, mithilfe dessen Staaten sich neue Gegner und neue Befugnisse verschaffen. China und Russland, die beiden großen staatlichen Player im Kampf gegen die westliche Ordnung, würden lediglich Cyberspionage und/oder Cyberkriminalität betreiben, aber sie hätten kein Interesse an einem Cyberkrieg. Der Politikwissenschaftler Thomas Rid fasste den Vorbehalt 2012 in der Auskunft zusammen, statt eines Cyberkriegs gebe es lediglich verschiedene Versionen von Subversion, Spionage und Sabotage.[3]

Ein Stichwortgeber dieser Debatte war der Journalist Seymour Hersh, der in einem einflussreichen Artikel von 2010 den „Cyberkrieg" als einen Kampf zwischen ziviler und militärisch-geheimdienstlicher Nutzung und Kontrolle des Internets beschrieb, bei dem die Militärs und Geheimdienste immer mehr versuchen würden, das Internet zu übernehmen. Hersh zufolge verdanken sich die großen Ängste einer Verwirrung zwischen Cyberkrieg und Cyberspionage, die lediglich der Rüstungsindustrie dienen würde, während sie für Datenschützer entmutigend sei. Denn die Rede vom Cyberkrieg würde lediglich eine Rechtfertigung für staatliche Organe schaffen, die Bürger auszuspionieren. Stattdessen forderte Hersh – ebenso wie viele vor und nach ihm – einen stärkeren Gebrauch von Verschlüsselungstechniken, einschließlich der staatlich verordneten Pflicht zur Verschlüsselung: „Die Regierung würde sowohl Unternehmen wie auch Privatleute verpflichten, die jeweils aktuellste Sicherheitssoftware zu installieren."[4] Einzig die Militärs und Geheimdienstler würden eine solche Lösung verhindern, da sie ihre Fähigkeit zum Abhören von Signalen beschränken würde.

Die großen Dystopien der Zerstörung kritischer Infrastrukturen durch Hacker sind Cyberkriegs-Folklore geblieben

Eine verwirrende Auskunft stammt vom US-amerikanischen Cybersicherheitsexperten Amit Yoran, der einerseits „ernste Konsequenzen" geltend macht, „wenn wir die Cybersicherheitskrise als Cyberkrieg bezeichnen. Die Konnotation des Kriegs oder das Etikett des Cyberkriegs verleiten uns dazu, die Rolle des Militärs und der Geheimdienste stärker hervorzuheben." Andererseits glaubt auch er: „Letztlich kommt es nicht darauf an, wie man Cyberkrieg definiert oder ob man glaubt, sich aktuell im Cyberkrieg zu befinden oder nicht."[5] Es bräuchte nicht eigens erwähnt zu

werden, dass die beiden Positionen („ernste Konsequenzen"/„es kommt nicht darauf an" gänzlich unvereinbar sind. Doch der Widerspruch registriert eine verbreitete Unsicherheit in Bezug auf das Verhältnis von Sprache und Gegenstand. Yoran versteht den Ausdruck einerseits als „Etikett" und scheint damit zu suggerieren, dass die sprachliche Bezeichnung bereits einen Akt des Kriegs darzustellen vermag – so als würde der Krieg im Akt der Bezeichnung erst erschaffen, anstatt dass die Bezeichnung auf einen kriegsähnlichen Zustand reagiert. Im zweiten Zitat stellt sich dagegen der gesunde Menschenverstand wieder ein, für den es tatsächlich nicht so sehr auf die genaue Bezeichnung, sondern primär ums Handeln geht. Am Ende versucht Yoran jedoch, die beiden gegenläufigen Aspekte durch eine gänzlich belanglose rhetorische Formel wieder zusammenzubringen: „Definitionen sind wichtig, aber wir müssen jetzt handeln."[6]

Der reale Kern der apodiktisch vorgetragenen Zurückweisung des Begriffs der Cyberkriege besteht darin, dass Cyberangriffe nicht als Casus Belli herhalten sollen

Der reale Kern der apodiktisch vorgetragenen Zurückweisung des Begriffs der Cyberkriege besteht darin, dass Cyberangriffe nicht als Casus Belli herhalten sollen. Befürchtet wird dabei, dass die USA (oder andere westliche Länder) durch die Berufung auf einen Cyberangriff den Eintritt in einen „richtigen" Krieg rechtfertigen können. Es ist in hohem Maß kennzeichnend für die Qualität dieser Debatte, dass die bloße Befürchtung eine eingehende Untersuchung der Frage, ob es Cyberkrieg gibt und wie die möglichen Cyberkriege der Zukunft aussehen könnten, von vornherein zu verbieten scheint. Dabei ist die Sorge weitaus weniger begründet als zunächst befürchtet. Zwar sehen westliche Militärdoktrinen durchweg vor, dass ein Cyberangriff auch mit konventionellen militärischen Mitteln beantwortet werden kann. Diese Auskunft ist jedoch Teil der strategischen Abschreckung insbesondere gegen Staaten, die durch Cyber-Gegenangriffe kaum verwundbar sind. (Das nordkoreanische Internet besteht aus lediglich 28 Webseiten.) Doch kein Staat würde wegen Spionage- oder Ransomware-Attacken in einen Krieg ziehen.

Krieg und Frieden

Es ist daher an dieser Stelle sinnvoll, ein paar begriffliche Unterscheidungen vorzunehmen. Denn typischerweise werden drei ganz verschiedene Dinge als „Cyberkrieg" bezeichnet:

1. Der Idee nach handelt es sich um einen Krieg zwischen zwei souveränen Staaten, der wesentlich mit Cybermitteln, also weitgehend nicht kinetisch geführt wird. Im Gegensatz zu Cyberkriminalität und Cyberspionage hat es Cyberkriege in diesem Sinne bislang nicht gegeben und es gibt keine Anzeichen, dass es sie in naher Zukunft geben wird. Als Ausnahme gilt gemeinhin Stuxnet, der mutmaßliche amerikanisch-israelische Angriff auf die Nuklearanlage im iranischen Natanz. Es ist jedoch umstritten, ob dieser Angriff sinnvoll als Kriegsakt bezeichnet werden kann.

2. Von Cyberkrieg wird auch dort gesprochen, wo begrenzte Cyberangriffe als Vorbereitung eines sogenannten kinetischen Kriegs vorgenommen werden. Inzwischen ist Cybertechnologie tief in eine Vielzahl von Waffensystemen integriert. Kriege der Zukunft werden damit in hohem Maße *auch* Cyberelemente enthalten, doch es scheint, dass eine solche Integration von Cyberelementen in den Krieg letztlich die Vorstellung vom Cyberkrieg obsolet machen wird. Einstweilen hat Cybertechnologie in dieser Verwendung eher die Wirkung der Minderung von kinetischer Zerstörung und damit der Einhegung des Kriegs – ein Umstand, der von Anfang an zum Szenario von Cyberkriegen gehörte und bis heute ein entscheidendes Argument gegen die großen Cyberdystopien bildet.[7]

3. Einer weiteren Auffassung zufolge beschreibt die Allgegenwart von Cyberkriminalität und Cyberspionage (die jederzeit in einen vollen Krieg übergehen *kann,* aber nicht tatsächlich in einen solchen Krieg übergeht) eine neue Art von Krieg, die den permanenten Ausnahmezustand zum neuen Normalzustand macht. Es handelt sich hier nicht um Krieg in dem Sinne, wie er durch das internationale Recht kodifi-

ziert ist, sondern eher um einen vorrechtlichen Kriegszustand im Sinne des Hobbes'schen Naturzustands, des Kampfes aller gegen alle.[8] Insbesondere in dieser Bedeutung fordert der Cyberkrieg in hohem Maß unsere Vorstellungen von Krieg und Frieden heraus.

Jener Cyber-Naturzustand bildet einen Grenzbereich zwischen Cyberkriminalität, Cyberspionage und Cyberkrieg im engeren Sinne. Man muss hier zunächst mit der begrifflichen Unschärfe leben, dass „Cyberkrieg" sowohl etwas von Cyberkriminalität und Cyberspionage jeweils Verschiedenes als auch die Summe aller drei bezeichnen kann. Grob gesprochen, bildet Cyberkriminalität die technologische Avantgarde, während Cyberspionage der Bereich ist, in dem Staaten und staatlich unterstützte Organisationen ihre Cyberkapazitäten aufbauen. Cyberangriffe im engeren Sinne zeichnen sich dadurch aus, dass in ihnen die Kapazitäten von Cyberkriminalität und Cyberspionage auf eine neue Stufe der Präzision und Durchschlagskraft gebracht werden. Solche Angriffe sind äußerst selten (Stuxnet ist vielleicht das einzige Beispiel, das alle Kriterien erfüllt), extrem aufwendig in der Vorbereitung, in ihrer Reichweite begrenzt und nicht reproduzierbar. Zugleich sind sie prinzipiell möglich und stellen eine kontinuierliche strategische Gefahr dar.

In den allermeisten Fällen findet der Cyberkrieg in jenem Grenzbereich zu Cyberkriminalität und Cyberspionage statt, und dies scheint in hohem Maß die neue Art des Kriegs im 21. Jahrhundert zu bilden. Die eigentliche Pointe daran ist, dass damit die Unterscheidung von Krieg und Frieden nahezu unmöglich wird. George Lucas bezeichnet diese Art des Kriegs als „dauerhafte, ‚grenzenlose' Kriegführung – eine Kriegführung ohne Regeln, ‚Krieg aller gegen alle' […]. Die Gefahr einer solchen Kriegführung besteht nicht nur darin, dass sie die Grenzen zwischen Krieg und ‚bloßen' kriminellen Aktivitäten verschwimmen lässt, sondern auch, dass ein solcher Kriegszustand immer schwerer vom Frieden zu unterscheiden ist."[9]

Wenn es zutrifft, dass diese Art von Cyberkrieg die neue Art des Kriegs im 21. Jahrhundert bildet, dann löst sich die Definition des Cyberkriegs von ihrer Anlehnung an den Kriegsbegriff bei Clausewitz: „Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen."[10] Dieser Begriff wird in der Cyberkriegsdebatte insbesondere von solchen Vertretern bevorzugt, die vom gerechten Krieg und vom Kriterium des Casus Belli ausgehen. Das eigentlich Neue am Cyberkrieg indes ist die prinzipielle Unklarheit, inwiefern es sich überhaupt um Krieg handelt – der Schwebezustand zwischen Krieg und Frieden. Die strategische Bedrohung durch Cyberkriege sorgt für eine Permanenz des Kriegs im Frieden.

Die strategische Bedrohung durch Cyberkriege sorgt für eine Permanenz des Kriegs im Frieden

Demnach muss man sich nicht so sehr an Clausewitz halten, sondern auf Hobbes und den Begriff des Krieges aller gegen alle zurückgehen – in diesem Zustand „nagt […] die Furcht vor Tod, Armut oder einem anderen Unglück den ganzen Tag über am Herzen des Menschen, der aus Sorge über die Zukunft zu weit blickt, und er hat vor seiner Angst nur im Schlaf Ruhe."[11] Dieser Zustand, der bei Hobbes durch die Abwesenheit eines starken Königs geprägt war, hat seine gegenwärtige Entsprechung in der Abwesenheit einer unipolaren Weltmacht und den Hegemoniekämpfen in einer multipolaren Welt. Cyberkrieg ist das Mittel der Wahl für aufstrebende Großmächte, um die immer noch starken USA innerhalb dieses Koordinatensystems herauszufordern und sich ihnen gegenüber technologische, informationelle, ökonomische oder ideologische Vorteile zu verschaffen.

Normen für den Cyberkrieg

Bei Hobbes sollte die These vom Kampf aller gegen alle die *Abkehr* vom Naturzustand und die Begründung der Zivilisation motivieren. Vieles spricht dafür, dass dem 21. Jahrhundert ein ähnlicher Prozess hinsichtlich des Cyberkriegs aller gegen alle bevorsteht. Doch wie lässt sich dieser Cyber-Naturzustand einhegen? Ist es eine Sache des internationalen Rechts, das die klassischen Normen des (analogen) Kriegs

auf den Cyberspace anwendet? Der ursprüngliche Völkerrechtsenthusiasmus, wie er noch im sogenannten *Tallin Manual* (2013/2017) zum Ausdruck kam, weicht dabei immer mehr einem komplexeren Verständnis der Prozesse, in denen sich Normen für den Cyberkrieg erst herausbilden.

Einzelne mögliche „starke" Normen wie die Beschränkung von Angriffen auf enge militärische Ziele, die Ächtung von Cyber-Erstschlägen oder die Verpflichtung, nicht staatliche Angriffe vom eigenen Territorium zu unterbinden, haben bislang insbesondere bei den großen Playern keine Zustimmung gefunden. Dabei haben auch diese großen Player wenig Interesse an einem großen Cyberkrieg. Zum Teil ist dies paradoxerweise in dem Prinzip der *mutually assured destruction* begründet, analog zur Aussicht auf gegenseitige atomare Vernichtung im Kalten Krieg. Abschreckung sorgt insbesondere dafür, dass es zwischen den USA und China, zwei der drei größten Player, bislang keinen Cyberkrieg gegeben hat und ein solcher Cyberkrieg wenig strategische Plausibilität besitzt. China könnte jederzeit von der Cyberspionage zum Cyberkrieg gegen die USA übergehen, was zumindest durch einige große Hacks nahegelegt wird; und die USA könnten ihrerseits China angreifen, insbesondere wo sie die durch chinesische Produktpiraterie entstehenden Sicherheitslücken ausnutzen können. Beide können durch einen Cyberkrieg wenig erreichen, aber viel verlieren.

Es scheint, als hätte auch dieses trotz aller verschiedenen Ziele gemeinsame Interesse, es zu einem großen Cyberkrieg nicht kommen zu lassen, die jüngste Konjunktur der Cyberdiplomatie befördert. Folgt man den entsprechenden Initiativen gerade aufseiten der Europäischen Union, so geht es dabei zunächst vor allem um Dialog- und Vertrauensbildung zwischen den Cybermächten. Idealerweise führt der diplomatische Dialog zu Vereinbarungen unterhalb der Schwelle des Rechts, die mit der Zeit quasi Gesetzeskraft erlangen.

Normen für den Cyberkrieg bilden sich ferner auch im Zusammenspiel mit dem Privatsektor heraus, so in dem schnell wachsenden Markt für Cyberversicherungen. Hier wird in nächster Zukunft über modellhafte Gerichtsurteile zu Haftungsfragen ein neuer Normierungsschub erfolgen – und dies in einem Umfang, der erheblich über das medial weithin sichtbare Thema der selbstfahrenden Autos hinausgeht. Recht wird demnach zunächst primär aus Gerichtsurteilen zu Haftungsfragen bei Schäden durch Cyberangriffe entstehen. So geht es bei der versicherungsrechtlichen Abwicklung von NotPetya – einem mutmaßlichen russischen Cyberangriff gegen die Ukraine, bei dem eine Ransomware-Schadsoftware (Petya) als Tarnung verwendet wurde – zentral um die Frage, ob es sich dabei um einen staatlichen russischen Angriff und damit einen kriegsähnlichen Akt handelt. Nach der Klage des Mondelez-Konzerns gegen die Zurich-Versicherungsgruppe, die nach dem NotPetya-Angriff aufgrund der Kriegsausschlussklausel die Zahlung verweigerte, wird die Frage demnächst von einem amerikanischen Gericht zu entscheiden sein. Der Fall ist für die Herausbildung von Normen für den Cyberkrieg von größter Tragweite und wird sich zweifellos auch auf die Normierung zwischenstaatlicher Cyberangriffe auswirken. Aber auch die Festlegung von „Good Practice"-Verfahren und Industriestandards werden den Umgang mit Bedrohungen stark verändern. Cyberethik sollte vornehmlich diese Prozesse reflektieren und kritisch begleiten, anstatt der Cyberpraxis eine normative Konzeption vorgeben zu wollen, die in den tatsächlichen Normierungsprozessen keine Rolle spielt.

Die multipolare Welt der Cybersicherheit

Folgt man solchen Beispielen für Normierungsprozesse und den daran beteiligten Instanzen, so zeigt sich auch, dass die befürchtete „Militarisierung" des Cyberspace nicht stattgefunden hat. Das Militär ist einer von vielen Playern im Bereich der staatlichen Cyberabwehr, aber es hat nicht den Cyberraum „unter Kontrolle" gebracht. Gerade im föderalen Deutschland teilt sich die Bundeswehr ihre Aufgaben mit den verschiedenen Landeskriminalämtern, dem BND, dem BSI und verschiedenen Ministerien. International ist die staatliche Cyberabwehr in die NATO und die EU eingebunden. Ferner ergeben sich immer wieder begrenzte Allianzen von hoher Durchschlagskraft, darunter die Five

Eyes (Australien, Großbritannien, Kanada, Neuseeland, Vereinigte Staaten) mitsamt ihren diversen Erweiterungen, zu denen teilweise auch Deutschland gehört (Eight Eyes, Nine Eyes, Fourteen Eyes). Zugleich haben auch Unternehmen, private IT-Sicherheitsfirmen und Cyberversicherungen einen immer größeren Anteil an der Cybersicherheit.

Die militärische Komponente ist in dieser Multipolarität der Kompetenzen und Zuständigkeiten ein wichtiges Element. Es wird vor allem dann bedeutsam sein, wenn ein Angriff militärischer Natur ist. Dies betrifft nicht allein die Ziele, sondern vor allem die Angriffsart, das heißt den Grad der Komplexität und strategischen Tiefe. Im Bereich der alltäglichen Cyberkriminalität übernehmen staatliche Stellen nur in geringem Maß selbst Abwehraufgaben. Sie sind hier weitgehend koordinierend tätig und können zudem über die Formulierung von technischen Mindeststandards – etwa bei der Vergabe von öffentlichen Aufträgen – oder rechtlichen Rahmenbedingungen auf die Cybersicherheit von Unternehmen, Infrastrukturen und privaten Nutzern einwirken.

Man darf also die militärische Cyberabwehr nicht mit zu hohen Erwartungen überfordern. Ihre tatsächlichen Aufgaben liegen im Normalfall in einem Bereich, der von anderen Playern nicht bedient werden kann. Im Ernstfall kann sie aufgrund ihrer größeren Möglichkeiten und Befugnisse eine stärker koordinierende Rolle einnehmen. Die Diskussionen über die notwendigen Kapazitäten und Befugnisse des Cyberkommandos der Bundeswehr haben sich stark auf die Frage konzentriert, ob es im Angriffsfall allein ihrem defensiven Mandat treu bleiben kann oder gegebenenfalls auch „zurückhacken" darf, etwa um den Server eines Angreifers abzuschalten. Ebenso könnte sie auch Teile der deutschen Infrastruktur vom Netz nehmen, um sie temporär dem Zugriff durch militärische Angreifer zu entziehen. Während eine flächendeckende militärische Kontrolle des Internets kaum wünschenswert wäre, gibt es wenig Grund, auf den relativen Schutz durch militärische Cyberkommandos zu verzichten.

1 Arquilla, John/Ronfeldt, David (1993): „Cyberwar is Coming!". In: *Comparative Strategy* 12 (1), S. 141–165, Nachdruck in: Arquilla, John/ Ronfeldt, David (Hg.) (1997): *In Athena's Camp. Preparing for Conflict in the Information Age.* Santa Monica, S. 23–60.
2 James Andrew Lewis (2018): „Rethinking Cybersecurity. Strategy, Mass Effect, and States. A Report of the CSIS Technology Program". https://www.csis.org/analysis/rethinking-cybersecurity (Stand: 25. April 2019).
3 Rid, Thomas (2012): „Cyber War Will Not Take Place." The Journal of Strategic Studies, 35 (1), S. 5–32, S. 6; vgl. ders. (2018): *Mythos Cyberwar.* Hamburg.
4 Hersh, Seymour M. (2010): „The Online Threat: Should We Be Worried About a Cyber War?". *The New Yorker,* 1.11.2010 (aus dem Englischen übersetzt).
5 Amit Yoran (2010): „Cyberwar or Not Cyberwar? And Why That Is the Question". *Forbes,* 25.3.2010 (aus dem Englischen übersetzt). www.forbes.com/sites/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-why-that-is-the-question/ (Stand: 25. April 2019).
6 Ebd.
7 Arquilla, John (2012): „Cyberwar Is Already Upon Us. But Can It Be Controlled?". *Foreign Policy,* 27.2.2012, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ (Stand: 25. April 2019).
8 Für Hobbes liegt die Schwelle zum Kriegszustand schon bei der drohenden Gefahr einer Eskalation: „Denn Krieg besteht nicht nur in Schlachten oder Kampfhandlungen, sondern in einem Zeitraum, in dem der Wille zum Kampf genügend bekannt ist. Und deshalb gehört zum Wesen des Krieges der Begriff Zeit, wie zum Wesen des Wetters. Denn wie das Wesen des schlechten Wetters nicht in ein oder zwei Regenschauern liegt, sondern in einer Neigung hierzu während mehrerer Tage, so besteht das Wesen des Kriegs nicht in tatsächlichen Kampfhandlungen, sondern in der bekannten Bereitschaft dazu während der ganzen Zeit, in der man sich des Gegenteils nicht sicher sein kann. Jede andere Zeit ist Frieden." Hobbes, Thomas (2011): *Leviathan.* Aus dem Englischen von Walter Euchner. Berlin, S. 122.
9 Lucas, George (2017): *Ethics and Cyber Warfare. The Quest for Responsible Security in the Age of Digital Warfare.* New York, S. 9 (aus dem Englischen übersetzt).
10 Clausewitz, Carl von (1973): *Vom Kriege.* 18. Aufl. Bonn, S. 191 f.
11 Hobbes, Thomas (2011): *Leviathan.* Aus dem Englischen von Walter Euchner. Berlin, S. 106.

Der Autor

Philipp von Wussow *studierte Philosophie, Germanistik und Informationswissenschaft an der Heinrich-Heine-Universität Düsseldorf. 2004/2005 war er als Gastwissenschaftler an der Hebräischen Universität Jerusalem. Promotion 2006 mit einer Arbeit über Theodor W. Adorno. Von 2007 bis 2013 arbeitete er an der Universität Leipzig, von 2014 bis 2016 an der Goethe-Universität Frankfurt am Main. 2016/2017 war er Visiting Research Fellow an der University of Pennsylvania, Philadelphia. 2017 Habilitation an der Goethe-Universität. Seit 2018 ist Philipp von Wussow als Projektleiter „Cyberethik" am Institut für Theologie und Frieden in Hamburg tätig.*

DIE AUSSICHT AUF FRIEDEN IM CYBERSPACE

Autor: ***George R. Lucas***

Abstract

In seinem Beitrag untersucht George R. Lucas ein grundlegendes ethisches Dilemma in Hobbes' ursprünglicher, ansonsten streng amoralischer Darstellung des Naturzustands: Wie sollte der Mensch einen scheinbar moralisch notwendigen Übergang zu einer stabileren, rechtsstaatliche Grundsätze beinhaltenden politischen Ordnung bewerkstelligen, durch die die Interessen der verschiedenen Bewohner an Leben, Eigentum und Sicherheit besser gewährleistet wären? Hobbes' Beschreibung zufolge erwächst der Widerstand gegen diesen moralisch gebotenen Übergang aus einer „universellen Zurückhaltung", dem gegenseitigen Misstrauen unter Individuen, gepaart mit dem fehlgeleiteten Glauben jedes oder jeder Einzelnen an seine oder ihre Überlegenheit. Dieser moralische Rahmen, so die Argumentation des Autors, eigne sich daher perfekt für die Analyse der Aussichten auf Frieden im Cyberspace.

Innerhalb dieses Rahmens lässt sich schnell feststellen, dass sich die bedeutendsten moralischen Fragen darauf beziehen, ob bereits eine allmähliche freiwillige Anerkennung und Akzeptanz allgemeingültiger Normen für das Verhalten des Einzelnen und des Staates im Cyberspace erkennbar ist, die sich aus Erfahrung und daraus folgendem aufgeklärtem Eigeninteresse ableiten lassen, oder ob die Interessen der verantwortungsbewussten Mehrheit letztlich einen wie auch immer gearteten Übergang vom Naturzustand erzwingen, indem sie sich im Interesse des Allgemeinwohls über die Wünsche vermeintlich unverantwortlicher oder böswilliger Außenseiter hinwegsetzen. Lucas lässt keinen Zweifel daran, dass wir uns dem Prozess der Normbildung deskriptiv annähern und die relative Rechtsfreiheit des Cyberraums aushalten müssen, anstatt uns für die moralisch inakzeptable zweite Lösung zu entscheiden.

Der Ruf nach Frieden im friedlosen Cyberspace

Wenn wir nicht gerade von den neuesten Technologien in Beschlag genommen werden, die uns das Internet der Dinge bietet, konzentrieren wir uns im Cyberspace gern auf die endlosen Konflikte und potenziellen „virtuellen Kriege", die wir dort ausmachen können. Doch wie steht es um die Aussicht auf Frieden? Inwieweit ist Frieden, im Gegensatz zu Krieg, hier ein wünschenswerter Zustand? Wichtiger noch: Wie groß ist die Bereitschaft der relevanten Akteure, sich für friedliche Verhältnisse einzusetzen, anstatt in endloser, unlösbar scheinender Zwietracht zu verharren?

Auf den ersten Blick dürfte nichts weniger aussichtsreich wirken als der Versuch, „Frieden" in diesem Kontext zu diskutieren. Selbst abseits der komplexen moralischen Fragen im Zusammenhang mit direkter Kriegführung wird der Cyberspace oft als „rechtsfreies Neuland" oder „Naturzustand" beschrieben, in dem jeder grundsätzlich in der Lage zu sein scheint, egal wem egal was anzutun, ohne sich dafür verantworten oder gar Vergeltung fürchten zu müssen. Dementsprechend ließe sich menschliches Verhalten und zwischenmenschlicher Umgang im Cyberspace wohl am ehesten als „Krieg aller gegen alle" charakterisieren.

Bei näherer Betrachtung erweist sich diese düstere Verallgemeinerung jedoch als nicht mehr oder weniger zutreffend als Hobbes' eigene ursprüngliche Darstellung, in der er das menschliche Wesen in einem hypothetischen Naturzustand verortet. Führen wir uns den Cyberspace einmal vor Augen, so erscheinen die meisten Akteure relativ harmlos: Sie kümmern sich um ihre persönlichen Angelegenheiten und verfolgen ihre eigenen Ziele. Sie schädigen nichts und niemanden absichtlich. Sie wünschen ihren Mitbürgern nichts Böses und wollen in der Regel ausschließlich die zahlreichen Vorteile des Internets nutzen: Zugang zu Informationen, Waren und Dienstleistungen, komfortable Finanztransaktionen

und Datenverarbeitungsangebote, aber auch die Steuerung der gesamten technischen Ausstattung im Haushalt, vom Kühlschrank und Toaster bis hin zum Swimmingpool im Garten, via Smartphone und Sprachassistenten wie Alexa und Echo.

Darüber hinaus bietet der digitale Raum eine Reihe „natürlicher" und allgemein als gut definierter Vorzüge: zum Beispiel Anonymität, (Wahl-)Freiheit sowie die erkennbare Abwesenheit äußerer Zwänge, Einschränkungen und Vorschriften. Diese Vorteile verteidigen insbesondere Online-Aktivisten gern; ganz offenbar gilt es, diese Freiheiten mit Entschlossenheit – und im Namen der „Rechtsstaatlichkeit" – vor jeder Form der Beeinträchtigung zu schützen. Man könnte das Internet als einen von Libertären und Anarchisten bevölkerten Raum bezeichnen, die sich, wenn man sie in Ruhe ließe, miteinander vertragen und ihre privaten und kollektiven Interessen ungestört verfolgen würden.

Wie überall in relativ rechtsfreiem Neuland kann diese natürliche Friedlichkeit durch das böswillige und schädigende Verhalten einiger weniger Akteure ohne Weiteres zunichtegemacht werden. Und in der digitalen Welt finden sich mehr als nur einige wenige „schädliche Akteure". In ihrem in Kürze erscheinenden Buch stellen die Cybersicherheitsexperten Seumas Miller und Terry Bossomaier dar, dass böswillige Aktivitäten im Netz hauptsächlich kriminelle Züge tragen und von Diebstahl, Erpressung, Vandalismus, Verleumdung und Desinformation (in Form des sogenannten Trollens und digitalen Mobbings) bis hin zu Morddrohungen reichen.[1]

In dieser Ausgabe schreibt Philipp von Wussow entsprechend, bei der „Kriegführung" im Cyberspace handle es sich um die von Thomas Hobbes beschriebene und nicht um die neuere und gängigere Darstellung von Carl von Clausewitz, der zufolge Krieg als Fortsetzung eines naturgegebenen Konflikts zwischen klar definierten, rivalisierenden politischen Zielvorstellungen gut organisierter Staaten eintritt. Für Hobbes hingegen ist Krieg der Naturzustand menschlicher Akteure außerhalb politischer Institutionen, gekennzeichnet durch Anarchie und die Abwesenheit jeglicher erkennbarer Obrigkeit oder Rechtsstaatlichkeit.

Doch im Gegensatz zu den Positionen der modernen politischen Philosophie bildet der derzeitige Konflikt im Netz keine hypothetische „Annahme" oder fiktive „Ausgangsposition", die einen privilegierten Standpunkt für die „Vernunft" als Entscheidungsgrundlage für bestimmte Tatsachen böte. Vielmehr erkennen wir im Internet den ersten wahrhaft gegenwärtigen und zutreffenden *Beleg* eines solchen Zustands, der akkurat mit dem Ausdruck *bellum omnium contra omnes* beschrieben werden darf – exakt dies stellt der digitale Raum dar.

Auf faszinierende Weise liefert uns der Cyberspace unbeabsichtigt das erste authentische Labor, in dem die wichtigsten Herausforderungen und das Rätsel des „Leviathan" untersucht werden können

Auf faszinierende Weise liefert uns der Cyberspace durch zahlreiche Konflikte und fehlende Strukturen unbeabsichtigt das erste authentische Labor, in dem die wichtigsten Herausforderungen und das Rätsel des *Leviathan* als solches untersucht werden können. Wie genau gelingt es der Zivilgesellschaft, der Sozialordnung und dem Rechtsstaat, aus diesem Zustand der ursprünglichen Anarchie hinauszutreten? Die dem *Leviathan* (implizit) zugrunde liegende Frage lautet schließlich: „Wo finden wir in dieser elenden, gefallenen Welt voll endloser Konflikte Aussichten auf Frieden?" Und wenn Frieden und Sicherheit, wie sie durch den Rechtsstaat gewährleistet werden, das oberste Ziel des *Leviathan* sind, wie soll dieses Ziel erreicht werden?

Wenn wir wie Philipp von Wussow in deskriptiver Absicht auf Hobbes zurückgreifen, kommen wir nicht umhin, auch die *normative* Dimension seiner Abhandlungen in Betracht zu ziehen, die oft genug außer Acht gelassen wird. Für einen Philosophen, der ansonsten für seine Ablehnung von Moral berühmt ist, erscheint dieser Ansatz zuge-

gebenermaßen wenig tragfähig. Gleichwohl liegt auch hierin ein Verständnis von Moral: dass nämlich all jene, die sich in diesem Naturzustand befänden, verpflichtet seien (wie Hobbes kommentiert), „diesen unverzüglich zu verlassen". Konfrontiert mit unserem Naturzustand, so seine Argumentation, dürfen wir nicht in ihm verharren, sondern müssen ihn in etwas Stabileres und Sichereres umwandeln. Hobbes' weitgehend realistischem oder „amoralischem" Standpunkt zufolge bestünde die einzige Handlung, die eine wahrhaft moralische oder ethische, über das eigene Interesse im engeren Sinne hinausgehende Entscheidung darstellen würde, in der aufgeklärten Entscheidung jedes Menschen, den Naturzustand zu verlassen und einen wie auch immer gearteten gesellschaftlichen Vertrag einzugehen, der wiederum durch strenge Auferlegung von Recht und Ordnung Sicherheit mit sich brächte.

Das Netz kennt weder Grenzen noch Regierungen, und digital mündige Bürger sind erklärtermaßen nicht bereit, sich diesbezüglich Einschränkungen auferlegen zu lassen oder diese zu tolerieren

An diesem Punkt stoßen wir jedoch in der digitalen Welt auf etwas, das als „Realitätsparadox" bezeichnet werden könnte. Anders als bei Hobbes' fiktiven Individuen, die auf unschöne Weise in einem hypothetischen Naturzustand ihr Dasein fristen, sind „Recht und Ordnung", ganz zu schweigen von Institutionen wie Polizei und Gerichtsbarkeit, genau das, was Einzelakteure und nicht staatliche Organisationen (wie Anonymous) im Cyberspace für gewöhnlich *beharrlich zu meiden suchen*. Zugleich würde kein digital bewanderter Bürger, der etwas auf sich hält, Hobbes' eigene Lösung für das Problem der Anarchie bereitwillig aufgreifen: nämlich die Vorstellung, dass eine sinnvoll regulierte Zivilgesellschaft nur durch die entschiedene Auferlegung autoritärer Herrschaft zu erlangen sei. In jüngster Zeit war zu beobachten, dass Nationen wie China sich anschicken, die Hobbes'sche Formel im digitalen Raum anzuwenden – mit mäßigem Erfolg. Jedoch ist diese Vorgehensweise nicht nur demokratischen Gesellschaften, die die Rechte ihrer Bürger achten, ein Dorn im Auge – sie wäre ein grundlegender Verrat dessen, was wir soeben als die naturgemäßen Tugenden und begrenzten natürlichen Rechte der digitalen Gemeinschaft bezeichnet haben: Freiheit, Anonymität, Privatsphäre und eine von Einmischung weitgehend ungestörte Handlungsfreiheit. Das Netz kennt weder Grenzen noch Regierungen, und digital mündige Bürger sind erklärtermaßen nicht bereit, sich diesbezüglich Einschränkungen auferlegen zu lassen oder diese zu tolerieren, egal, was die chinesische Regierung für die Zukunft planen mag.[2]

Ein sehr bekanntes, wenngleich ungelöstes Problem bei Hobbes besteht darin, dass der Übergang von der Anarchie zur Zivilgesellschaft nie wirklich ausreichend erklärt wird. Andererseits scheint Hobbes zu behaupten, dieser Übergang werde sich mehr oder weniger selbstverständlich vollziehen, sobald die Menschen einsähen, dass sie ihren Eigeninteressen besser dienen, wenn sie einige ihrer Freiheiten und Rechte für die von einem autoritären System gewährleistete Sicherheit opfern. Gleichzeitig räumt Hobbes jedoch ein, dass es für das Eintreten dieses gutartigen Übergangs keine Garantie gibt: Manche, insbesondere jene mit bösen Absichten, würden sich dem widersetzen. Die wahrhaft Mächtigen, die Stärksten in dem Naturzustand, würden ihre persönliche Autorität nie bereitwillig an den Rechtsstaat abgeben, schlicht, weil dies nie in ihrem eigenen Interesse liegen könne.

Im Gegensatz zu unserem oben erwähnten „Realitätsparadox" der digitalen Welt erzeugt dieser Widerspruch etwas, das allgemein als „Hobbes'sches Paradox" bekannt ist: Um zu erreichen, was eindeutig im Eigeninteresse aller läge, müsste *auf irgendeine Art und Weise Gewalt ausgeübt* werden. Nur so könne man sich über die eng gefassten Eigeninteressen von Tyrannen im Naturzustand hinwegsetzen. Wer aber würde im Naturzustand einer Beseitigung der Tyrannen zustimmen? Und wie könnten wir anderen weiterhin darauf vertrauen, dass jeder, der freiwillig dazu

bereit wäre, es auch *in die Tat umsetzt,* ohne einfach ihren Platz einzunehmen? Der moralische Imperativ – der einzige moralische Imperativ, den Hobbes anerkennt – besagt, dass dieser Übergang zur Zivilgesellschaft bewerkstelligt werden muss. Offenbar ist er aber nicht möglich. Oder zumindest existiert kein klarer Weg und auch keine hieb- und stichfeste Garantie, dass er stattfinden kann oder wird.

Die Herausbildung von Normen zum Umgang mit Konflikten im digitalen Raum

Betrachten wir Cyberkonflikte von der Warte der internationalen Beziehungen aus, so sind die in böser Absicht Handelnden primär Schurkenstaaten, Terroristen und nicht staatliche Akteure (neben der Organisierten Kriminalität). Die herrschende Konflikttheorie auf der Ebene der internationalen Beziehungen – die Theorie der internationalen Anarchie oder des „politischen Realismus" – beruht auf Rousseaus metaphorischer Ausweitung der Hobbes'schen Analyse von Einzelpersonen auf Staaten. Hinsichtlich der internationalen Anarchie besteht jedoch zwischen Hobbes und Rousseau ein wesentlicher Unterschied. Auch wenn der „Naturzustand" bei Einzelpersonen in Hobbes' Darstellung meist als hypothetisches Gedankenexperiment gelesen wird (und nicht als Versuch einer geschichtlichen oder evolutionären Beschreibung), bezeichnet jener Zustand des endlosen Konflikts und Streits zwischen den Nationen (wie erstmals von Rousseau beobachtet) genau das, was in den internationalen Beziehungen aktuell und andauernd vor sich geht.

Der Konflikt zwischen internationalen Entitäten entsteht somit als Folge eines unausweichlichen Wettstreits und Aufeinanderprallens der Interessen eigenständiger Staaten – sofern institutionelle Gefüge fehlen, die den Konflikt abseits rivalisierender Nationen und deren relativer Widerstandskraft gegen die Übergriffe der jeweils anderen Partei lösen könnten. In Anlehnung an Hobbes' Darstellung des amoralischen Naturzustands bei hypothetischen Einzelpersonen vor der Errichtung eines Rechtsstaats gehen beinahe alle Politologen und Experten für internationale Beziehungen davon aus, dass dieser Zustand des Konflikts zwischen den Nationen immun gegen Moralvorstellungen im herkömmlichen Sinne sei – immun gegen Abwägung und Handeln auf der Grundlage von Moral und Tugend, gegen das übergeordnete Pflichtgefühl, die Anerkennung und Achtung grundlegender Menschenrechte oder das Streben nach Stärkung des Gemeinwohls.

Wie auch immer wir gewöhnliche zwischenstaatliche Beziehungen beschreiben – der gegenwärtige Zustand der Beziehungen und Konflikte zwischen Nationen und Einzelpersonen im Cyberraum entspricht diesem Modell eines rechtsfreien Neulands, das (vermeintlich) frei von tugendhaften Bestrebungen oder der Sorge um das übergeordnete Gemeinwohl ist, perfekt. Es handelt sich dabei um ein „Gemeingut", in dem jeder, der alle anderen nach seinem Gutdünken behandelt, seinen Vorteil daraus zu ziehen scheint, ohne befürchten zu müssen, dafür zur Rechenschaft gezogen oder bestraft zu werden. Wie bereits bemerkt, scheint hier – viel mehr noch als in den herkömmlichen Bereichen politischer Rivalität – im wahrsten Sinne des Wortes der Zustand eines Kriegs aller gegen alle vorzuliegen.

Der moralische Imperativ – der einzige moralische Imperativ, den Hobbes anerkennt – besagt, dass der Übergang zur Zivilgesellschaft bewerkstelligt werden muss

Vom Sommer 2014 an – ich arbeitete gerade an meiner eigenen Monografie zur Cyberkriegführung[3] – beobachtete ich einige sonderbare und recht verwirrende Trends, die meinen Erwartungen krass zuwiderliefen. Wissenschaftler und andere Experten hatten seit Langem die Eskalation der „wirkungsorientierten" digitalen Kriegführung und die Weiterverbreitung von Cyberwaffen wie dem Stuxnet-Virus vorausgesagt. Die größte Befürchtung bestand darin, Schurkenstaaten

und Terroristen könnten Staudämme zerstören, nationale Stromnetze zum Erliegen bringen und Verkehr und Handel auf eine Art und Weise beeinträchtigen, die in ihrer verheerenden Wirkung, Zerstörung und der Zahl der Todesopfer einem intensiven konventionellen bewaffneten Konflikt gleichkäme. Diese Prognosen waren bereits vor der Entdeckung von Stuxnet geäußert worden, aber seine Entdeckung wurde (trotz offenkundiger Beteiligung der USA und Israels an der Entwicklung genau dieser Waffe im Rahmen der „Operation Olympic Games") als Vorbote eines digitalen Pearl Harbor oder eines Cyber-Armageddon aufgefasst.

Staaten verhielten sich zunehmend wie Einzelpersonen und nicht staatliche Gruppen im Cyberspace: Sie beteiligten sich an Identitätsdiebstahl, Erpressung, Desinformation und manipulierten Wahlen

Mir wurde jedoch zunehmend klar, dass dies *nicht* die Richtung war, die der internationale Konflikt im digitalen Raum eingeschlagen hatte. Das Verhalten von Einzelpersonen und nicht staatlichen Akteuren glich sich nicht immer mehr dem der Nationalstaaten an; ganz im Gegenteil stellte ich fest, dass sich Staaten zunehmend wie Einzelpersonen und nicht staatliche Gruppen im Cyberspace verhielten: Sie beteiligten sich an Identitätsdiebstahl, Erpressung und Desinformation, manipulierten Wahlen und wandten sonstige digitale Taktiken an, die sich hinsichtlich der Entwicklung und des Einsatzes als einfacher und kostengünstiger erwiesen und dabei weniger leicht zuzuordnen oder abzuwehren (geschweige denn zu vergelten) waren. Besonders auffällig war die Erkenntnis, dass sich damit im Vergleich zu wirkungsorientierten Cyberwaffen (die, wie auch Stuxnet selbst, umfangreich, komplex, teuer und zeitaufwendig sind und im Prinzip die Möglichkeiten der meisten Nationen übersteigen) eine fast gleich große, wenn nicht größere politische Wirkung erzielen lässt.

In einem 2015 erschienenen Artikel[4] habe ich diese sonderbaren, revolutionären militärischen Taktiken als staatlich unterstützten Hacktivismus *(state-sponsored hacktivism,* SSH) bezeichnet und vorausgesagt, dass sich dieser rasch zur vorherrschenden Form der Cyberkriegführung entwickeln werde. Aufgrund der politischen Motive und Wirkungen sollten wir ihn deshalb als neue Form der Kriegführung ernst nehmen. SSH passt zum Beispiel perfekt zu Carl von Clausewitz' oben genannter Definition des Kriegs als Fortsetzung der Politik mit anderen Mitteln. Wir hatten es also nicht mit einer, sondern mit *zwei* klar unterscheidbaren Formen von Cyberkriegführung zu tun: mit einer, die von großen, ressourcen- und technologiereichen Nationen betrieben wird, welche bestrebt sind, kinetische, wirkungsorientierte Waffen nachzubilden, und mit einer zweiten, die intelligente, skrupellose, jedoch etwas weniger ressourcenstarke Schurkenstaaten gewählt hatten, um insgesamt die politische Wirkung eines herkömmlichen Konflikts zu erzielen. Ich habe damit keine Allgemeingültigkeit beansprucht, sondern lediglich dafür plädiert (ohne jegliche Vorstellung dessen, wie sich die Lage entwickeln würde), dass wir die Möglichkeit in Betracht ziehen, uns geirrt zu haben. Wäre es nicht möglich, dass wir mit unseren Annahmen über die Form(en), die Cyberkonflikte letzten Endes annehmen können, wenn sie von den Streitkräften anderer Nationen ausgetragen werden, schlicht und ergreifend falschlagen? Vielleicht wenden wir uns einfach den falschen Dingen zu.

2016 schließlich versuchten russische Kräfte, die US-Präsidentschaftswahlen zu manipulieren. Nordkorea verlegte sich darauf, die der National Security Agency der USA gestohlene Software WannaCry aus dem Darknet herunterzuladen. WannaCry wurde für Angriffe auf die zivile Infrastruktur (Banken und Krankenhäuser) in europäischen Ländern verwendet, die die von den USA gegen das nordkoreanische Kernwaffenprogramm verhängten Sanktionen unterstützt hatten. Wirklich! Wie konnten wir, die Betroffenen, nur so töricht sein? Während

der staatlich unterstützte Hacktivismus zur verheerenden „Lieblingswaffe“ der Schurkenstaaten wurde, hielten wir trotz der erdrückenden Beweislast sträflicherweise an unseren kurzsichtigen politischen und taktischen Vorurteilen fest – und wurden auf dem falschen Fuß erwischt.

Gleichzeitig verwirrten meine Warnungen vor dem staatlich unterstützten Hacktivismus meine (nicht allzu zahlreichen) Leser und meine Kritiker. Anscheinend verstand niemand, was ich meinte! Mein Verlag in Oxford gab noch nicht mal meinen ursprünglich für das Buch geplanten Untertitel „Ethics & The Rise of State-Sponsored Hacktivism“ (Ethik und der Aufstieg des staatlich geförderten Hacktivismus; eigene Übersetzung) frei. Diese These musste ich stattdessen in den Kapiteln des Buches unterbringen. Doch dann kam der Tag der Abrechnung! Als das Buch schließlich direkt im Anschluss an die amerikanischen Präsidentschaftswahlen im Januar 2017 erschien, dankte ich meinem „PR- und Marketing-Team“: Wladimir Putin, Gastronom Jewgeni Prigoschin, dem russischen Inlandsgeheimdienst FSB, der Einheit 61384 der PLA Shanghai (die einige Jahre zuvor meine Personalakte und die von 22 Millionen weiteren US-Staatsbediensteten gestohlen hatte) und den nordkoreanischen Cyberkriegern, die zu diesem Zeitpunkt bereits einige beachtliche Triumphe auf unsere Kosten vorzuweisen hatten. Staatlich geförderter Hacktivismus war zu diesem Zeitpunkt bereits gängige Praxis geworden!

Aber wo ist bei all diesen Erörterungen die Verbindung zur Ethik? Das zentrale Thema meines Buchs sollte nicht in einer einfachen mechanischen Anwendung konventioneller Moraltheorie und Argumentation (Utilitarismus, Deontologie, Tugendethik, „Care-Ethik“ et cetera) auf bestimmte ungelöste Fragen bestehen. Vielmehr sollte es um eine sorgfältige Untersuchung dessen gehen, was in den internationalen Beziehungen als „Herausbildung von *Normen für verantwortungsvolles staatliches Handeln*“ bezeichnet wird. Dies sei, so meine Argumentation, von weitaus grundlegenderer Bedeutung als die konventionelle analytische Ethik. Bei diesem Ansatz geht es nicht hauptsächlich um Deontologie, Nutzen oder das Weichenstellerproblem. Vielmehr besteht er in einer Art historisch-moralischer Untersuchung, die sich mit dem Kern der Moralphilosophie selbst befasst, von Aristoteles über Hobbes, Rousseau und Kant bis hin zu Rawls und Habermas – und dem hauptsächlichen intellektuellen Leitbild des Buches, dem aristotelischen Philosophen Alasdair MacIntyre.

Für Philosophen besteht das große Rätsel natürlich darin, *inwiefern* es sinnvoll ist, von *„sich herausbildenden“* Normen zu sprechen. Es geht nicht nur darum, woher sie kommen oder wie sie Gültigkeit erlangen, sondern um die Frage: *Wie kann ein solcher historischer Prozess gültig sein* angesichts der Diskrepanz zwischen normativem und deskriptivem Ansatz und Diskurs? Vielleicht ist meine Bereitschaft, mich dieser uralten Frage anzunehmen und sie im Zentrum der gegenwärtigen Diskussionen zu Cyberkonflikten zu verorten, der Grund dafür, dass sich nur wenige die Mühe gemacht haben, das Buch zu lesen! Wen kümmert schon dieses abstrakte, theoretische Zeug? Entweder wollen wir den neuesten „Klatsch“ über Zero-Day-Software-Schwachstellen im Internet der Dinge besprechen oder unsere moralische Analyse zu Nutzen, Pflicht, Tugend und dem berüchtigten Weichenstellerproblem zum Besten

Für Philosophen besteht das große Rätsel darin, inwiefern es sinnvoll ist, von „sich herausbildenden“ Normen zu sprechen

Der Autor

George R. Lucas hatte bis vor Kurzem im Vice Admiral James B. Stockdale Center for Ethical Leadership an der US-Marineakademie in Annapolis einen Lehrstuhl für Ethik inne. Zudem war er Professor für Ethik und öffentliche Ordnung an der Graduate School of Public Policy der Naval Postgraduate School in Monterey/Kalifornien. Zu seinen neuesten Veröffentlichungen zählen die Titel: „Ethics and Military Strategy in the 21st Century: Moving Beyond Clausewitz“ (2019), „Ethics and Cyber Warfare“ (2017), „Military Ethics: What Everyone Needs to Know“ (2016) und „The Routledge Handbook of Military Ethics“ (2015).

geben – wobei wir vielleicht gerade einmal die Straßenbahnwagen durch selbstfahrende Fahrzeuge ersetzen (und uns dann fragen, „ob das autonome Fahrzeug den Tod seines eigenen Passagiers in Kauf nehmen sollte, um ein Manöver auszuführen, das fünf Fußgängern das Leben retten könnte", und so weiter).

Stattdessen hielt ich es für notwendig, die Grundlagen der Theorie des gerechten Kriegs und die Moral der Ausnahme oder „Exzeptionalismus" (mit anderen Worten: Wie rechtfertigen wir, dass wir mitunter Dinge tun müssen, die uns normalerweise verboten sind?) sowie die Herangehensweise der internationalen Beziehungen an entstehende Normen an sich auf Aristoteles und auf seine Abhandlung der Kultivierung moralischer Normen und Handlungsmaximen innerhalb einer Anwendergemeinschaft zurückzuführen, die sich durch eine gemeinsame Auffassung des Guten auszeichnet. Ich habe mich auf Kant, Rawls und Habermas gestützt, um zu erklären, wie sich wiederum eine ausschließlich von Eigeninteresse geleitete Anwendergemeinschaft dennoch zu einer Gemeinschaft entwickeln kann, die von genau den Formen der Anerkennung gemeinsamer moralischer Werte gekennzeichnet ist, auf die sich Hobbes ebenfalls implizit beruft, um den Übergang von einem „bösen, brutalen" Naturzustand zu einem wohlgeordneten Gemeinwesen zu erklären – *exakt das, was wir nun innerhalb des Cyberspace auszumachen versuchen*. Kant nannte diesen evolutionären Lernprozess „die List der Natur", wohingegen der dezidiert aristotelische Philosoph Hegel Kants ursprüngliche Begrifflichkeit übernahm und zur „List der Geschichte" abwandelte.

Moral bewegt sich in den kalten Gefilden des Cyberspace eindeutig auf dünnem Eis

Schließlich wandte ich eine ähnliche historisch-experimentelle Methode auf die jüngste Geschichte der Cyberkonflikte an – von Estland (2007) bis in die Gegenwart –, um eine Reihe solcher Normen des verantwortungsvollen digitalen Handelns zu veranschaulichen und zusammenzufassen, die anscheinend tatsächlich „entstanden" sind und „sich durchgesetzt" haben – sowie andere, die sich mit ein wenig mehr Zeit und Erfahrung mit einiger Wahrscheinlichkeit ebenfalls in diese Richtung bewegen werden. Selbst die Abkehr von der katastrophalen Zerstörung durch die kinetische, „wirkungsorientierte" Kriegführung (wie sie lauthals von Richard Clarke und anderen vorausgesagt wurde) hin zum staatlich geförderten Hacktivismus als bevorzugtem internationalem Konfliktmodus zeigte gleichermaßen die Herausbildung dieser Normen der vernunftgeleiteten Zurückhaltung. Es entstand weit weniger tatsächlicher Schaden, gleichzeitig wurden ähnliche politische Wirkungen erzielt – nicht weil wir „nett" sind, sondern weil wir schlau sind, wie bei Kants „Rennen der Teufel", die bekanntlich an der Schwelle zu echter Moral stehen.

Diese letzte Entwicklung bezieht sich im Fall des Cyberkriegs zum Beispiel auf die intuitive, unbewusste Anwendung einer Art Verhältnismäßigkeit durch diese schlauen „Teufel", etwas, das wir in der Militärethik als „Ökonomie der Gewalt" bezeichnen. Demzufolge ist ein schädlicher Cyberangriff einer noch zerstörerischeren Alternative vorzuziehen, sollte es diese geben – und zwar ebenfalls nicht, weil jemand die Absicht hat, „nett" zu sein, sondern weil ein solcher Angriff mit höherer Wahrscheinlichkeit gelingen und seine politischen Ziele erreichen wird, ohne eine vergleichbar harte Reaktion hervorzurufen. Derlei Angriffe sollten, anders als im Fall von Estland (wir gehen sodann zur Vernunft über), tatsächlich nur zur Unterstützung eines berechtigten Anliegens verfolgt werden und nicht gegen nicht militärische Ziele gerichtet sein. (Ich freue mich zwar nicht darüber, dass die PLA meine Personalakte stiehlt, aber schließlich bin ich – oder war ich – ein Staatsbediensteter, keine Privatperson.) Und somit ist die evolutionäre Entstehung moralischer Normen, Kants List der Natur (oder Hegels List der Geschichte),

bereits im Gange. Selbst ein Rennen der Teufel kann dazu dienen, die äußeren Umstände und Zwänge von Recht und Moral zu simulieren – wenn es sich dabei nur um „vernünftige“ Teufel handelt.

Fazit: das Hobbes'sche Paradox

Es ist gut möglich, dass diese Darstellung eines Normbildungsprozesses erneut als wenig tragfähiges Konzept von Moral kritisiert wird – genauso wie jene von Hobbes' Versuch, Schurken und Verbrecher dazu zu bringen, den Rechtsstaat anzunehmen. Diesen Befund kann ich nicht abstreiten: Moral bewegt sich in den kalten Gefilden des Cyberspace eindeutig auf dünnem Eis. Aber was ist die Alternative?

Um auf die Tatsache zu reagieren, dass wir uns im Cyberraum in fortwährender Geiselhaft befinden, müssten wir einen Vorgang von gewaltiger Immoralität hinnehmen. Tatsächlich sind unser Eigentum, unsere Sicherheit, selbst unsere Identität – genauso wie unsere öffentlichen Einrichtungen, unser zivilgesellschaftlicher Diskurs und unsere politische Entscheidungsfindung – unweigerlich dem Risiko ausgesetzt, von skrupellosen Personen, Organisationen oder Schurkenstaaten gekapert, gestohlen oder manipuliert zu werden. Das erscheint inakzeptabel, deshalb müssen offensichtlich wirkungsvolle Gegenmaßnahmen in Betracht gezogen und letztlich auch in Angriff genommen werden. Die Frage lautet nur: von wem – und mit welcher Berechtigung? Müssen nun alle Staaten ihre Grenzen wieder mit virtuellen „Firewalls“ absichern, um Eindringlinge abzuweisen (und ihre eigenen Bürger und Einwohner auf Linie zu halten)? Auch das erscheint nicht hinnehmbar.

Entweder würdigen und begünstigen wir die fragilen Normen, die im dünnen moralischen Boden des Cyberspace sprießen, oder wir kolonisieren und tyrannisieren dieses neue Gebiet, indem wir dort auf Kosten seiner vielversprechendsten Vorzüge mit Gewalt das Recht durchsetzen.

1 Miller, Seumas/Bossomaier, Terry (2019): *Ethics & Cyber Security*. Oxford (in Vorbereitung).
2 Es ist bemerkenswert, dass China seinerseits den USA und deren westlichen Verbündeten vorgeworfen hat, sie versuchten, dem „Gemeingut“ Cyberspace durch Arbeiten wie das Tallinn-Handbuch *(Tallinn Manual on International Law)* für dieses Terrain eine eigene Form von Hegemonie aufzuerlegen. Die offizielle Sichtweise besagt, dass der Cyberspace ein „Gemeingut“ ist, in dem alle Akteure (Einzelpersonen, Körperschaften und Nationen) uneingeschränkt handeln können. Diese internationale Sichtweise stimmt jedoch nicht mit der Praxis im eigenen Land überein.
3 Lucas, George R. (2017): Ethics & Cyber Warfare. Oxford.
4 Lucas, George R. (2015): „Ethical Challenges of 'Disruptive Innovation': State Sponsored Hacktivism and 'Soft' War.“ In: *Evolution of Cyber Technologies and Operations to 2035.* Hg. von Misty Blowers. [Advances in Information Security, Vol. 63.] Basel, S. 175–184.

ÜBER CYBER, KRIEG UND CYBERKRIEG

Autoren: ***Eneken Tikk und Mika Kerttunen***

Abstract

Eneken Tikk und Mika Kerttunen führen mit kaum verhohlener Ironie in ihren Essay ein. Erstere schildert in einem Prolog ihre Erlebnisse am Tage des großen Cyberangriffs auf Estland im Jahr 2007. Die durch den Ausfall von Regierungs- und Medienseiten hervorgerufene Konfusion erschwerte viele Abläufe – aber schon damals registrierte Tikk mit Befremden die weitgehend kritiklose (und heute zum Allgemeinplatz gewordene) Rede von „Krieg" und „Selbstverteidigung", während die Situation (völker-)rechtlich schwer einzuordnen war.

Mehr als zehn Jahre später nehmen die Autoren eine (immer noch mehr als dringende) Klarstellung vor. Anstatt den Kriegsbegriff inflationär zu gebrauchen und so unter anderem die Schrecken eines tatsächlichen Krieges kleinzureden, vertreten sie eine klar an Clausewitz ausgerichtete Definition des Krieges – unter die sich weder die aktuellen noch die zu erwartenden Cyberaktivitäten subsumieren lassen. Denn diese seien nach wie vor und voraussichtlich auch in Zukunft nicht in der Lage, größeren physischen Schaden anzurichten. Dass das Militär auf der ganzen Welt seine Fähigkeiten zur Kriegführung mit elektronischen Mitteln auf- und ausbaut, stehe dazu nicht im Widerspruch, sondern sei eine logische Folge der zunehmenden Digitalisierung und Vernetzung.

Dennoch, und hier kommen die Autoren zu ihrer Kernaussage, erschöpft sich das Problem gerade nicht in terminologischen Fragen. Das Kriegsgerede mache blind für die eigentlichen riskanten Entwicklungen im Konfliktfeld Cyberraum. Ihr unterschwelliger Charakter lasse Cyberoperationen aller Art als Standardmittel zur Machtprojektion attraktiv erscheinen – gerade für kleinere Staaten und neue Cybermächte. Das verheiße Destabilisierung, die schrittweise Entwertung völkerrechtlicher Grundsätze und eskalatorische Automatismen bis hin zum Risiko eines konventionellen kinetischen Kriegs.

Prolog: Cyberodyssee 2007

Fangen wir mit einer Geschichte vom Krieg an. Ohne Zweifel gibt es Kriegsgeschichten auch im Cyberkrieg. Dies ist Enekens Geschichte:

„Ich habe den ersten Cyberkrieg überlebt. Vielleicht bin ich sogar eine Veteranin. Was Letzteres angeht, bin ich mir allerdings nicht ganz sicher.

Ende April 2007 wurden Cyberbomben auf Estland abgeworfen. Niemand konnte die Bomben sehen oder hören, aber jeder erfuhr davon, als Verteidigungsminister, Parlamentspräsidentin, Justizminister und Ministerpräsident versicherten, dass es sie gebe. Plötzlich waren die Unruhen in den Straßen nebensächlich. Wir waren mit Massenvernichtungswaffen angegriffen worden. Wir lebten in einem Zustand der Blockade. Russland, der riesige Nachbar im Osten, hatte (nun wirklich) zugeschlagen.

Am winzigen Flughafen von Tallinn ging der Flugbetrieb bereits am nächsten Morgen weiter. Ich musste das Flugzeug nehmen – in Brüssel fand eine Konferenz zum Schutz persönlicher Daten statt, und meine Anweisung zur Teilnahme war nicht zurückgenommen worden. Zumindest hatte mich niemand angerufen, um die Reise zu verschieben. Ich hätte auf dem regulären Dienstweg ohnehin keine Weisungen entgegennehmen können, da der Zugang zum Informationssystem der Regierung blockiert war.

Also reiste ich schweren Herzens ab. Was packt man ein, wenn man ein Kriegsgebiet verlässt? Als meine Großeltern während des Zweiten Weltkriegs ihre Heimat verließen, hatten sie die Wertgegenstände der Familie im Garten vergraben. Aber das half mir nicht weiter, weil ich nichts dergleichen besaß. Wertgegenstände, meine ich.

In Brüssel konnte ich mich kaum auf die technokratische Arbeit konzentrieren. Ich versuchte immer wieder, Nachrichten aus Estland zu bekommen, aber vergeblich: Keine Webseite ließ sich öffnen, die Regierungsseiten waren ebenfalls nicht erreichbar. Allerdings erstatteten die Kollegen von der NATO Bericht von unserem Krieg, und auch bei der EU-Kommission gab es kaum ein anderes Thema.

Am Abend dieses Tages, an dem eine Schlagzeile die nächste gejagt hatte, nahm ich ein Taxi zum Flughafen. Nach dem Einchecken fühlte ich mich etwas besser. Es gab immerhin noch ein Land, in das ich zurückkehren konnte. Ich war erleichtert und dankbar. Egal was am kommenden Tag geschehen sollte – gemeinsam mit meiner Familie und meinen Freunden würde ich mich ihm stellen.

Am nächsten Tag im Büro – ich hatte zwei Jobs – merkte ich, was es heißt, in der öffentlichen Verwaltung eines Landes tätig zu sein, das sich im Krieg befindet. Nicht dass etwas mein bisheriges, angenehmes Leben direkt bedroht hätte, aber die Situation war dennoch chaotisch: Ich hatte eine sofortige juristische Einschätzung der Lage zu erstellen, stündliche technische Updates wurden verlangt, ständig kamen neue Themen dazu, die Telefone klingelten ununterbrochen.

Während der Arbeit am Rechtsgutachten wurde mir bewusst, wie schlecht ich darauf vorbereitet war, mit dem Kriegsbegriff zu operieren. Ich war nicht nur unfähig, völkerrechtliche Bestimmungen auf die Lage anzuwenden, sondern musste immer wieder Exkurse in kommunales und nationales Recht, ins Strafrecht und ins Datenschutzgesetz unternehmen – bis hin zu unserem Informationsgesetz, welches das Kopieren Hunderter E-Mail-Adressen von Webseiten der Ministerien und ihr direktes Einfügen in das Programm erleichtert hatte, das nun als Waffe eingesetzt wurde. Ich stieß auf den Kommentar eines Völkerrechtlers, der befand, das Völkerrecht sei auf den Umgang mit der Art Krieg nicht ausgelegt, in dem sich Estland nun befand. Das erschien mir sehr nachvollziehbar. Der Artikel legte allerdings auch nahe, das Völkerrecht müsse weiterentwickelt werden, um für Angriffe aus dem Cyberspace gerüstet zu sein. Dessen war ich mir schon weniger sicher – aber für eine fundierte Einschätzung war ich auch hier nicht tief genug in der Materie.

Auf dem Flur hörte ich den Oberbefehlshaber unserer Streitkräfte sagen, nichts von dem, was vor sich gehe, sei von militärischer Relevanz. Er musste sich geirrt haben. Ich wusste nicht, wie es sich genau verhielt, aber bei dieser Lage konnte es sich eindeutig nur um einen Konfliktfall handeln, da das Verteidigungsministerium involviert war. Das Centre of Excellence der NATO sollte ebenfalls involviert bleiben. Ich sollte involviert bleiben. Der Oberbefehlshaber der Streitkräfte musste also schlicht etwas verwirrt gewesen sein: Wir hatten nun eine ganze andere Art von Krieg zu führen, die es während seiner eigenen Ausbildung noch nicht gab.

Am nächsten Tag war der Krieg vorbei. Die Cyberangriffe wurden bei uns im Zentrum natürlich mit großem Eifer untersucht. Wir Wissenschaftler und Forscher durften plötzlich an zahlreichen Treffen teilnehmen – in Brüssel, Bergen, Redmond, an großen britischen und US-amerikanischen Universitäten und Thinktanks – und unsere Geschichte erzählen. Die Geschichte von einer neuen Art von Krieg.

Bei einer der vielen Konferenzen erwähnte jemand, Estland habe den Bündnisfall nach Artikel 5 des NATO-Vertrags erklärt. Das war mir neu, deshalb wollte ich es prüfen. In der Tat hatte die NATO einen Brief aus Estland erhalten, in dem vor Cyberangriffen gewarnt wurde, die unserer Expertise und besten Einschätzung zufolge wahrscheinlich eine Bedrohung für alle NATO-Staaten darstellten.

‚Wir haben Artikel 5 nicht in Anspruch genommen', notierte ich. Zur Bekräftigung fügte ich hinzu: ‚Kein Land kann sich ohne das Eintreten eines bewaffneten Angriffs auf den Bündnisfall berufen. Einige Staaten definieren den Einsatz von Gewalt als Schwelle, aber der Vorfall in Estland war weit von dieser Schwelle entfernt.'

Anscheinend befand ich mich erneut auf dem Holzweg. Einige Monate später war das Cooperative Cyber Defence Centre of Excellence der NATO (CCDCOE) einsatzbereit, jedoch nicht mit der erforderlichen Mindestanzahl von drei Mitarbeitern, sondern gleich mit sieben! Estland war zum bevorzugten Ansprechpartner beim Thema Cyberverteidigung und Cyberkrieg geworden. Der erste Ausschuss der UN-Generalversammlung nahm sich der Problematik der internationalen Cybersicherheit an. Estland erhielt einen Sitz in der Gruppe der anfangs 15, später 20 und schließlich 25 Experten, die sich mit dem Thema auseinandersetzen sollten.

Als ich Jahre später die Positionen verschiedener Staaten zum Völkerrecht in dieser Frage analysierte, entdeckte ich, dass Russland bis 2006 als einziger Staat das Szenario der Infor-

mations- und Kommunikationstechnologien (IKT) als Kriegsschauplatz bei den UN vorangetrieben hatte. Das geht aus den Akten im Archiv des ersten UN-Ausschusses hervor. Inzwischen ist der Cyberkrieg allgegenwärtig. Oft in ähnlicher Form wie 2007 in Estland. Dennoch erscheint es nicht sinnvoll, das Kriegsrecht auf diese Fälle anwenden zu wollen. Stattdessen sollten wir uns fragen, ob wir nicht auf Resilienz und mehr Cyberhygiene setzen sollten – auch in den Institutionen der Regierung. Denn Cybersicherheit fängt im eigenen Land an.

Merkwürdigerweise fühle ich mich wie eine Veteranin eines Krieges, den es nie gegeben hat, der aber eine neue Vorstellung von Krieg geschaffen hat. Und diese Vision ist nun plötzlich Normalität."

*

Eine Krise sollte man nie ungenutzt verpuffen lassen. Die Saga von 2007 nützte gleichermaßen dem kontrollwütigen Osten, dem operationsversierten Westen, dem unsicheren Süden, dem zaudernden Norden, der allzeit bereitstehenden Industrie und den wohlmeinenden Verfechtern friedlicher Lösungen. Viele äußerten damals sehr nachdrücklich die Meinung, der Cyberkrieg sei bereits in vollem Gange, und führten entsprechende Belege an. Wir schenken diesen Bezeugungen keinen Glauben.

Über Krieg

Selbstverständlich geschehen im Cyberspace schlechte, schädliche und böse Dinge. Kinder werden gemobbt, bloßgestellt und ausgebeutet. Betrug und Diebstahl im Netz scheinen leicht durchführbar und profitabel zu sein, Gewaltvideos sind frei verfügbar, und selbst Staaten, eigentlich die zivilisierten Mitglieder der internationalen Gemeinschaft, betreiben Massenüberwachung und gezielte Informationsbeschaffung (Spionage) und führen teilweise zerstörerische Operationen durch. Aber wollen wir hier wirklich von „Krieg" sprechen?

Natürlich hat es schon viele „Kriege" gegeben. Zwar haben wir hoffentlich das vielfach bemühte Konzept des „Kriegs gegen den Terrorismus" überwunden. Doch mittlerweile ist ein weiterer unsinniger Gedanke, die „hybride Kriegführung", aufgetaucht – nach dem Protokoll- und dem Browserkrieg, dem „Colakrieg" zwischen Coca-Cola und Pepsi Cola und dem Krieg gegen die Fettleibigkeit, den die Menschheit zwar führt, aber sicher verlieren wird. In der Tat wird die Idee des Kriegs, vermutlich ähnlich wie beim „Dschihad", umgangssprachlich oder zur rhetorischen Verstärkung der Argumentation genutzt. Wer aber ständig vom Krieg spricht, bagatellisiert und normalisiert damit den Schrecken eines echten Kriegs. Wenn überall Krieg herrscht, reduziert sich das menschliche und gesellschaftliche Leben auf einen Zustand permanenten Konflikts. Doch in jedem Fall gilt: Sollten wir ernsthaft an einen andauernden oder lauernden Krieg im Cyberspace glauben, müssen wir uns konsequenterweise auch darauf vorbereiten, ihn zu führen. Das haben viele Regierungen bereits vorgeschlagen.

Wir raten dringend an, nur dann von Krieg zu sprechen, wenn ein Staat organisierte Gewalt gegen einen anderen Staat oder eine politisch organisierte Einheit richtet. Die Wortwahl spielt eine geringere Rolle als die Idee dahinter. Krieg ist immer organisiert. Genauer gesagt sind Kriegführung und die damit verbundenen Handlungen grundsätzlich organisiert und zielgerichtet, politisch motiviert, systemisch und systematisch. Krieg ist inhärent gewaltsam: Er führt zu Tod und Zerstörung. Krieg spielt sich grundsätzlich zwischen Staaten ab; Einzelpersonen, die Gewalt anwenden, sind Kriminelle. Man kann Krieg auch als Phänomen begreifen, das im bewaffneten Kampf zwischen Staaten sichtbar wird. Dennoch folgen die strukturellen und phänomenologischen Annäherungen derselben Logik.

In *Bürgerkriegen* (sic!), der *Intifada* und im Fall von Aufständen und Befreiungskriegen hingegen ist eine der kämpfenden Parteien ein Staat und die andere eine organisierte Gruppe, die nicht unbedingt den formellen Status eines Staates hat, aber als politische Einheit handelt. Die politische Natur von Befreiungs*fronten, -armeen* und *-organisationen,* ja sogar von Befreiungsstämmen, ist offensichtlich: Dafür braucht es kein Parlament oder Parteien, sondern Wünsche, konkrete Ziele sowie Mittel und Maßnahmen, um diese Ziele zu erreichen. Harold Lasswells 1936 erschienenes Buch verdeutlichte dies schon im Titel: *Politics. Who Gets What, When, How* (Politik. Wer was wann wie bekommt; eige-

ne Übersetzung). Wenn eine politisch organisierte und motivierte Einheit mit systematischer, organisierter Gewalt, die Tod und Zerstörung zur Folge hat, gegen eine ähnliche Einheit vorgeht, dann, seien wir ehrlich, ist das ein Krieg – selbst wenn das Völkerrecht anderer Ansicht ist. Im völkerrechtlichen Sinne wurden allerdings seit dem Koreakrieg (der übrigens formal nie beendet wurde) nur sehr wenige Kriege geführt.

Wir vertreten hier die Clausewitz'sche Auffassung von Krieg. Auch wenn er sich, entsprechend dem berühmten Chamäleonvergleich, immer wieder in neuen Farben und Strukturen zeigt, ist und bleibt Krieg doch vom Wesen her gewalttätig, ungewiss und zielgerichtet. Die gegenwärtigen und für die Zukunft zu erwartenden Aktivitäten und Einsätze im Cyberspace erfüllen diese Kriterien nicht, selbst dann nicht, wenn Staaten sie ausführen.

Über Cyber

Cybereinsätze haben bislang keine großflächigen Zerstörungen angerichtet. Zwar wurde die Kommunikation blockiert, die Stromversorgung unterbrochen, Websites wurden verunstaltet, Informationen vernichtet und industrielle Prozesse aufgehalten. Es hat finanzielle Verluste und Identitätsdiebstahl gegeben. Doch keine Stadt wurde bislang in Schutt und Asche gelegt. Vor allem sind Menschen bislang nicht an Leib und Leben zu Schaden gekommen. In der Tat ist fast jede andere Aktivität des Menschen potenziell tödlicher als Operationen im Cyberspace.

Vor allem werden deren übliche Folgen, von verschiedenen Manipulationen über die Blockierung von Zugangsrechten bis hin zur Vernichtung von Informationen und Systemen, kaum dazu führen, dass Staaten in den Krieg ziehen. Operationen im Cyberspace bedrohen weder die Existenz von Staaten, noch rütteln sie am Gleichgewicht der Mächte. Zudem haben sie nicht die umfassenden, langfristigen und entscheidenden Folgen, wie sie militärische Einsätze, also Krieg im eigentlichen Sinne, anvisieren und erreichen können. Im Kontext der brutalen Realität politischer Entscheidungsfindung geht es beim Cyberangriff nicht um die Inkaufnahme von Tod und Zerstörung, sondern um das Ausmaß gewaltsamer, zerstörerischer und schmerzhafter Wirkungen.

Warum entwickeln dann so viele Nationen dennoch cybermilitärische Fähigkeiten? Warum schaffen sie cyberspezifische Einheiten und Kommandos, bilden Personal für Cyberoperationen aus und führen Krieg im Cyberspace? Zum Beispiel überarbeiten die USA seit 2012 systematisch ihre nationalen Strategien, gemeinsamen Militärdoktrinen und Feldhandbücher, um cyberspezifische Fähigkeiten als wesentlichen Bestandteil aller militärischen Operationen und Funktionen zu verankern. Dazu würde auch die Stationierung von Cybereinheiten und -teams bei den taktischen Landstreitkräften, möglicherweise bis hin zu den Manöverbrigaden, gehören, sodass cyberspezifische Fähigkeiten in die volle Bandbreite militärischer Operationen integriert würden. Russland und China sind ebenfalls dabei, Instrumente der Informationskriegführung in ihre Streitkräfte einzugliedern. Die angeblich so friedlichen Skandinavier bauen Kapazitäten für die Cyberkriegführung auf, und sogar Estland, ein Land mit lediglich rund einer Million Einwohnern, verfügt seit November 2018 über ein eigenes Cyberkommando. Ist das nun *Militarisierung?*

Die gegenwärtigen und zu erwartenden Aktivitäten und Einsätze im Cyberspace erfüllen nicht die Kriterien eines Kriegs

Die Streitkräfte stehen von jeher beim Einsatz aktueller Informations- und Kommunikationstechnologien an vorderster Front. Computer wurden ursprünglich zum Rechnen genutzt. Doch bereits in den 1950er Jahren wurden Überwachungsstationen, Kommandoposten sowie Feuer- und Manövereinheiten miteinander vernetzt. Im Anschluss an die Kubakrise richteten die USA ein (schlecht funktionierendes) „weltweites Militärkommando- und Kontrollsystem" ein. Die Digitalisierung hat die Zielgenauigkeit in diesem Bereich erhöht. Zurzeit bringen die meisten Streitkräfte ihre Kommando- und Kontrollsysteme sowie Waffensysteme auf den modernsten Stand der Technik. Auf der Suche nach mehr Effektivität integrieren die am weitesten Fortgeschrittenen ihre Systeme und Netzwerke. Intelligente und vernetzte Technologien werden auf alle militärischen Funktionen angewendet,

auf die administrativen ebenso wie auf potenziell tödliche. Überall geht es darum, Daten und Netzwerke zu schützen.

Mit Sicherheit kommen cyberspezifische Fähigkeiten in allen Konflikten unserer Zeit zum Einsatz. Regierungen nutzen Cybermethoden auch für Spionage in Politik und Wirtschaft. Einigen wird nachgesagt, dass sie außerdem kriminell im Netz agieren. Ein konzeptuell korrekter und faktisch präziser Begriff, der das Entwickeln, Stationieren und Anwenden von IKT und cybermilitärischen Fähigkeiten beschreibt, wäre die Bezeichnung Cyberkriegführung als Kombination von Wegen und Mitteln, Methoden, Fähigkeiten, Instrumenten und deren Einsatz.

Dass die Operationen im Cyberspace genau nicht die Definition von Krieg erfüllen, macht sie so lukrativ und gefährlich zugleich. Einige sehen diese Operationen als neue Standardform der Machtprojektion. Manche Länder sind offenkundig stolz auf ihre cyberspezifischen Fähigkeiten und Operationen, möglicherweise in der Annahme, diese seien frei von Risiken. Das Gegenteil ist der Fall.

Konflikte und Auseinandersetzungen sind trotz aller Digitalität niemals per se virtuell, sondern grundsätzlich politisch und real. Selbst die reinste Form, die verklärendste Vorstellung von Cybereinsätzen – der Schlagabtausch mittels virtueller Geschosse und hitziger Softwaregefechte –, findet weder im luftleeren Raum noch mit Lichtgeschwindigkeit statt.

Gepaart mit den realen Gegebenheiten der Operationen im Cyberspace, führt die Logik des Kriegs und der Politik zu einer paradoxen Situation:

Solange Cybereinsätze lediglich eine relativ geringe, temporäre und sekundäre Wirkung erzielen, überschreiten sie nicht die Schwelle zum Krieg. Der (wenn auch unwahrscheinliche) Fall einer digitalen Operation mit ernsthaften existenziellen oder zerstörerischen Auswirkungen dagegen würde die Situation eskalieren lassen und zu herkömmlichen politischen und militärischen Konflikten und Kriegen führen.

Statistisch gesehen, handelt es sich bei fast allen nachweislich oder mutmaßlich von staatlicher Hand gesteuerten Cyberangriffen um Spionage. Zudem sind einige Dutzend weiterer Vorfälle dokumentiert, die jedoch nur relativ geringfügige Schäden anrichteten: Verunstaltung von Websites, Blockierung von Diensten, Manipulation sowie in sehr wenigen Fällen Vernichtung von Daten, Sabotage und materielle Schäden. Dieses Lagebild ist also weit von einem Kriegsszenario entfernt.

Das wahre Problem

Wir sind derart auf die Idee des Cyberkriegs fixiert, dass wir übersehen, was sich *tatsächlich* abspielt. Die zunehmende Militarisierung im digitalen Raum betrifft nicht nur bekannte, etablierte Mächte, denen der Cyberspace sogar Möglichkeiten bieten könnte, Todesopfer und Zerstörung zu vermeiden. Vielmehr ist rund um den Globus das Entstehen völlig neuer operativer Einheiten zu beobachten – in der EU insbesondere in Estland, den Niederlanden und Polen.

Das Erscheinen von Cyberneulingen auf der Bühne der globalen Konflikte ist besorgniserregend und stellt eine potenzielle Destabilisierung dar. Ihre Präsenz zeugt vom Verlangen, durch Machtprojektion Relevanz zu erlangen. Obwohl den neuen Cybermächten bewusst ist, dass sie sich durch die Entwicklung und Nutzung dieser Fähigkeiten gegenüber ihren Kontrahenten exponieren, lassen sie ihre operativen Bestrebungen die Oberhand über ihre rechtsstaatlichen Verpflichtungen gewinnen. Auf den ersten Blick geht es um Nichtigkeiten, um winzig kleine Eingriffe in puncto Souveränität oder gebührende Sorgfaltspflicht. Diese Einschnitte schlagen jedoch ernste Wunden in die völkerrechtlich begründete öffentliche Ordnung. Wer sich dazu aufschwingt, einem Staat das Recht auf die eigene Souveränität abzusprechen, spricht es automatisch allen anderen Staaten ab.

Die Entwicklung neuer operativer Fähigkeiten treibt das Perpetuum mobile der politischen Spannungen an und kann leicht zu unerwünschter oder unerwarteter Eskalation führen. In keinem Fall lässt sich vorhersagen, wie diese neu entstandenen Mächte reagieren werden oder inwieweit die neuen Cybermächte politischer Manipulation und Provokation standhalten können. Während wir also fasziniert den Cyberkrieg verfolgen, der keiner ist, verpassen wir genau die Entwicklungen, die zu einem tatsächlichen Konflikt führen könnten.

Cybereinsätze durchzuführen ist eine riskante Angelegenheit. Das Klima eines Cyberkonfliktes und dessen (falsche) Wahrnehmung destabilisieren das empfindliche Gleichgewicht zwischen Normalität und Krise zusätzlich. In einem Cyberkonflikt sind politische Entscheidungen oft durch ein Gefühl von Dringlichkeit, das vorrangige Gebot der hard security und den Irrtum motiviert, auf diese Weise mächtig zu erscheinen. Schließlich werden Entscheidungen mitten in einem Dickicht aus Fehlinformation, Fehleinschätzungen, Unsicherheit und Angst getroffen. In ihren Übungen zelebrieren Staaten und Organisationen einen eskalierenden Sprachgebrauch, flankiert durch entsprechende Maßnahmen. Es scheint kaum möglich, an Deeskalation überhaupt nur zu denken. Dabei ist genau das nötig.

Wir alle hoffen, dass diese Zeiten niemals kommen werden. Vermutlich hoffen wir vergebens. Niemand weiß, wie viele Schnitte die internationale Ordnung noch verkraften kann, bevor sie endgültig ausblutet. Menschenrechte, Rechtsstaatlichkeit und das Leitmotiv des Friedens bleiben im Spiel um die Macht im Cyberspace außen vor. Dieser Voluntarismus fördert den Mangel der Staatengemeinschaft an Verantwortungssinn zutage. Er unterstreicht, dass Staaten im Gegensatz zu sozialen Gemeinschaften nicht durch eine gemeinsame Identität oder gemeinsame Werte gebunden sind. Stattdessen zeigt er, dass der einzige gemeinsame Nenner zwischen Staaten in ihrer politischen Identität besteht. Die Aussicht auf irgendeine Art von internationalem Kontrollregime bleibt schiere Utopie.

Dies führt uns zu einer weiteren Unsinnigkeit: freiwillige, nicht bindende Normen verantwortlichen staatlichen Handelns. Sie sind das Placebo, das der internationalen Gemeinschaft als Ersatz zum Völkerrecht angeboten wird. Da gegenwärtig kein Krieg zwischen den USA und der Russischen Föderation ins Haus steht, können es sich beide leisten, im Ballsaal der Schrankenlosigkeit ein Tänzchen miteinander zu wagen. Derart eng umschlungen, fühlen sie sich viel zu wohl und sicher, um sich mit dem überwältigenden Mangel an Resilienz, Umsicht und Verantwortlichkeit abzugeben, der überall auf der Welt lauert. So bieten die immer längeren Listen neuer Cybermächte dem einen potenzielle neue Verbündete, dem anderen potenzielle Ausreden … bis es zu spät ist.

Die Welt schien inzwischen so friedlich geworden zu sein, dass viele Staaten es sich erlaubt haben, ihre Schutzschilde sinken zu lassen. Doch die Informations- und Kommunikationstechnologien können wirklich zur Gefahr werden, wenn wir ihre Entwicklung und Nutzung nicht ernst genug nehmen. Diese Gefahr besteht allerdings nicht in einem Cyberkrieg, sondern in einem echten Krieg. In der Art von Krieg, für die das humanitäre Völkerrecht geschaffen wurde.

Bücher

Clausewitz, Carl von (1991 [1832]): *Vom Kriege.* Köln.

Lasswell, Harold (1936): *Politics. Who Gets What, When, How.* New Haven.

Libicki, Martin C. (2012): *Crisis and Escalation in Cyberspace. Santa Monica.* https://www.rand.org/pubs/monographs/MG1215.html (Stand: 20. Mai 2019).

Rid, Thomas (2018): *Mythos Cyberwar.* Hamburg.

Skinner, Quentin/Stråth, Bo (2003): *States and Citizens.* Cambridge.

Tikk, Eneken/ Kerttunen, Mika (2018): *Parabasis: Cyber-diplomacy in Stalemate.* Oslo. http://hdl.handle.net/11250/2569401 (Stand: 20. Mai 2019) .

Tikk-Ringas, Eneken (2016) (Hg.): *Evolution of the Cyber Domain.* Abingdon.

Artikel

Arquilla, John/Ronfeldt, David (1993): „Cyberwar is Coming!" In: *Comparative Strategy* 12 (2), S. 141–165.

Kerttunen, Mika (2018): „Cyber Warfare – from Science Fiction to Reality". In: *Sicherheit und Frieden* 36 (1), S. 27–33.

Libicki, Martin C. (2015): „The Cyberwar that Wasn't". In: Geers, Kenneth (Hg.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, S. 49–54. https://ccdcoe.org/uploads/2018/10/Ch05_CyberWarinPerspective_Libicki.pdf (Stand: 20. Mai 2019).

Raitasalo, Jyri (2019): „America's Constant State of Hybrid War". In: *The National Interest,* https://nationalinterest.org/feature/americas-constant-state-hybrid-war-48482 (Stand: 20. Mai 2019).

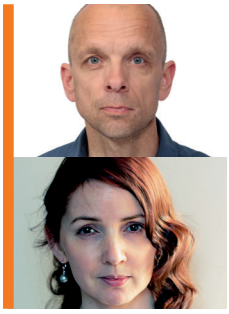
Sonstiges

Council on Foreign Relations: „Cyber Operations Tracker". https://www.cfr.org/interactive/cyber-operations (Stand: 20. Mai 2019).

NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/ (Stand: 20. Mai 2019).

Die Autoren

Dr. Mika Kerttunen und Dr. Eneken Tikk sind Gründer und Direktoren des Cyber Policy Institute (Institut für Cyperpolitik) sowie Forscher an der Technischen Universität Tallinn. Beide verfügen über langjährige Erfahrung in den Bereichen Cyberdiplomatie und Hilfe zur Selbsthilfe, unter anderem als Berater für die (finnischen beziehungsweise estnischen) nationalen Experten der UN-Gruppe von Regierungsexperten für Entwicklungen im Bereich Information und Telekommunikation im Kontext der internationalen Sicherheit.



RISKANTE KRIEGSSPIELE

WARUM WIR IM CYBERWAR NUR VERLIEREN KÖNNEN

Autorin: ***Anke Domscheit-Berg***

Abstract

Sosehr das Internet in sämtliche Lebensbereiche der Moderne Einzug gehalten hat, so schwer erscheint es vorstellbar, dass es ursprünglich eine militärische Entwicklung war, die im Jahr 1968 einige wenige Computer miteinander vernetzte. Anke Domscheit-Berg ruft dem Leser dies in Erinnerung, um dann festzustellen, dass heute unter dem Begriff der „aktiven Cyberabwehr" eine Remilitarisierung des Internets erkennbar ist. Der Cyberraum werde zum Kriegsgebiet, und die Waffenarsenale würden um Cyberwaffen ergänzt. Gleichzeitig unterliegen die Menschen weltweit der Überwachung durch Geheimdienste, wie wir seit den Enthüllungen Edward Snowdens wissen.

Als ein normales Mittel moderner Verteidigung verharmlost, werden auch in Deutschland Forderungen einer „aktiven Cyberabwehr" sowie nach staatlichen „Hackbacks" immer lauter. Dabei, so die Autorin, seien solche Instrumente mit dem Grundgesetz nicht vereinbar. Hinzu kommt, dass die Eskalationsgefahr solcher Maßnahmen massiv unterschätzt würde: Unbeteiligte Personen können allzu leicht in Mitleidenschaft gezogen werden. Eine Trennung zwischen zivilen und militärischen Zielen ist im Cyberspace äußerst schwierig.

Daher gebe es nur einen Weg, unser aller Sicherheit im digitalen Zeitalter zu verbessern, nämlich für möglichst sichere Soft- und Hardware zu sorgen. Dem jedoch stünden die Begehrlichkeiten der Geheimdienste und des Militärs im Wege, die Überwachungsmöglichkeiten und Cyberangriffskompetenzen hoch priorisieren. Neu identifizierte Schwachstellen in Soft- und Hardware würden deshalb systematisch und im Geheimen offengelassen. Auf diese Weise werde der Staat selbst zum Sicherheitsrisiko.

Schließlich plädiert Domscheit-Berg für Transparenz in der Entwicklung von Soft- und Hardware sowie für umfassende digitale Bildung – denn der Mensch sei immer noch „eine der größten Schwachstellen".

Die Wurzeln des Internets gehen zurück in das Jahr 1968, als im Auftrag der US-Luftwaffe die Entwicklung des Computernetzwerkes ARPANET in Kooperation zwischen Verteidigungsministerium und dem Massachusetts Institute of Technology begann. ARPANET vernetzte anfangs eine Handvoll Forschungseinrichtungen, die für das US-Militär tätig waren. Die Vernetzung von Computern und die Übermittlung von Informationen, die in kleine Datenpakete zerteilt wurden, bildeten das Grundprinzip, nach dem auch heute noch das Internet funktioniert. Gefördert wurde das ARPANET von der DARPA, der Defense Advanced Research Projects Agency, die dem US-Verteidigungsministerium unterstellt ist und deren Hauptaufgabe die Förderung militärisch nutzbarer Forschungsaktivitäten ist, mit dem Schwerpunkt auf Grundlagenforschung. Die DARPA wurde schon Ende der Fünfzigerjahre gegründet und verfügt inzwischen über ein jährliches Budget von mehr als drei Milliarden Dollar.[1] Einige der von DARPA geförderten Forschungen prägen heute die digitale Welt, wie beispielsweise das Internetprotokoll TCP/IP oder die Erfindung der Computermaus, andere flossen ein in die Raumfahrt, wie die Entwicklung von Satelliten, sehr viele wurden militärisch genutzt, von der Luftwaffe (zum Beispiel Ortungsschutz für Flugzeuge, Drohnen) über die Marine (U-Boot-Abwehr, Unterwasserdrohnen) bis hin zu sonstigen Streitkräften (M16, Antipanzerwaffen, Helmdisplays, autonome Waffen, Feldroboter).[2]

Von der Militärtechnologie zur digitalen Gesellschaft

In den nächsten Jahrzehnten entstand das, was wir heute als Internet bezeichnen. Es vernetzte zuerst vor allem Wissenschaftler*innen. Erst 1994 nutzten mehr Menschen das Internet kommerziell als im Rahmen einer wissenschaftlichen Tätigkeit. Seitdem hat sich das Internet von seinen militärischen Wurzeln emanzipiert, es wurde zur Grundlage der digitalen Gesellschaft, zum Ausgangspunkt einer digitalen Revolution. Neue Geschäftsmodelle entstanden und mit ihnen unzählige kleine, aber auch un-

vorstellbar große und mächtige Unternehmen, jene, die wir heute als GAFA bezeichnen – die Quasimonopole von Google, Amazon, Facebook und Apple. Das Wissen der Welt wurde mit einem Mausklick erreichbar, Milliarden Menschen konnten sich vernetzen und direkt miteinander kommunizieren. Im Jahr 2019 hat Facebook 2,3 Milliarden Nutzer*innen, auf YouTube teilten oder konsumierten 1,9 Milliarden Menschen Videos, auf WhatsApp schickten sich 1,5 Milliarden Menschen Chatnachrichten, Bilder oder Videos.[3] Ein Smartphone hat heute mehr Rechenleistung als die NASA-Apollo-Mondmission, es könnte 120 Millionen Apollos gleichzeitig zum Mond fliegen.[4] Egal, welchen Aspekt man betrachtet, wir bewegen uns zunehmend in Dimensionen, die man sich kaum vorstellen kann. Im Jahr 2022 werden etwa 4,8 Zettabytes Daten über das Internet übertragen.[5] Ein Zettabyte sind 1000 hoch sieben Bytes, das entspricht einer Trillion Gigabytes oder einer Eins mit 21 Nullen dahinter. Während Datenmengen und vernetzte Geräte exponentiell wachsen, fallen die Preise in den Keller: Ein Gigabyte Speicherplatz kostete 1981 noch 500.000 US-Dollar, im Jahr 2017 waren es nur noch 3 Dollar-Cent.[6]

Die Remilitarisierung des Cyberraums

In dieser vernetzten Gesellschaft der Big Data erfolgt seit einiger Zeit eine wahrnehmbare Remilitarisierung. Der Cyberraum wird zum Kriegsgebiet, das Waffenarsenal wird um Cyberwaffen ergänzt, die Begehrlichkeiten der Geheimdienste sind nicht nur gewachsen, sondern werden in beunruhigendem Maßstab umgesetzt. Dank NSA-Whistleblower Edward Snowden haben wir alle durch ein unerwartet geöffnetes Fenster einen Blick in eine sonst verschlossene Welt werfen dürfen und einen Eindruck vom schier grenzenlosen Ausmaß der globalen Überwachung des Internet- und Kommunikationsverkehrs durch US-Geheimdienste erhalten. Wir alle erinnern uns an die Monate, in denen eine Schockwelle nach der anderen durch die Medien rollte, weil immer wieder neue, unvorstellbare Dimensionen der Spionage aufgedeckt wurden, die neben der Wirtschaftsspionage unter eigentlich befreundeten Staaten selbst das Abhören von Angela Merkels Handy umfassten, aber auch eine Verquickung deutscher Geheimdienste offenbarten. Untersuchungsausschüsse befassten sich in der Folge mit der Aufklärung, führten aber nicht dazu, dass illegale Überwachungsmaßnahmen zu juristischen oder personellen Konsequenzen führten, sondern zu einer nachträglichen Legalisierung,[7] etwa der maßlosen Anzapfung des größten deutschen Internetknotens DE-CIX in Frankfurt/Main.

Immer häufiger ist von „aktiver Cyberabwehr" die Rede, die eben keine Verteidigung mehr ist, sondern ein Angriff

Ganz offensichtlich hat hier die parlamentarische Kontrolle völlig versagt, was nicht zuletzt daran liegt, dass sie strukturell nicht funktionieren kann; dafür sind die Kräfteverhältnisse zu ungleich. Immer neue Begehrlichkeiten werden bekannt, Polizeigesetze werden ausgeweitet, neue Cyberinstitutionen geschaffen, es ist immer häufiger die Rede von „aktiver Cyberabwehr", die eben keine Verteidigung mehr ist, sondern ein Angriff, auch wenn er sich Gegenangriff nennt. Bundesinnenminister Seehofer forderte mehrfach diese Option in Form eines staatlichen „Hackbacks", die völkerrechtswidrig wäre und auch mit dem Grundgesetz nicht vereinbar ist, denn Gefahrenabwehr ist Ländersache und nicht Aufgabe von Geheimdiensten, Militär oder anderen Institutionen des Bundes. Es ist hochgradig irritierend, dass selbst der Präsident des BSI, Arne Schönbohm, die Möglichkeit eines Hackbacks fordert,[8] denn das Bundesamt für Sicherheit in der Informationstechnik ist ausschließlich zuständig für mehr IT-Sicherheit, für Prävention und Hilfsmaßnahmen bei Hackerangriffen.

Der Staat wird zum digitalen Angreifer

Ein staatliches „Zurückhacken" ist nicht das Gleiche wie ein konventioneller militärischer Gegenschlag im Falle eines Angriffs. Ein Problem ist die mangelhafte Attributionsmög-

lichkeit, also die sichere Identifikation eines Angreifers. Bei einer Langstreckenrakete lässt sich recht sicher ermitteln, aus welchem Land sie gestartet wurde, bei einem Hackerangriff ist das nicht möglich. Kein Geheimdienst der Welt kann mit 100-prozentiger Sicherheit sagen, woher ein Cyberangriff kam. Zu vielfältig sind die Möglichkeiten der Verschleierung, zu häufig werden falsche Fährten gelegt, „Handschriften" bekannter Hackergruppen imitiert, fremde Server für Angriffe genutzt, ohne dass deren Besitzer eine Ahnung davon haben. Man kann bestenfalls Hinweise und Verdachtsmomente haben, sicher sein kann man sich nicht.

Das Spiel mit dem Feuer ist potenziell gefährlicher als ein Nuklearkrieg

Stellen wir uns einfach mal vor, ein derartiger Hackback wird ausgeführt und ein Server im Ausland mit Schadsoftware aus Deutschland angegriffen, weil man glaubt, dass er sich in der Hand von Tätern befindet. Aber was, wenn es ein Server in einem Krankenhaus ist? Oder in einer Behörde? Was, wenn man Schulen oder Stromversorger damit lahmlegt? Was würde ein solcher Angriff bedeuten, wenn man zwar das richtige Land im Visier hatte, aber die Täter Kriminelle waren, die im Auftrag eines anderen Landes oder ganz unabhängig agierten? Was, wenn man solche Server in einem Drittland angegriffen hat, das rein gar nichts mit der ganzen Angelegenheit zu tun hatte? Wer sich dieses irrwitzige Vorgehen einmal bei konventioneller Kriegführung vorstellt, merkt schnell, wie gefährlich und absurd ein solcher Ansatz ist. Wir bombardieren ja auch nicht ein Drittland, weil ein terroristischer Einzeltäter oder Angehöriger einer Terrorgruppe aus diesem Land kommt („mutmaßlich") oder auf seinem Weg zum Terroreinsatz nur durch dieses Land gereist ist.

Ein derartig angegriffenes Drittland könnte den unberechtigten Hackback feststellen und vielleicht auf die Idee kommen, dass er von Deutschland ausgeführt wurde und das seinerseits als Angriff interpretieren, vor allem dann, wenn aus Versehen eine kritische Infrastruktur getroffen wurde oder wenn der Hackback außer Kontrolle geraten ist, weil die für den Angriff genutzte Schadsoftware sich weiterverbreitet hat. Schon könnte eine Eskalationsspirale in Gang gesetzt werden, die keineswegs auf zwei Länder oder den Cyberraum begrenzt sein muss. Dieses Spiel mit dem Feuer darf nicht einmal in Gedanken gespielt werden, es ist potenziell gefährlicher als ein Nuklearkrieg. Wer diesen Vergleich übertrieben findet, sollte darüber nachdenken, was alles heute miteinander vernetzt ist, wo überall Software installiert ist, in welchen gesellschaftlichen Bereichen und in welchen Branchen es zu dramatischen Konsequenzen käme, wenn es zu Teil- oder Totalausfällen der IT käme. In Krankenhäusern, bei Verkehrsleitsystemen, Stromnetzen und Kraftwerken, in Behörden und vielen Unternehmen wäre das eine große Katastrophe. Wenn der Cyberspace, der alle diese zivilen Institutionen umfasst, zum Kriegsschauplatz wird, gibt es keine Trennung mehr zwischen zivilen und militärischen Beteiligten an einer Auseinandersetzung. Es würde viele zivile Opfer geben, und der Konflikt könnte rasend schnell eskalieren und sich ausbreiten, denn das Internet kennt keine nationalen Grenzen.

Leider fehlt uns offensichtlich noch die Erkenntnis, dass der einzige Spielzug, mit dem man einen Cyberwar gewinnen kann, die Entscheidung ist, diese Art Kriegsspiel gar nicht erst zu beginnen – so wie es der Simulationscomputer für einen potenziellen Nuklearkrieg seinerzeit im Film *War Games* so anschaulich errechnete.

Gefahren gehen aber nicht nur von einem staatlichen Hackback aus, denn alle möglichen Akteure, nicht staatliche und staatliche, können aus kriminellen Absichten oder zum Zwecke der Überwachung Schadsoftware in die Welt setzen und damit unser aller Sicherheit kompromittieren. Anders als bei Atomwaffen, die sich nur in der Hand weniger Länder befinden, deren Anschaffung durch weitere Länder sanktioniert ist und deren Herstellung so viele Ressourcen erfordert, dass die Hürden dafür sehr hoch liegen, gibt es keine umfassende Ächtung von Cyberwaffen oder digitalen Waffen, und die für ihre Entwicklung benötigten Ressourcen sind um Magnituden kleiner. Die Gefahr ist groß,

weil Angriffe viel leichter und gleichzeitig ihre potenziellen Auswirkungen viel größer geworden sind. Es ist vorstellbar, dass Hackerangriffe uns quasi in das Mittelalter zurückkatapultieren, wenn die Büchse der Pandora einmal geöffnet ist.[9] Die Bedrohung für unsere Zivilisation als Ganzes ist vergleichbar mit den Folgen des Klimawandels, nur noch schlechter vorhersagbar.

Es kann nur eine einzige sinnvolle Schlussfolgerung aus dieser Erkenntnis gezogen werden: Wir müssen alles dafür tun, unsere IT-Systeme sicherer zu machen. Stattdessen begegnet uns eine Maßlosigkeit, die ethische Grenzen vermissen lässt und den Blick für das Ganze verliert. Wie die Snowden-Enthüllungen zeigen, sehen Geheimdienste zuallererst die Überwachungspotenziale, die ihnen eine digitalisierte Gesellschaft bietet. Sie stellen sich vor, wie schön es wäre, wenn sie nicht nur Telefone abhören könnten, sondern auch virtuelle Assistenten wie Alexa oder Siri, wenn sie das Internet der Dinge anzapfen und Kühlschränke, Toaster und Waschmaschinen aushorchen könnten, sie wünschen sich eingebaute Überwachungssoftware in Autos, damit sie nicht nur verfolgen können, wann sich jemand von A nach B bewegt, sondern auch, mit wem man im Auto sitzt und worüber man redet.[10]

Staatliche Überwachungsfantasien

Ich bin in der DDR aufgewachsen, ich habe die Stasi noch erlebt. Als ich Studentin war, wurden meine Briefe geöffnet, mein Wohnheimzimmer mit der Schreibmaschine darin durchsucht. Ich lebte im Bewusstsein, überwacht zu werden, und weiß aus eigenem Erleben, dass es keine Freiheit mit Überwachung geben kann, denn wer überwacht wird, ist nicht frei. Massenüberwachung ist mit einer Demokratie nicht vereinbar. Sie ist das Werkzeug totalitärer Systeme, die dadurch ihre Existenz verlängern wollen, dass sie ihre Bevölkerung kontrollieren. Geheimdienste aller Länder haben aber das inhärente Bedürfnis, immer mehr wissen zu wollen, möglichst viele Daten zu sammeln und auszuwerten, auch wenn sie sich in einem demokratischen Land befinden. Ihr Wunschtraum ist eine transparente Bevölkerung bei möglichst vollständiger eigener Obskurität. Wie der Teufel das Weihwasser scheuen sie daher parlamentarische Kontrolle, die ein notwendiges Sicherheitsnetz für unsere Demokratie ist und den Zweck hat, klare Grenzen für geheimdienstliche Aktivitäten zu ziehen, die sich an unseren demokratischen Werten orientieren. Dass es sich bei dieser Beschreibung nicht um eine Orwell'sche Wahnvorstellung handelt, zeigen die Aktivitäten der NSA nur zu deutlich. Auch Massenüberwachung hat heute ein ganz anderes Gefahrenpotenzial als zu Stasi-Zeiten, wo die Welt noch weitgehend analog funktionierte, als es weder Facebook noch WhatsApp gab, keine Cookies auf Webseiten und kein Internet der Dinge.

Massenüberwachung ist mit einer Demokratie nicht vereinbar. Sie ist das Werkzeug totalitärer Systeme

Neben den Geheimdiensten wachsen aber auch die Begehrlichkeiten des Militärs in Deutschland, und immer häufiger arbeiten sie Hand in Hand, mitunter sogar zusammen mit der Polizei. So wurde 2017 die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) gegründet, eine neue Einrichtung, die auf dem Gelände der Bundeswehr in München ihren finalen Sitz haben wird, zu deren Hauptaufgaben das Brechen von Verschlüsselungen, das Ausforschen von sozialen Netzwerken in Echtzeit und die Telekommunikationsüberwachung gehören und in deren Beirat Bundespolizei, BKA, BND, das Bundesamt für Verfassungsschutz und der Militärische Abschirmdienst gemeinsam über das Arbeitsprogramm bestimmen.[11] Diese Zusammensetzung verletzt das Trennungsgebot zwischen Polizei und Geheimdiensten, das es seit den Erfahrungen mit der Gestapo aus der Nazizeit gibt. Eine parlamentarische Kontrolle der ZITiS ist praktisch unmöglich, denn sie unterliegt nicht den im Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit geregelten Zuständigkeiten des Parlamentarischen Kontrollgremiums (PKGrG), aber auch nicht der allgemeinen parlamentarischen Kontrolle:

Die Beantwortung konkreter Fragen der Linksfraktion im Bundestag wurde abgelehnt, weil die erfragten Informationen nicht einmal als eingestufte Verschlusssachen in der Geheimschutzstelle des Bundestages hinterlegt werden könnten.[12] So befindet sich die die ZITiS in einer Kontrolllücke. Die Verquickung mit dem Militär ist auch daran erkennbar, dass die Behörde Studienförderungen an der Universität der Bundeswehr anbietet.

Bis 2020 sollen bei ZITiS 400 Mitarbeiter*innen angestellt sein. Der Markt für Cybersecurity-Expert*innen ist leergefegt, was ein zusätzliches Sicherheitsproblem darstellt. So wurden im Oktober 2018 die ersten 81 Stellen bei der ZITiS besetzt, aber drei von vier eingestellten Personen waren aus anderen Behörden abgeworben worden, nur jeder Vierte kam vom „freien Markt". Die ZITiS bietet im Durchschnitt höhere Gehälter als andere Behörden. So liegen Anfang 2019 veröffentlichten Stellenanzeigen[13] zufolge die Einstiegsgehälter im Bereich Telekommunikationsüberwachung[14] über denen des BSI.[15] Wenn Cybersicherheitsexpert*innen in einer auf Angriff ausgelegten Behörde besser bezahlt werden als bei einer Behörde, deren Aufgabe die Verteidigung ist, kann man sich vorstellen, was passiert und welche Konsequenzen das für die Qualität unserer Verteidigungskompetenzen hat.

Die wachsenden Risiken in einer digitalisierten Gesellschaft werden wir nicht beherrschen können, wenn wir uns nicht vollständig auf die Verteidigung konzentrieren

Ein weiteres Beispiel für die Militarisierung des Cyberraums in Deutschland ist die Schaffung der Cyberagentur (vormals ADIC). Diese Agentur für Innovation in der Cybersicherheit wird 2019 im Raum Halle-Leipzig gegründet und soll etwa 100 Mitarbeiter*innen umfassen. Die Bundesregierung sagt ganz klar, dass die Funktionsweise der Einrichtung zur Förderung von Cybersicherheitsforschungsprojekten sich an der DARPA in den USA orientieren soll, und hat dafür ein Budget von 200 Millionen Euro über die ersten fünf Jahre bewilligt. Die Cyberagentur soll mit den Worten der Bundesverteidigungsministerin Ursula von der Leyen im „militärischen und zivilen Sektor […] als ‚Schatzsucher'"[16] agieren und mit sämtlichen Cyberstellen der Bundeswehr kooperieren – mit dem Cyber Innovation Hub in Berlin, dem Kommando Cyber- und Informationsraum und – wie die ZITiS – auch mit dem Studiengang Cybersicherheit an der Bundeswehruniversität in München.[17] Wenn diese Einrichtung auch gemeinsam von BMI und BMVg gegründet wurde, ist doch offensichtlich, dass sie eher unter der Kontrolle der Bundeswehr und des Bundesverteidigungsministeriums steht. Allerdings sollen im Feld der IT-Sicherheit explizit innere und äußere Sicherheit stärker miteinander verknüpft werden,[18] mit anderen Worten, Militär und Geheimdienste sollen stärker miteinander verbunden werden – eine beunruhigende Vorstellung, denn so wird auch ein Cybereinsatz der Bundeswehr im Inneren denkbar, was genauso ein No-Go sein muss wie jeder andere militärische Einsatz der Bundeswehr im Inland. Um höhere Gehälter zahlen zu können, erhielt die Cyberagentur eine Ausnahmegenehmigung vom Finanzministerium und wirbt damit ganz wie die ZITiS wichtige IT-Sicherheits-(Verteidigungs-)fachkräfte von anderen Behörden ab. Und wie die ZITiS entzieht sich auch die Cyberagentur vollständig jeder parlamentarischen Kontrolle, denn sie wurde wie ein beliebiges öffentliches Unternehmen als eine GmbH gegründet.

Verteidigung der digitalen Sicherheit

Die wachsenden Risiken in einer digitalisierten Gesellschaft werden wir nicht beherrschen können, wenn wir uns nicht vollständig auf die Verteidigung konzentrieren. Wir reden schon lange nicht mehr nur von Computern oder Handys. In wenigen Jahren werden wir 50 Milliarden vernetzte Geräte[19] auf der Welt haben, vom Smart Meter über die Fitnessarmbanduhr bis zum autonom fahrenden Auto. Gerade das exponentiell wachsende Internet der Dinge stellt uns vor große Herausforderungen hinsichtlich der IT-Sicherheit, denn viele Produkte verfügen über ein sehr mangelhaftes Sicherheitsniveau, haben keinen oder nur un-

genügenden Passwortschutz, keine oder ungenügende Wartung durch Software-Updates sowie zahlreiche Sicherheitslücken, die offen stehen wie Scheunentore. Verbraucher*innen sind völlig damit überfordert, die Risiken überhaupt einzuschätzen, die mit dem Kauf derartiger Produkte einhergehen, zumal in den meisten Fällen die Risiken intransparent sind, weil die dafür nötigen Informationen nicht angegeben werden.

Auch wegen dieser so häufig mangelhaften Produktqualität ist die Ausweitung der Produkthaftpflicht auf IT-Hersteller überfällig und muss eben auch Schäden umfassen, die ein smarter Toaster anrichtet, wenn er aufgrund mangelnder IT-Sicherheit Teil eines schädlichen Botnetzes geworden ist.

Schon jetzt gibt es laut BSI über 600 Millionen bekannte Schadprogramme, jeden Tag kommen ca. 280 000 hinzu. Allein für die zehn am häufigsten verwendeten Softwareprodukte waren schon 2016 etwa 1000 Schwachstellen bekannt.[20] Wer Angriffskompetenzen, also Hackerfähigkeiten, aufbaut, schädigt vorsätzlich unser aller IT-Sicherheit, denn man kann nur IT-Systeme hacken, wenn man Sicherheitslücken ausnutzt, anstatt sie zu schließen. Es gibt aber keine guten Sicherheitslücken, um Terroristen zu überwachen, und böse Sicherheitslücken, die den Rest der Gesellschaft Hackerrisiken aussetzen; es gibt nur ganz allgemein Sicherheitslücken in Hardware oder Software, die für jeden Menschen, der ein Gerät mit dieser Hardware oder Software verwendet, ein Risiko darstellen. Deshalb erhöht jede Sicherheitslücke, die ein Geheimdienst entdeckt oder auf dem schwarzen Markt für Steuergelder ankauft, um sie später einmal selbst zum Hacken zu verwenden, die Gefahr für uns alle.

Der Staat als Sicherheitsrisiko

Nach Pressemeldungen soll der BND selbst ein Budget von 4,5 Millionen Euro über einen Zeitraum von 2015 bis 2020 erhalten haben, um Sicherheitslücken aufzukaufen.[21] Bei der NSA in den USA waren es im Jahre 2013 sogar mehr als 25 Millionen Dollar. Von den Risiken dieser Praxis erhielten wir im Jahr 2017 einen Eindruck, denn Kriminelle setzten zu Erpresserzwecken das Schadprogramm WannaCry ein, das eine Sicherheitslücke bei Windows ausnutzte – die der NSA bereits fünf Jahre bekannt war, von dieser aber geheim gehalten wurde –, und konnten so mehr als 230 000 Computer in 150 Ländern infizieren. Betroffen waren unter anderem das Unternehmen Telefónica, der britische National Health Service, das rumänische Außenministerium, das russische Innenministerium, aber auch 450 Rechner der Deutschen Bahn, wodurch eine regionale Leitstelle und viele Anzeigetafeln ausfielen.

Der Handel mit Sicherheitslücken sollte international geächtet werden

Was es stattdessen braucht, ist ein striktes Verbot für staatliche Stellen, Informationen zu bisher unbekannten Schwachstellen aufzukaufen, und eine verbindliche, allgemeine Meldepflicht für Sicherheitslücken, die natürlich von Geheimdiensten entdeckte Schwachstellen einschließen muss. Der Handel mit Sicherheitslücken sollte international geächtet werden; dafür können andere Anreize geschaffen werden, die das Entdecken und Melden von Sicherheitslücken attraktiv machen.

Unsere Bundeswehr muss eine reine Friedensarmee sein, die auf Defensive statt auf Offensive setzt, selbst im Verteidigungsfall. Eine „aktive Cyberabwehr“ ist jedenfalls nicht denkbar ohne die Entwicklung von Angriffskompetenzen, ohne Erhöhung der allgemeinen Sicherheitsrisiken und bei Berücksichtigung der unsicheren Attribution von Cyberangriffen außerdem gleichbedeutend mit einer „Selbstverteidigung auf Verdacht“ gegen einen Staat, dem der Angriff zugeschrieben wird – was völkerrechtlich gar nicht zulässig ist.

Das humanitäre Völkerrecht schreibt auch klar ein Unterscheidungsgebot vor: Militärische Angriffe dürfen nur gegen militärische Ziele, nicht auf zivile Objekte oder Zivilpersonen gerichtet werden. Bei Hackbacks ist es nicht sicher möglich, genau vorherzusagen, welche

Art von Ziel man eigentlich angreift. Hohe zivile Kollateralschäden sind daher nicht auszuschließen. Noch ist nicht klar, wer eigentlich in Deutschland derartige Hackbacks ausführen soll, aber wenn dafür die Cyberwar-Kompetenzen der Bundeswehr genutzt werden sollten, stellt sich zusätzlich die Frage nach dem Parlamentsvorbehalt. Es ist ja wohl unrealistisch, davon auszugehen, dass ein staatlicher Hackerangriff auf ein Ziel im Ausland vorher im Bundestag offen debattiert wird. Bundesinnenminister Seehofer sprach im Digitalausschuss des Bundestages im Kontext der von ihm gewünschten Hackback-Legalisierung mittels einer Grundgesetzänderung auch davon, dass solche Entscheidungen „gegebenenfalls in wenigen Minuten gefällt werden müssten" – dann wäre der vorgeschriebene Parlamentsvorbehalt für Einsätze der Bundeswehr ohnehin nicht machbar.

Transparenz und digitale Bildung für mehr digitale Sicherheit

Investitionen in IT-Sicherheit und IT-Sicherheitsforschung sind richtig, aber auch sie sollten sich auf die Defensive konzentrieren. Dazu gehört auch eine klare Ausweitung der Entwicklung und Nutzung von Open Source und Open Hardware, denn in einer immer komplexer werdenden, digital vernetzten Welt werden Transparenz und Nachvollziehbarkeit immer wichtigere Voraussetzungen für mehr Sicherheit und Vertrauen. Offene Produkte erlauben den Innenblick, sie sind keine Blackboxes, in denen man besonders gut heimliche Hintertüren verstecken kann. Open Source ist nicht per se sicherer, aber ihre Überprüfbarkeit macht es wahrscheinlicher, dass Schwachstellen gefunden und damit auch, dass sie geschlossen werden. Wir sollten weltweit mehr Fokus auf Chips und Software legen, die längere Entwicklungszyklen haben, aber dafür verlässlicher und überprüfbar sind. Security by Design und Security by Default[22] sollten die Richtschnur für alle IT-Produkte sein, aber auch staatliche Vorgaben zu Mindeststandards in der IT-Sicherheit sind erforderlich. Mindestupdatepflichten für Software sollten genauso dazugehören wie ein Passwortschutz für vernetzte Geräte, der diesen Namen verdient und eben keine selbst gewählten Passwörter akzeptiert, die „123456",„qwertz" oder „Passwort" heißen. Dass diese Passwörter millionenfach genutzt werden können, hat ja nicht nur mit den Anwendern zu tun, sondern auch mit verantwortungslosem Produktdesign.

Eine der größten Schwachstellen ist jedoch tatsächlich auch der Mensch selbst, deshalb braucht es mehr lebenslange Bildungs- und Aufklärungsangebote, auch niedrigschwellig und für alle gesellschaftlichen Schichten, um Grundkompetenzen in Sachen IT-Sicherheit zu verbessern. Zu oft noch wird ein gefundener USB-Stick arglos in den privaten oder den Dienstrechner gesteckt, zu häufig auf Links in Phishing-Mails geklickt oder ein leicht zu ratendes Passwort verwendet, viel zu selten werden Mails verschlüsselt, Konten bei sozialen Netzen durch Zwei-Faktor-Authentifizierung geschützt und wird Software regelmäßig aktualisiert. Das BSI sollte auch zu diesem Zweck als nationale Verbraucherschutzbehörde ausgebaut werden, denn bessere Prävention in der Fläche ist ein wichtiger Beitrag. Mehr Sicherheit für uns alle erfordert Engagement von allen, von Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Ich hoffe sehr, dass es nicht erst zu einer Katastrophe kommen muss, um zu verstehen, dass wir nur gemeinsam die Infrastruktur und Basis der digitalen Gesellschaft sicherer machen können – und dass gemeinsam auch bedeutet, damit aufzuhören, IT-Sicherheit in nationalen Grenzen zu denken.

Die Autorin

Foto: Jesco Denzel

Anke Domscheit-Berg (51) ist Publizistin, Netzaktivistin und Mitglied des Deutschen Bundestages. Für die Fraktion DIE LINKE ist sie netzpolitische Sprecherin, Obfrau im Ausschuss Digitale Agenda sowie stellvertretendes Mitglied in der Enquetekommission Künstliche Intelligenz. Nach fast 15 Jahren bei Accenture, McKinsey und Microsoft war sie seit 2011 selbständig. Die Autorin mehrerer Bücher publiziert in zahlreichen Medien und hält Vorträge im In- und Ausland. Ihr Schwerpunkt ist die gemeinwohlorientierte Gestaltung der digitalen Geslellschaft.

1 „Budget“. https://www.darpa.mil/about-us/budget (Stand: 28. März 2019).
2 „A Selected History of DARPA Innovation“. https://www.darpa.mil/Timeline/index.html (Stand: 28. März 2019).
3 „Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im Januar 2019 (in Millionen)“. https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (Stand: 6. Juni 2019).
4 Puiu, Tibi (2019): „Your smartphone is millions of times more powerful than all of NASA's combined computing in 1969“. https://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/ (Stand: 6. Juni 2019).
5 „Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper“. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html (Stand: 28. März 2019).
6 Klein, Andy (2017): „Hard Drive Cost per Gigabyte“. https://www.backblaze.com/blog/hard-drive-cost-per-gigabyte/ (Stand: 28. März 2019).
7 „BND darf am Internetknoten weiter Daten abzapfen“. https://www.spiegel.de/netzwelt/netzpolitik/de-cix-betreiber-von-internet-knoten-verliert-klage-gegen-bnd-a-1210243.html (Stand: 13. Mai 2019).
8 Unger, Christian (2018): „Hackerangriffe kann man sich wie eine Pizza bestellen“. https://www.morgenpost.de/politik/article215355473/Hackerangriffe-kann-man-sich-wie-eine-Pizza-bestellen.html (Stand: 28. März 2019).
9 Ein solches Szenario beschreibt Marc Elsberg sehr eindrücklich in seinem Roman *Blackout – Morgen ist es zu spät.* (https://de.wikipedia.org/wiki/Blackout_%E2%80%93_Morgen_ist_es_zu_sp%C3%A4t).
10 Linder, Roland/Theile, Gustav (2019): „Auch die Geheimdienste wollen mit Alexa spionieren“. https://www.faz.net/aktuell/wirtschaft/diginomics/geheimdienste-wollen-alexa-offenbar-zur-ueberwachung-nutzen-16136726.html (Stand: 23. Mai 2019).
11 Deutscher Bundestag, Drucksache 19/6246 (2019): „Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. André Hahn, Gökay Akbulut, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE“. Berlin. http://dipbt.bundestag.de/dip21/btd/19/062/1906246.pdf (Stand: 1. April 2019).
12 Ebd.
13 Siehe hierzu die Stellenangebote des ZITiS unter https://www.zitis.bund.de/DE/Karriere/Stellenangebote/stellenangebote_node.html (Stand: 1. April 2019).
14 Biselli, Anna (2018): „Statt Mate: Hackerbehörde ZITiS findet nicht genug Personal und probierts mit 2.000 Koffein-Shots“. https://netzpolitik.org/2018/statt-mate-hackerbehoerde-zitis-findet-nicht-genug-personal-und-probierts-mit-2-000-koffein-shots/ (Stand: 1. April 2019).
15 „Tabelle TVöD Bund, gültig vom 1. März 2018 bis 31. März 2019“. https://www.bsi.bund.de/SharedDocs/Stellenangebote/DE/Entgelttabelle.pdf?__blob=publicationFile&v=6 (Stand: 28. März 2019).
16 Bundesministerium der Verteidigung (2019): „BMVg und BMI geben Standort für neue Cyberagentur bekannt“. https://www.bmvg.de/de/aktuelles/standort-fuer-neue-cyberagentur-30534 (Stand: 28. März 2019).
17 Ebd.
18 Bundesministerium der Verteidigung (2018): „Bundeskabinett beschließt Cyberagentur“. https://www.bmvg.de/de/aktuelles/bundeskabinett-beschliesst-cyberagentur-27392 (Stand: 28. März 2019).
19 „Prognose zur Anzahl vernetzter Geräte weltweit in den Jahren 2003 bis 2020“. https://de.statista.com/statistik/daten/studie/479023/umfrage/prognose-zur-anzahl-der-vernetzten-geraete-weltweit/ (Stand: 13. Mai 2019).
20 Steiner, Henning (2017): „Die Lücke der Software: Wie eine Hackerin ins System kommt“. https://www.hr-inforadio.de/programm/dossiers/die-luecke-in-der-software-wie-eine-hackerin-ins-system-kommt,schwachstellen-in-software_einfallstor-fuer-hacker-100.html (Stand: 28. März 2019).
21 Voss, Oliver (2017). „Erpressersoftware ‚WannaCry‘: Sicherheitslücken auf der ganzen Welt“. https://www.tagesspiegel.de/wirtschaft/erpressersoftware-wannacry-sicherheitsluecken-auf-der-ganzen-welt/19806608.html (Stand: 28. März 2019).
22 Security by Design: Entwicklung von Produkten und Diensten mit einem dem Stand der Technik entsprechenden Sicherheitsniveau.
Security by Default: Die Grundeinstellungen eines Produkts müssen möglichst sichere Einstellungen sein, also keine voreingestellten Passwörter, die „0000“ oder „admin“ heißen.
Quelle: Hahn, André (MdB), Domscheit-Berg, Anke (MdB) et. al. (2018). Fraktion DIE LINKE. im Bundestag (Hg.): „Cybersicherheit“ – ein Beitrag für einen sicheren digitalen Raum“, S. 12. https://www.linksfraktion.de/fileadmin/user_upload/180709_Digitale_Sicherheit.pdf (Stand 23. Mai 2019).

CYBERSICHERHEIT UND CYBERVERTEIDIGUNG

STÄRKERER SCHUTZ DURCH RESSORTÜBERGREIFENDE ZUSAMMENARBEIT

Autor: ***Andreas Könen***

Abstract

Angesichts der zunehmenden Bedrohungsszenarien, die ihren Ausgangspunkt im Cyberspace haben, wird es für Staaten immer wichtiger, in der gesamtstaatlichen Sicherheitsarchitektur den Cyberspace miteinzubeziehen. Die Bundesrepublik Deutschland hat daher 2016 eine Cybersicherheitsstrategie entworfen, die heutigen und zukünftigen Bedrohungen Rechnung tragen soll. Darin werden auch militärische Aspekte der Cyberverteidigung benannt, denn die Verteidigungsfähigkeiten der Bundeswehr im Cyberraum seien ein „wesentlicher Teil der Cyber-Sicherheitsarchitektur". Daher, so der Autor, sei mit der Aufstellung des Kommandos Cyber- und Informationsraum der Bundeswehr (KdoCIR) 2017 eine herausragende Maßnahme der deutschen Cybersicherheitsstrategie umgesetzt worden.

Die Bundeswehr ist zur Aufrechterhaltung ihrer Einsatzbereitschaft auf das Funktionieren ziviler kritischer Infrastruktur angewiesen, weshalb es gelte, bereits im Friedensfall wirksame Mechanismen zum Schutz dieser zu entwickeln. Der Beitrag Könens erörtert kurz die gesetzlichen und organisatorischen Grundlagen zum Schutz dieser Infrastruktur, bevor er auf die Notwendigkeit der engen Kooperation verschiedener Ressorts eingeht. Die Gefährdungslage im Cyberraum sei schlichtweg nur gemeinsam zu bewältigen. Bei zunehmender Komplexität der Sicherheitslage müssten technische Bewertung von Cyberaktivitäten sowie außenpolitische und militärische Lage im Zusammenhang betrachtet werden, um zu einer umfassenden Einschätzung der Gefahrenlage kommen zu können.

Für den äußersten Fall, dies stellt Könen heraus, sollte die technische Möglichkeit vorgehalten werden, Angreifersysteme zu isolieren oder ganz abzuschalten. Dies sei notwendige Bedingung für eine aktive Cyberabwehr. Wichtig hierfür wäre es, Schwellenkriterien festzulegen und Entscheidungsprozesse zu etablieren. Die dazu notwendige Diskussion habe jedoch gerade erst begonnen.

In der von der Bundesregierung 2016 verabschiedeten Cyber-Sicherheitsstrategie für Deutschland werden im Handlungsfeld 3 „Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur" Kriterien und Handlungsmaximen für die nationale Cyber-Sicherheitsarchitektur dargelegt. Wesentliches strategisches Ziel und Maßnahme zugleich ist dabei die Stärkung der Verteidigungsaspekte der Cybersicherheit. Bereits in der Cyber-Sicherheitsstrategie werden daher im entsprechenden Absatz die vordringlichen Aspekte der Cyberverteidigung als militärischer Teil der Gesamtverteidigung im Cyberraum benannt: „Die Verteidigungsfähigkeiten der Bundeswehr im Cyber-Raum sind […] wesentlicher Teil der Cyber-Sicherheitsarchitektur. Sowohl die inhaltliche Übereinstimmung bei der technischen Umsetzung von Schutzmaßnahmen als auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyber-Abwehr unter verteidigungsrelevanten Aspekten und Situationen zeigen die enge Abhängigkeit."[1]

Mit der Aufstellung des Kommandos Cyber- und Informationsraum (KdoCIR) hat das BMVg im April 2017 eine herausragende Maßnahme umgesetzt, die in der Cyber-Sicherheitsstrategie angekündigt wurde. Es lohnt sich daher, einige strategische Ziele und Maßnahmen, die im Jahr 2016 beschrieben wurden, erneut zu beleuchten, in Beziehung zu aktuellen Entwicklungen in der Cyberpolitik zu setzen und daraus gegebenenfalls neue Schlussfolgerungen zu ziehen. Dies betrifft vor allem das Zusammenwirken von zivilen und militärischen Cybersicherheitsmaßnahmen in den Feldern Schutz kritischer Infrastrukturen, Gefährdungslage im Cyberraum, internationale Cybersicherheitspolitik und aktive Cyberabwehr.

Der Schutz kritischer Infrastrukturen

Besondere Aufmerksamkeit wurde in den letzten Jahren dem Schutz kritischer Infrastrukturen gewidmet. Mit dem IT-Sicherheits-

gesetz von 2015, der daraus resultierenden Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (KRITIS-Verordnung) und der europäischen Netzwerk- und Informationssicherheits-Richtlinie wurde ein gesetzlicher Rahmen für den Schutz der versorgungskritischen Infrastrukturen geschaffen.

Hierbei nutzt der Gesetzgeber einen doppelten Ansatz, um Cyber- und Informationssicherheit zu befördern: Einerseits legt er den Unternehmen die Pflicht zur Erstellung von firmenspezifischen Informationssicherheitskonzepten sowie deren Realisierung und Auditierung auf. Dieser präventive Ansatz wird idealerweise durch die Schaffung eines branchenspezifischen Mindeststandards gestützt, an dem sich die Unternehmen orientieren können. Dies wurde zum Beispiel in der Versicherungsbranche erfolgreich umgesetzt. Im zweiten Ansatz, durch den Detektion und Reaktion unterstützt werden sollen, etabliert der Gesetzgeber mit der Einführung einer Meldepflicht für Cybersicherheitsvorfälle die Basis für eine branchen- und sektorenübergreifende Erstellung eines Cybersicherheitslagebildes der kritischen Infrastrukturen.

Mit dem Entwurf des IT-Sicherheitsgesetzes 2.0 wird nun ein nächster Schritt zum Schutz herausragender Unternehmen der deutschen Wirtschaft unternommen. Neben einer Ausweitung des bisherigen versorgungskritischen Ansatzes etwa auf die Branche Entsorgung beziehungsweise den Sektor Kultur und Medien sollen in einer Anpassung dieses versorgungsorientierten Ansatzes nun auch Unternehmen reguliert werden, die durch fortschreitende Digitalisierung in einem erhöhten Maße von Informationstechnologie abhängig sind und bei denen Ausfälle der IT, die etwa durch einen Cyberangriff verursacht werden, die Geschäftstätigkeit zum Erliegen bringen oder sogar in der Folge zu Großschadensereignissen führen können. Es handelt sich bei solchen Unternehmen unter Prägung einer neuen Begrifflichkeit um IT-kritische Unternehmen. Diese IT-Kritikalität würde aber allein eine Regulierung nicht rechtfertigen. Erst wenn eine besondere Bedeutung für das Gemeinwesen sichtbar wird, ergibt sich eine Fürsorgepflicht des Staates zum Schutz der Unternehmen und letztlich für die Bürgerinnen und Bürger: Herausragende Beispiele für die Notwendigkeit einer solchen Regulierung sind etwa die chemische Industrie wegen ihres Großschadenspotenzials, die Verteidigungs- und Sicherheitswirtschaft in ihrer Rolle als Lieferant für die Bundeswehr und die anderen Sicherheitsbehörden in Bund und Ländern, die Automobilwirtschaft wegen ihrer gesamtwirtschaftlichen Bedeutung mit Blick auf die Produktions- und Steuerungs-IT oder auch Unternehmen mit substanziellem schützenswerten Know-how („Intellectual Property“).

Mit dem Entwurf des IT-Sicherheitsgesetzes 2.0 wird ein nächster Schritt zum Schutz herausragender Unternehmen der deutschen Wirtschaft unternommen

Wo besteht nun in der gesamten zivilen Thematik der Cybersicherheit kritischer Infrastrukturen der Bezug zu den Strukturen der militärischen Verteidigung? Betrachtet man den erweiterten Begriff kritischer Infrastrukturen als IT-kritische Unternehmen mit gesamtgesellschaftlicher Bedeutung, so wird unmittelbar klar, dass man die Bundeswehr und ihre Zulieferindustrie in diesem Sinn durchaus als kritische Infrastruktur identifizieren kann, und dies auch bereits in Friedenszeiten. Mit der Digitalisierung und Vernetzung der Streitkräfte generell, mit dem Einsatz hochkomplexer IT in Waffensystemen, der Automatisierung mobiler Fahr- und Flugzeuge sowie einer voll digitalisierten Kommunikations- und Führungsinfrastruktur wird dies unmittelbar deutlich. Andererseits ist die Bundeswehr sowohl in Friedenszeiten als auch im Verteidigungsfall auf das Funktionieren der zivilen kritischen Infrastrukturen im obigen erweiterten Sinne angewiesen. Die Verfügbarkeit der nationalen und internationalen Telekommunikation sowie des nationalen und internationalen Internets ist hier ein wichtiges Beispiel.

Aufgrund der Zuständigkeit des BMI für die öffentliche Sicherheit und die Versorgungssicherheit der Bevölkerung im Friedensfall auf der einen Seite sowie der Notwendigkeit des Rückgriffs auf die kritischen Infrastrukturen durch BMVg beziehungsweise Bundeswehr im Verteidigungsfall entsteht auch bei Gefährdungen und Angriffen aus dem Cyberraum eine neue Herausforderung für eine gemeinsame Aufstellung beider Ressorts. Eine sorgfältige Analyse und Bewertung der jeweiligen IT-Abhängigkeiten von den kritischen Infrastrukturen sowie deren Interdependenzen sind daher für die innere und äußere Sicherheit schon im Friedensfall unerlässlich. Dies betrifft insbesondere die Vorsorge für Krisen- und Katastrophenfälle und letztlich auch den Verteidigungsfall. Hieraus müssen abgestimmte Reaktionsmechanismen abgeleitet werden, die auch bereits im Vorfeld geübt werden.

Ein gemeinsames Vorgehen in der Standardisierung von Cybersicherheitsanforderungen in europäischen und internationalen Standardisierungsgremien ist wünschenswert

Konkret betrifft dies zum Beispiel abgestimmte oder sogar identische Informationssicherheitsanforderungen an IT-Produkte oder an die Cybersicherheit von (gemeinsam oder etwa im Rahmen der NATO genutzten) Netzwerk- oder Kommunikationsinfrastrukturen. Viele dieser Anforderungen werden bereits heute, etwa in Zulassungsverfahren des BSI im Rahmen des Geheimschutzes oder bei Beschaffungsvorhaben der IT-Konsolidierung des Bundes, gemeinsam erstellt und in die Praxis überführt. Der neue IT-Grundschutz des BSI mit anwenderspezifischen Profilen bei Cybersicherheitsanforderungen ist hier das Werkzeug der Wahl auch für die Bundeswehr.

Angesichts der fortschreitenden Digitalisierung ergeben sich hier aber permanent weitere Handlungsfelder, zum Beispiel bei der Cybersicherheit von „Internet of Things"-Produkten oder bei der Kommunikation über (virtuelle) Netzwerke unterschiedlicher Sicherheitsniveaus. Für die gemeinsam von BMVg und BMI aufgestellte Agentur für Innovation in der Cybersicherheit resultiert hieraus bereits jetzt eine Fülle möglicher Forschungsansätze. Darüber hinaus ist aber auch ein gemeinsames Vorgehen in der Standardisierung von Cybersicherheitsanforderungen in europäischen und internationalen Standardisierungsgremien wünschenswert.

Die Gefährdungslage im Cyberraum und ihre gemeinsame Bewältigung

Mit dem Cyberabwehrzentrum (CyberAZ) wurde beim BSI 2011 eine Kooperations- und Koordinierungsplattform geschaffen, der aus dem Geschäftsbereich des BMVg insbesondere auch das Kommando Cyber- und Informationsraum (KdoCIR) zuarbeitet. Das KdoCIR arbeitet hier gemeinsam mit den anderen Sicherheitsbehörden des Bundes, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), aber auch den Aufsichtsbehörden kritischer Infrastrukturen zusammen und tauscht Informationen, Analysen und Bewertungen zur Cyberlage aus. Auf Basis dieses Informationsaustauschs hat die Arbeit des CyberAZ folgende herausragenden Ziele: koordinierte operative Bearbeitung von Cybersicherheitsvorfällen, Erstellung des dynamischen nationalen Cybersicherheitslagebildes und die Bereitstellung abgestimmter und eingeübter Krisenreaktionsmechanismen der beteiligten Behörden für die Cyberkrise. Perspektivisch sind eine Erweiterung des CyberAZ und die Einbeziehung der Bundesländer und der Wirtschaft geplant.

Für das CyberAZ stellen sich an der Nahtstelle zwischen ziviler und militärischer Verteidigung neue Herausforderungen: Das Cybersicherheitslagebild des CyberAZ fußt zu einem herausragenden Anteil auf den Erkenntnissen ziviler Einrichtungen wie der Computer Emergency Response Teams (CERT) verschiedener Behörden und Einrichtungen. Die verwendeten Quellen spiegeln im Regelfall eine Situation in den nationalen

und internationalen Netzen wider, die von verschiedensten Cybersicherheitsvorfällen zivilen Charakters geprägt ist, die vornehmlich auf cyberkriminelle Aktivitäten, Cyberspionage oder Cybersabotage zurückzuführen sind. Militärische Cybersicherheitsszenarien gehören nicht zum Spektrum der Aufgaben der beteiligten Behörden und werden vom KdoCIR klarerweise in eigener Verantwortung und in eigenen Strukturen wahrgenommen. Auch die militärische Cybersicherheitslage wird dort erstellt. Eine Differenzierung zwischen zivilen und militärischen Cybersicherheitsszenarien erschloss sich dabei in der Vergangenheit aus der Einbettung von Cybersicherheitsvorfällen in Sicherheitsvorkommnisse in der physischen Welt. Diese klare Trennung ist allerdings mittlerweile nicht mehr möglich.

Denn Cybersicherheitsvorfälle der jüngeren Vergangenheit machen deutlich, dass mit einer Zunahme von Vorfällen im Cyberraum zu rechnen ist, die hybriden Charakter tragen. Cyberangriffe können und werden zunehmend unterhalb der Schwelle militärischer Angriffe in Szenarien zwischenstaatlicher diplomatischer oder politischer Krisen genutzt werden und führen zu einer erhöhten Komplexität der Cybersicherheitslage. Eine konsistente und alle Aspekte umfassende Analyse und Bewertung solcher Vorfälle kann daher nur in Kooperation zwischen dem KdoCIR, dem BSI und den anderen Behörden im CyberAZ erfolgen. Eine spezifische Herausforderung bei der Bewertung hybrider Angriffe besteht klarerweise darin, die technische Bewertung des CyberAZ mit der Bewertung der außenpolitischen und militärischen Lage zusammenzuführen. Hier sind insbesondere BMVg, Auswärtiges Amt, BKA und BMI aufgerufen, gemeinsam mit den nachgeordneten Behörden eine Kooperation und Koordination der jeweiligen Lagezentren zu ermöglichen und zu strukturieren.

Auch für einen eventuellen Verteidigungsfall muss entsprechende Vorsorge getroffen werden, damit alle Informationen der zivilen Cybersicherheitslage in einem zum Verteidigungsfall eskalierenden Krisenfall an die Bundeswehr und das KdoCIR übermittelt werden können. Die hierfür erforderlichen Strukturen, Rechtsgrundlagen und darauf aufbauenden Prozesse stehen aber noch am Anfang.

Internationale Cybersicherheitspolitik

Auch in der europäischen und internationalen Cybersicherheitspolitik spielt im Sinne einer aktiven Positionierung Deutschlands die enge Zusammenarbeit zwischen dem BMVg und dem BMI sowie zwischen dem KdoCIR und dem BSI eine wichtige Rolle, insbesondere im Rahmen der Maßnahme „Die Cyber-Verteidigungspolitik der NATO weiterentwickeln“. Hierzu erneut ein Zitat aus der Cyber-Sicherheitsstrategie von 2016:

„Das Nordatlantische Bündnis ist als ein Eckpfeiler der Sicherheit Deutschlands sowie der euroatlantischen Sicherheit auf einen ausreichenden Schutz vor Angriffen aus dem Cyber-Raum angewiesen, um seine Kernaufgaben insbesondere im Bereich der kollektiven Verteidigung und bei internationalen Stabilisierungseinsätzen erfüllen zu können. [...] Ziel ist es, die Resilienz der Alliierten und der Allianz insgesamt kontinuierlich zu erhöhen und nicht zuletzt im Kontext hybrider Bedrohungen die Abschreckungs- und Verteidigungsfähigkeiten zu steigern.“[2]

Eine klare Differenzierung zwischen zivilen und militärischen Cybersicherheitsszenarien ist mittlerweile nicht mehr möglich

Weitgehend unbekannt ist aber die Tatsache, dass das BSI sowohl die deutsche NATO Crypto Security Authority (NCSA) als auch Cyberdefence Authority (NCDA) darstellt und damit Deutschland in verschiedenen Gremien der NATO gemeinsam mit dem KdoCIR bzw. dem BMVg vertritt. Dies trägt in der historischen Entwicklung vor allem der Tatsache Rechnung, dass das BSI im Rahmen des Geheimschutzes sowohl die nationale Zulassung von militärischem Kommunikationsequipment verantwortet als auch in den

entsprechenden NATO-Zulassungsgremien seine Kompetenzen einbringt. Konsequenterweise wurde dann die Rolle des BSI auch auf die entsprechenden Fragestellungen in der Cybersicherheit (hier gleich Cyberdefence) vor allem in Netzen erweitert.

Hieran gilt es nun auch in der zukünftigen Weiterentwicklung anzuknüpfen. Für die NATO wird es in Verteidigungslagen essentiell sein, dass die Mitgliedstaaten über entsprechend robuste und verlässliche kritische Infrastrukturen verfügen, insbesondere etwa bei den Netzinfrastrukturen, auf die im Verteidigungsfall zurückgegriffen werden müsste. Es sind hier daher neben die oben formulierten nationalen und europäischen Cybersicherheitsanforderungen entsprechende Anforderungen vonseiten der NATO zu stellen und national zu realisieren. Um sowohl im zivilen Krisen- oder Katastrophenfall als auch im Verteidigungsfall über resiliente Netze zu verfügen, ist eine Abstimmung der aus dem IT-Sicherheitsgesetz resultierenden Anforderungen mit denen der NATO erforderlich. Zur Abstimmung dieser aktuell noch lose nebeneinanderstehenden Anforderungen sollten KdoCIR und BSI künftig stärker kooperieren.

Für zivile Maßnahmen der aktiven Cyberabwehr besteht noch gesetzgeberischer Handlungsbedarf

Zivile und militärische Aspekte einer aktiven Cyberabwehr

Für den Einsatz bei zivilen Krisen oder Katastrophen im Cyberraum, die sich als Cybersabotage gegen kritische Infrastrukturen mit entsprechender Wirkung äußern, werden zurzeit Mittel der zivilen Verteidigung unter dem Begriff „Aktive Cyberabwehr“ diskutiert. Während der Einsatz aktiver Verteidigungsmaßnahmen im Cyberraum im Falle der Landesverteidigung, des NATO-Bündnisfalles oder eines Auslandseinsatzes durch eine entsprechende Mandatierung der Bundeswehr beziehungsweise der Kräfte des KdoCIR durch den Deutschen Bundestag erfolgen kann, besteht hier für zivile Maßnahmen der aktiven Cyberabwehr einerseits noch gesetzgeberischer Handlungsbedarf.

Andererseits ist auch überhaupt der Aufbau entsprechender Fähigkeiten auf Basis entsprechender Befugnisse für die Maßnahmen einer zivilen Verteidigung im Cyberraum notwendig: Ein erweiterter Schutz für nationale Infrastrukturen gegen Cybersabotageangriffe aus dem Ausland könnte im ersten Schritt etwa durch (teilweise) Netzsperren, durch gezielte Blockade der Angreifer und Abriegelung der Opfersysteme durch den jeweiligen Provider erreicht werden. Im Inland wären hierzu bei Feststellung einer Krisen- und Katastrophenlage im nationalen Teil des Cyberraums Anordnungsbefugnisse und Anordnungsmaßnahmen des BSI als Ordnungsbehörde vorstellbar. Die Polizeien des Bundes und der Länder könnten das BSI in der polizeilichen Gefahrenabwehr unterstützen und zusätzlich in der Kooperation mit Polizeien im Ausland für die Unschädlichmachung von Angreifersystemen dort Sorge tragen.

Im äußersten Fall sollte zur Abwehr auch die Isolation oder Abschaltung von Angreifersystemen durch aktive Cyberabwehrmaßnahmen möglich sein, etwa wenn Gefahr im Verzuge eine Reaktion in kürzester Frist erforderlich macht. Hierzu wären dann auch geeignete Entscheidungsprozesse zu etablieren.

Selbst die Einrichtung einer zivilen aktiven Cyberabwehr wie oben skizziert ließe den-

Der Autor

*Diplom-Mathematiker **Andreas Könen** ist Abteilungsleiter CI - Cyber- und Informationssicherheit im Bundesministerium des Innern, für Bau und Heimat (BMI). Zuvor war er der Leiter der Stäbe IT II - IT- und Cybersicherheit; sichere Informationstechnik und ÖS III - Cybersicherheit im Bereich der Polizeien und des Verfassungsschutzes im BMI. Von 2006 bis 2016 hatte er verschiedene Leitungspositionen im Bundesamt für Sicherheit in der Informationstechnik (BSI) inne, zuletzt war er dessen Vizepräsident. Zuvor war er in verschiedenen Bereichen der Bundesverwaltung mit dem Schwerpunkt Informationstechnik tätig. Andreas Könen ist verheiratet und Vater zweier Kinder.*

noch komplexe Fragestellungen offen: Hybride Bedrohungsszenarien, in denen zum Beispiel nicht mehr scharf zwischen Sabotage und militärischen Angriffen unterschieden werden kann, sind heute in der „analogen Welt“ gängige Methodik zur Destabilisierung des Opfers. Vergleichbare Szenarien sind in der virtuellen Welt des Cyberraums erst recht und in vielfältiger Form vorstellbar. Angreifer könnten destabilisierende Maßnahmen in der analogen Welt mit Cybersabotage koppeln und somit für eine doppelt hybride Gefährdungslage – zivil versus militärisch und analog versus digital – sorgen.

Lösungen oder Lösungsansätze für solche komplexen Verteidigungsszenarien existieren heute noch nicht und bedürfen einer tiefergehenden Analyse und Bewertung. Hier eröffnet sich ein weiteres Feld für eine intensive Zusammenarbeit militärischer und ziviler Stellen im Inland wie mit unseren Partnern im Ausland, vor allem in der EU und in der NATO. Hierzu sind neben der Lösung von Fragestellungen des Völkerrechts, des Rechts der Gefahrenabwehr, der Entwicklung entsprechender technischer, organisatorischer und politischer Lösungen sowie der Schaffung geeigneter Krisenreaktionsmechanismen auch noch einmal grundsätzliche Erörterungen ethischer Verhaltensmaßstäbe in der Digital- und Cyberwelt erforderlich. Die Diskussion hat gerade erst begonnen.

1 Bundesministerium des Innern (2016): *Cyber-Sicherheitsstrategie für Deutschland 2016.* Berlin, S. 33. https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Stand: 26. April 2019).
2 Ebd., S. 40.

DER ORGANISATIONSBEREICH CYBER- UND INFORMATIONSRAUM (CIR) ALS WICHTIGER TEIL EINER GESAMTSTAATLICHEN SICHERHEITSVORSORGE

Autor: ***Generalleutnant Ludwig Leinhos***

Die Digitalisierung ist das dominierende kulturelle und gesellschaftliche Merkmal der Gegenwart, der Megatrend für das 21. Jahrhundert. Die Digitalisierung und nahezu grenzenlose Vernetzung ermöglichen enorme Verbesserungen und Innovationen. Prozesse und Kommunikation sind schneller und effizienter. Vieles ist bequemer und einfacher geworden. Wann fährt der nächste Bus? Wie wird das Wetter heute Abend? Schnell noch von unterwegs die Heizung ein wenig herunterregeln. Der technische Fortschritt ermöglicht Erleichterungen in allen Bereichen des Lebens und der Gesellschaft.

Auch bei der Bundeswehr macht sich die Digitalisierung einschlägig bemerkbar. Waffensysteme wie der Eurofighter oder eine Fregatte kommen nicht mehr ohne digitale Sensorik, Netzwerke und Entscheidungen unterstützende Computersysteme aus. Logistikketten sind ohne Abbildung in IT kaum noch beherrschbar, und auch der Infanterist der Zukunft wird zunehmend zum digitalisierten Sensor und Effektor.

Die Einbindung moderner IT in den militärischen Planungs- und Entscheidungsprozess hat prägenden Einfluss auf den Einsatz moderner Streitkräfte. Sie bestimmt zunehmend auch Führungsverfahren und Führungskultur.

Herausforderungen der Digitalisierung

Bei allen Vorteilen und Errungenschaften gibt es aber auch die Kehrseite der Medaille: Die Digitalisierung hat neue Abhängigkeiten und Verwundbarkeiten geschaffen. Viele Staaten und Unternehmen betrachten die Risiken aus dem Cyberraum als eine der größten, wenn nicht sogar als die größte Bedrohung der nächsten Jahre und Jahrzehnte. Cyberangriffe auf Staaten, kritische Infrastrukturen und private Haushalte sind schon lange Realität. Angriffe kommen täglich, sind automatisiert oder hoch differenziert und werden immer anspruchsvoller. Die Auswirkungen des Erpressungstrojaners WannaCry, der Schadsoftware NotPetya oder der Angriff auf den Informationsverbund Berlin-Bonn (IVBB) Ende 2017 sind vielen von uns noch sehr gut in Erinnerung. Staaten, Wirtschaftsunternehmen und Privatpersonen sind gleichermaßen betroffen. Bei Unternehmen können selbst niedrigschwellige Cyberangriffe Schäden in Milliardenhöhe erzeugen. Wie hoch eine persönliche Betroffenheit sein kann, wurde ab Ende 2018 deutlich, als ein Schüler ohne formale IT-Kenntnisse viele persönliche Daten unterschiedlicher Personen, die sich im privaten Bereich unzureichend geschützt hatten, gesammelt und auf Twitter für die Allgemeinheit zugänglich hochgeladen hat.

Neben Angriffen aus dem Cyberraum nehmen auch Aktivitäten im Informationsumfeld wie etwa Fake-News-Kampagnen weiter zu. Unruhen werden so gezielt geschürt. Staatliche und innerstaatliche Konflikte werden mehr und mehr durch Propaganda und Desinformation beeinflusst. Information wird zu einer Kernressource der Zukunft.

Diese Entwicklungen werden in Qualität und Quantität weiter zunehmen. Ein adäquater Schutz ist daher von elementarer Bedeutung für Staat, Wirtschaft und Gesellschaft. Der Staat muss handlungsfähig bleiben und den Schutz und die Versorgung der Bevölkerung sicherstellen können. Die Fähigkeiten der Bundeswehr im Cyber- und Informationsraum können dafür einen wesentlichen Beitrag liefern.

Aufstellung der Bundeswehr im Cyber- und Informationsraum

Die Bundeswehr beschäftigt sich bereits seit den Neunzigerjahren intensiv mit dem Thema IT-Sicherheit. Sie betreibt seit mehr als 20 Jahren eine eigene IT-Sicherheitsorganisation mit rund 600 Angehörigen und legt besonderen Wert auf die Awareness ihrer Angehörigen im Umgang mit IT. Als Reaktion auf die Auswirkungen der zunehmenden Digitalisierung wurde im April 2017 der neue Organisationsbereich Cyber- und Informationsraum (CIR) aufgestellt. Bereits exis-

tierende Einheiten mit entsprechender Expertise wurden dort gebündelt. Vorhandenes Know-how wurde und wird weiter ausgebaut.

Das Aufgabenportfolio des neuen Organisationsbereichs ist sehr vielfältig: Ein Tätigkeitsschwerpunkt liegt auf dem Schutz und dem Betrieb des IT-Systems der Bundeswehr – und zwar im In- und im Ausland. Auch die Fähigkeiten zur Aufklärung und Wirkung im Cyber- und Informationsraum werden gestärkt und weiterentwickelt. Hierzu zählen Cyberoperationen, wie beispielsweise das Eindringen in gegnerische IT-Netze, Elektronischer Kampf und Operative Kommunikation in den Auslandseinsätzen. Durch die Angehörigen des Geoinformationsdienstes werden alle Bereiche der Bundeswehr mit hochauflösenden, qualitätsgesicherten digitalen Geoinformationen jeglicher Art bei ihrer Auftragserfüllung unterstützt. Darüber hinaus trägt der Organisationsbereich Cyber- und Informationsraum durch den Austausch und die Kooperation mit anderen nationalen und internationalen Institutionen zu einer gesamtstaatlichen Sicherheitsvorsorge bei und stärkt die Cybersicherheitsarchitektur Deutschlands.

Im Kommando CIR wurde bereits ein eigenes Lagezentrum für die Dimension Cyber- und Informationsraum etabliert. Durch die Fusion existierender Lagen aus allen Bereichen von Relevanz für die Dimension Cyber- und Informationsraum wird ein valides Lagebild als Basis für Handlungsoptionen und Synergien generiert. Analysten verarbeiten unterschiedliche strukturierte und unstrukturierte Daten aus verschiedenen Quellen – künftig unter Nutzung von künstlicher Intelligenz und Big-Data-Methoden. So könnten beispielsweise durch Korrelationen von Daten aus dem IT-System der Bundeswehr mit Erkenntnissen aus dem Bereich des Militärischen Nachrichtenwesens sowie offen zugänglichen Informationen aus sozialen Netzwerken Rückschlüsse auf eine zunehmende hybride Bedrohung oder einen koordinierten Cyberangriff gezogen werden. Die so gewonnenen Analysen stellen wir Nutzern in der Bundeswehr und anderen Behörden zur Verfügung. Darüber hinaus haben wir das Zentrum Cybersicherheit der Bundeswehr weiter mit entsprechendem Fachpersonal gestärkt. Zum 1. April 2018 wurde das Zentrum Cyberoperationen aufgestellt, zum 1. April 2019 folgte das Zentrum für Softwarekompetenz der Bundeswehr. Mit all diesen Maßnahmen sind wir unserem selbst gesteckten Ziel, den Cyber- und Informationsraum mit all seinen Facetten ganzheitlich zu gestalten, bereits ein gutes Stück näher gekommen.

Besonderheiten der Dimension Cyber- und Informationsraum

Die NATO betrachtet den Cyberraum bereits seit dem Warschauer Gipfel von 2016 als eigenständigen Operationsraum – analog zu Land, Luft, See und Weltraum. Im Cyberraum können Streitkräfte mithilfe von entsprechender Software gegnerische Systeme aufklären und auch gegen sie wirken. Konkret könnten beispielsweise logistische Ketten unterbrochen, wichtige Daten für die Operationsführung des Gegners verändert, Führungs- und Informationssysteme lahmgelegt werden. In der Bundeswehr fassen wir diese neue militärische Dimension bewusst noch weiter als die NATO und beziehen den Informationsraum mit ein. Jenseits der Technik werden dort Informationen von Menschen wahrgenommen, interpretiert und verbreitet. Die sogenannte „veröffentlichte Meinung“ ist dabei ein wesentlicher Bestandteil unserer Betrachtungen.

Der Cyber- und Informationsraum ist durch einige Besonderheiten im Vergleich zu den anderen klassischen Operationsräumen geprägt. Er zeichnet sich durch ein hohes Maß an Komplexität aus. Territorialität wird durch Virtualität ergänzt. Ein Aufteilen in Gefechtsstreifen mit klaren räumlichen Grenzen ist nicht möglich. Gleiches gilt für das Manövrieren von Truppen. Trotzdem können auch im Cyber- und Informationsraum durchaus physische Wirkungen erzielt werden. Der Ort der Auswirkung von CIR-Operationen kann allerdings Zehntausende Kilometer entfernt von der Quelle der Aktivität liegen. Auch die Zeit hat eine andere Bedeutung. Schließlich

Unserem selbst gesteckten Ziel, den Cyber- und Informationsraum mit all seinen Facetten ganzheitlich zu gestalten, sind wir bereits ein gutes Stück näher gekommen

kann die Wirkung im Cyberraum über eine beliebige Entfernung ohne Zeitverzug erzielt werden. Effekte können in Echtzeit erfolgen.

Problematisch gestaltet sich die Attribuierung von Angriffen. Aufgrund der technischen Möglichkeiten können Handlungen besonders gut verschleiert werden. Zudem gibt es eine Vielzahl potenzieller Tätergruppen und Motive. Durch die Möglichkeiten der Digitalisierung können inzwischen nicht staatliche Akteure über Cyberangriffe Effekte erzielen, die bisher staatlichen Akteuren vorbehalten waren. Die Gefahrenlage hat sich durch die Digitalisierung deutlich verkompliziert. Es gilt grundsätzlich zu klären: Von wem werden wir gerade angegriffen und mit welchem Ziel? In diesem Zusammenhang kommt der Attributionsthematik in ihren technischen, rechtlichen und politischen Aspekten eine besondere Bedeutung zu. Für den Fall der Bündnis- oder gar Landesverteidigung müssen verbindliche internationale Regelungen, die vergleichbar für bewaffnete Konflikte zwischen Staaten gelten, auch auf den Cyber- und Informationsraum übertragen werden.

Die Wahrscheinlichkeit klassischer militärischer Auseinandersetzungen zwischen Industrienationen reduziert sich hin zu eher wahrscheinlichen hybriden Konfliktformen

Folgen der Digitalisierung

Veränderung des militärischen Konfliktbildes

Die zunehmende Digitalisierung hat gravierende Auswirkungen auf denkbare militärische Szenarien. Ein zukünftiges Konfliktbild wird im Kern von Hybridität, die Konfliktaustragung von Digitalität, künstlicher Intelligenz und Autonomie geprägt sein. Die Intensität der Aktionen kann dabei gezielt unterhalb der angenommenen Schwelle bleiben, die erforderlich ist, um sie als bewaffneten Angriff einstufen zu können. Damit reduziert sich die Wahrscheinlichkeit klassischer militärischer Auseinandersetzungen zwischen Industrienationen hin zu eher wahrscheinlichen hybriden Konfliktformen. Dennoch müssen konventionelle militärische Kräfte weiterhin in hinreichender Qualität und Quantität vorgehalten werden, um eine glaubhafte Abschreckung zu gewährleisten.

CIR-Operationen – eigenständig oder unterstützend – gewinnen weiter an Bedeutung. Sie sind als Operationen der ersten Stunde denkbar, gegebenenfalls schon zu einem Zeitpunkt, zu dem „konventionelle Kräfte“ noch nicht alarmiert sind. Schließlich werden bereits heute staatliche und innerstaatliche Konflikte mehr und mehr durch Propaganda und Desinformation beeinflusst. Streitkräfte werden zukünftig differenzierter und spezialisierter sein. Es ist ein neues Denken für Operationen im Cyber- und Informationsraum notwendig. Sie sind ein eigenständiges Operationsfeld, unterstützen aber auch im Rahmen klassischer militärischer Einsätze als Bestandteil von Land-, Luft- oder Seeoperationen. Wir müssen Fähigkeiten zu CIR-Operationen im gesamten Spektrum ausbauen und damit der Politik nicht kinetische Handlungsoptionen bieten.

Konsequenzen für Organisation und Prozesse

Die zunehmende Digitalisierung hat Auswirkungen auf unterschiedlichste Bereiche innerhalb der Streitkräfte. Dabei versucht die Bundeswehr selbstverständlich möglichst viele Vorteile der Digitalisierung zu nutzen. Anwendungsmöglichkeiten gibt es neben den Führungs- und Waffensystemen zum Beispiel auch im Bereich des Personalmanagements, der Logistik, des Energiemanagements sowie bei der Erstellung von Lagebildern und Vorhersagen.

Die Organisation muss sich an die Anforderungen der Digitalisierung anpassen. So geht es nicht um die IT-Unterstützung für bestehende Prozesse, sondern um die Anpassung und Optimierung von Prozessen aufgrund der Möglichkeiten der Digitalisierung. Wir benötigen neue Strategien als gesamtstaatliche Antwort auf das von mir dargestellte hybride Konfliktbild. Brauchen wir gesamtstaatlich eine Anpassung von Regelungen und Befugnissen, um auf Szenare eines „digitalen Verteidigungsfalls“ adäquat reagieren zu können?

Außerdem muss die Ethik eines digitalen Konfliktes gesamtgesellschaftlich und in der Bundeswehr intern diskutiert werden. Aus meiner

Sicht ist es zwingend erforderlich, verbindliche internationale Regelungen zu schaffen. Es gilt, das Kriegsvölkerrecht an die modernen Formen der Konfliktführung anzupassen. Hierfür muss ein internationaler Konsens zur Anwendung unter anderem ethischer Schlüsselbegriffe wie beispielsweise „Leid“ und „Angriff“ auf die Domäne Cyber gefunden werden. Als Richtschnur sollten dabei die ethischen Normen dienen, die sich als Grundlage bisherigen Völkerrechts bewährt haben. Mit dem *Tallinn Manual 2.0* existiert bereits seit 2017 eine gute Basis.

Zudem müssen insbesondere bei Waffensystemen auch ethische Aspekte berücksichtigt werden. Ein verantwortungsvoller Umgang mit neuen Technologien ist zwingend notwendig. Nicht alles, was technisch möglich ist, sollte zwingend realisiert und legitimiert werden. Das gilt auch für das Thema künstliche Intelligenz.

Konsequenzen für Führung und Führungsverfahren, für Ausbildung und „Kultur“

Führungsebenen und Führungsverfahren müssen geprüft und adaptiert werden. Ein umfassendes Lagebild und automatisierte Handlungsempfehlungen werden zukünftig vermehrt auf höheren Ebenen zusammenkommen. Befehlsgebung und deren Umsetzung in Hierarchien müssen vor diesem Hintergrund neu betrachtet werden. Grundsätzlich müssen wir uns Fragen stellen wie: Sind die Werkzeuge und Verfahren von früher heute noch die richtigen? Bieten nicht moderne Werkzeuge wie Design Thinking hier alternative Ansätze?

Die Digitalisierung wird auch das Berufsbild des Soldaten verändern. Wir benötigen eine digitale Unternehmenskultur in den Streitkräften. Der Ausbau einer Cyber-Awareness bei allen Angehörigen der Bundeswehr bis hin zur Entwicklung einer Cybersicherheitskultur ist von elementarer Bedeutung. Im digitalen Zeitalter sind andere Qualifikationen gefordert als noch zu Zeiten des Kalten Krieges. Dies gilt es auch bei der Führung zu berücksichtigen. Wir müssen innovatives Denken zulassen, reflektieren und nicht durch Konformitätszwang unterdrücken. Eine schnelle, hierarchieübergreifende Kommunikation muss akzeptiert und gelebt werden. Und natürlich müssen die Streitkräfte bei den Themen Personalgewinnung und Karrierepfade flexibler werden, um die dringend benötigten Talente zu gewinnen und zu binden.

Das Kommando Cyber- und Informationsraum hat sich auf die neuen Gegebenheiten bereits eingestellt. Wir sehen uns als wesentlichen Treiber für die Weiterentwicklung der Bundeswehr mit Blick auf die Digitalisierung. Wir gehen in unserem Organisationsbereich neue und innovative Wege, etablieren schnellere Prozesse – beispielsweise durch die Nutzung spezieller kollaborativer Software – und fördern Eigeninitiative. Hierfür wenden wir neue Verfahren und Prinzipien in der Zusammenarbeit an und sind damit Vorreiter für die gesamte Bundeswehr.

Voraussetzung für den Schutz vor den Herausforderungen der Digitalisierung

Enge nationale und internationale Zusammenarbeit

Das Internet kennt keine natürlichen Grenzen. Effekte und Angriffe können alle Treffen: Staaten, Wirtschaftsunternehmen und Privatpersonen. Eine enge nationale und internationale Zusammenarbeit ist daher für einen effektiven Schutz gegen die Gefahren aus dem Cyberraum zwingend erforderlich.

Grundlage für die nationale Zusammenarbeit bildet die Cyber-Sicherheitsstrategie der Bundesregierung, die 2016 erlassen wurde. Danach liegt die Verantwortung für die Cybersicherheit beim Bundesministerium des Inneren. Verteidigungsaspekte der gesamtstaatlichen Cybersicherheitsarchitektur werden gemäß Weißbuch 2016 als originäre Aufgaben dem Bundesverteidigungsministerium und als verfassungsgemäßem Auftrag der Bundeswehr zugewiesen. Dabei ist es Aufgabe der Sicherheits- und Verteidigungspolitik, die territoriale Unversehrtheit sowie die Souveränität Deutschlands und seiner Verbündeten zu wahren.

Im digitalen Zeitalter sind andere Qualifikationen gefordert als noch zu Zeiten des Kalten Krieges. Dies gilt es auch bei der Führung zu berücksichtigen

Hybride Strategien nutzen die Nahtstellen von Zuständigkeiten, wie beispielsweise der inne-

ren und äußeren Sicherheit, für ihre Ziele aus. Ein enger Schulterschluss und Austausch im nationalen Rahmen ist daher äußerst wichtig. Hierfür wurde bereits 2011, unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik, ein erstes Forum für die Zusammenarbeit staatlicher Stellen im Cyber- und Informationsraum geschaffen, das Nationale Cyber-Abwehrzentrum. Dieses wird aktuell zu einer ressortübergreifenden, operative Institution unter Einbindung aller wichtigen Akteure weiterentwickelt – ein essenziell wichtiger Schritt, um die zukünftige Handlungsfähigkeit Deutschlands auf diesem Gebiet zu gewährleisten. Dabei ist auch die Einbindung nationaler Internet Service Provider unabdingbar. Der Organisationsbereich CIR bringt sich in diesen Prozess als Vertreter der Bundeswehr aktiv ein. In einem weiterentwickelten Nationalen Cyberabwehrzentrum könnten wir unter anderem Informationen aus unserem neuen gemeinsamen Lagezentrum zur Verfügung stellen.

Der Organisationsbereich CIR ist auf nationaler Ebene bereits eng mit allen wesentlichen Behörden und staatlichen Stellen vernetzt

Der Organisationsbereich CIR ist auf nationaler Ebene bereits eng mit allen wesentlichen Behörden und staatlichen Stellen vernetzt. Darüber hinaus haben wir erste Kooperationen mit Institutionen aus Wissenschaft und Wirtschaft abgeschlossen. So existieren beispielsweise eine Kooperation mit der Telekom und ein Bündnis für IT-Sicherheit mit dem Fraunhofer Institut FKIE. Die Ziele der Zusammenarbeit sind in beiden Fällen ein allgemeiner Informationsaustausch und Wissenstransfer, ein personeller Austausch im Rahmen von gegenseitigen Hospitationen sowie die beidseitige Öffnung und Unterstützung von Aus- und Weiterbildungsmaßnahmen für IT-Fachleute. Das Kommando CIR ist zudem Mitglied im Beirat des Ende letzten Jahres gegründeten Cyber Security Cluster Bonn e.V.

Ein enger Austausch ist auch auf internationaler Ebene zwingend erforderlich, denn: Der Cyber- und Informationsraum macht nicht an Staatsgrenzen halt. Im militärischen Bereich findet bereits eine sehr enge bilaterale Zusammenarbeit, aber auch eine auf EU- und NATO-Ebene statt. Der fachliche Transfer mit entsprechenden NATO-Stellen und die Beteiligung an gemeinsamen Foren sind mittlerweile etabliert. Gemeinsame Übungen auf strategischer und operativer Ebene finden in regelmäßigen Abständen statt.

Fazit

Bei allen beschrieben Aspekten wird deutlich: Die Digitalisierung hat die Bundeswehr bereits entscheidend geprägt und wird dies in Zukunft noch deutlicher tun. Die damit verbundenen Herausforderungen erfordern in vielen Bereichen neue Lösungen und Denkansätze. Wir müssen uns den erweiterten Möglichkeiten und auch den daraus resultierenden militärischen Szenaren stellen und uns entsprechend vorbereiten. Eine erfolgreiche Cyberabwehr ist eine strategische Frage für Staat, Wirtschaft und Gesellschaft. Eine wesentliche Rahmenbedingung hierfür sind verbindliche internationale Regelungen, die die Besonderheiten und die Schnelllebigkeit des Cyber- und Informationsraums berücksichtigen. Entscheidend hierbei sind nicht zuletzt völkerrechtliche und ethische Aspekte.

Nur gemeinsam können wir die Widerstandsfähigkeit gegenüber den Bedrohungen aus dem Cyber- und Informationsraum gewährleisten – eine Voraussetzung für die Zukunft moderner Gesellschaften. Der Organisationsbereich Cyber- und Informationsraum der Bundeswehr wird einen maßgeblichen Beitrag zu dieser wichtigen gesamtstaatlichen Aufgabe leisten und dabei mit allen ihm zur Verfügung stehenden Mitteln unterstützen!

Der Autor

__Ludwig Leinhos__ (geb. 1956) trat 1975 in die Bundeswehr ein. Der Generalleutnant der Luftwaffe hat nach dem Studium der Elektrotechnik Verwendungen in den Bereichen Nachrichtengewinnung und Aufklärung/ Elektronische Kampfführung absolviert. Sein militärischer Werdegang war von verschiedenen Führungsverantwortungen im In- und Ausland im Bereich Führungssysteme, IT-Planung und Anwendung geprägt; unter anderem war er Director NATO Headquarters C3 Staff in Brüssel. Seit dem 1. April 2017 ist General Leinhos der erste Inspekteur Cyber- und Informationsraum der Bundeswehr.

„ES GIBT HEUTE KEINE MILITÄRISCHE OPERATION, KEINEN MILITÄRISCHEN KONFLIKT OHNE EINE CYBERDIMENSION“

Interview mit
Generalmajor José Luis Triguero de la Torre

Herr Generalmajor, in der Abschlusserklärung des Brüsseler Gipfels von 2018 bekräftigt die NATO ihre Entschlossenheit, „das ganze Spektrum an Fähigkeiten einschließlich Cyberfähigkeiten für die Abschreckung in Bezug auf das gesamte Spektrum an Cyberbedrohungen einzusetzen“. Nur zum Verständnis: Wie sieht Abschreckung im Cyberspace aus?

Im weiteren Sinne definiert die NATO Abschreckung folgendermaßen: Es gilt, „einen potenziellen Angreifer davon zu überzeugen, dass die Folgen von Zwang oder bewaffneten Konflikten die potenziellen Gewinne überwiegen würden. Dies setzt die Aufrechterhaltung einer glaubwürdigen militärischen Fähigkeit und Strategie mit dem klaren politischen Willen zum Handeln voraus.“

Cyberbedrohungen für die Sicherheit des Bündnisses werden zunehmend häufiger, komplexer und zerstörerischer. Ein Cyberangriff auf einen Verbündeten kann uns alle betreffen.

Die Verbündeten haben deutlich gemacht, dass viele staatliche und nicht staatliche Akteure ihre Cyberfähigkeiten weiterentwickeln, wobei diese kostengünstig und zunehmend wirkungsvoll sind.

Angesichts der zunehmenden Vernetzung der Welt erwarten wir, dass potenzielle Gegner stärker auf den Cyberraum zurückgreifen, wenn sie politische, militärische oder wirtschaftliche Vorteile erzielen möchten.

Die NATO-Verbündeten tragen die Hauptverantwortung für ihre nationalen Cyberabwehrmechanismen. Auf dem Warschauer Gipfel 2016 haben sich die Staats- und Regierungschefs der Alliierten verpflichtet, vorrangig ihre Cyberabwehr zu stärken. Die NATO unterstützt ihre Mitgliedstaaten bei diesen Bemühungen.

Die NATO schützt ihre eigenen IT-Netzwerke rund um die Uhr vor Cyberangriffen. Wir verfügen über eine NATO Computer Incident Response Capability (NCIRC), die unter anderem ein reaktionsschnelles Cyberverteidigungsteam im 24-Stunden-Bereitschaftsmodus umfasst, das angegriffenen Alliierten helfen kann. Solche Teams können auf Anforderung eines Mitgliedstaates eingesetzt werden, um die nationalen Bemühungen in verschiedenen Bereichen zu unterstützen.

Abschreckung funktioniert auf herkömmliche Weise durch die Kommunikation von Fähigkeit und Bereitschaft. Ist dieses Konzept noch auf den Cyberbereich anwendbar? Wie können Cyberfähigkeiten kommuniziert werden, ohne sichtbar gegen den Adressaten der Abschreckung ausgeführt zu werden?

Maßnahmen der NATO, die im Hinblick auf die Cyberabwehr ergriffen wurden, waren transparent. Die Absicht der NATO, ihre Bevölkerung und ihr Territorium vor jeglicher Bedrohung, einschließlich Cyberbedrohungen, zu schützen, wurde klar kommuniziert.

Durch unsere öffentlichen Ankündigungen hat die Allianz deutlich gemacht, dass sie über die Fähigkeiten und die Bereitschaft verfügt, jeglichen potenziellen Angreifer und auch Angriffe aus dem Cyberbereich abzuschrecken.

Durch die Cyberabwehr konnten etwa Verbündete die Cybernetzwerke des IS stören, um dessen Rekrutierungs-, Finanzierungs- und Kommunikationsmöglichkeiten zu einzuschränken.

Im Juli 2016 bekräftigten die Alliierten das Verteidigungsmandat der NATO und erkannten den Cyberspace als Einsatzgebiet an.

Ein aktualisierter Aktionsplan zur Cyberabwehr wurde im Februar 2017 von den Mitgliedsstaaten gebilligt.

Die Richtlinie legt fest, dass Cyberverteidigung als Teil der kollektiven Verteidigung zur Kernaufgabe des Bündnisses gehört, bestätigt, dass das Völkerrecht im Cyberspace gilt, und intensiviert die Zusammenarbeit der NATO mit der Industrie. Oberste Priorität hat der Schutz der Kommunikationssysteme, die der Allianz gehören und von ihr betrieben werden.

Nach dem Brüsseler Gipfel 2018 einigten sich die Alliierten auch darauf, ein neues Cyberspace-Operationszentrum im Rahmen der ge-

stärkten Kommandostruktur der NATO einzurichten, und dass die NATO für ihre Missionen und Operationen auf nationale Cyberfähigkeiten zurückgreifen kann.

Die NATO Computer Incident Response Capability (NCIRC) mit Sitz im SHAPE, Mons, Belgien, schützt auch die eigenen Netzwerke der NATO, indem sie die verschiedenen NATO-Standorte zentral und rund um die Uhr bei der Cyberverteidigung unterstützt.

Offizielle Verlautbarungen unterstreichen die Notwendigkeit von Partnerschaften mit Industrie und Wissenschaft in Bezug auf Fragen der Cybersicherheit. Da Cyberoperationen Sicherheitslücken in Hard- und Software benötigen und die beste Cyberverteidigung darin besteht, relevante Sicherheitslücken zu schließen: Welche Rolle spielt die Industrie in der Zusammenarbeit mit der NATO und ihren Mitgliedstaaten genau?

Unsere erweiterte Cyberpolitik definiert Wege, um Sensibilisierung, Bildung, Schulung und Übungsaktivitäten voranzubringen, und ermutigt zu weiteren Fortschritten bei verschiedenen Kooperationsinitiativen, einschließlich solcher mit Partnerländern und internationalen Organisationen.

Wir bauen außerdem unsere Partnerschaft mit Industrie und Wissenschaft aller Alliierten weiter aus, um mit dem technologischen Fortschritt durch Innovation Schritt zu halten. Das Fachwissen im privaten Sektor ist von entscheidender Bedeutung, weshalb die NATO ihre Beziehungen zur Industrie in der NATO Industry Cyber Partnership (NCIP) durch Informationsaustausch, Schulung und Übungen stärkt. Diese Partnerschaft stützt sich auf bestehende Strukturen und umfasst NATO-Einheiten, nationale Computer Emergency Response Teams (CERTs) und Industrievertreter der NATO-Mitgliedstaaten.

Um auf dem neuesten Stand der Cyberverteidigungspraxis zu bleiben, führt die NATO auch regelmäßig Übungen durch, wovon einige auch für Industriepartner offen sind. Cyber Coalition ist die jährliche Leuchtturmübung der NATO im Bereich der Cyberverteidigung und eine der größten der Welt. Die Übung testet und schult Cyberverteidiger aus dem gesamten Bündnis in ihrer Fähigkeit, NATO- und nationale Netzwerke zu verteidigen.

Von der Abwehr von Malware über hybride Herausforderungen, in denen auch soziale Medien eine Rolle spielen, bis hin zu Angriffen auf mobile Geräte bietet die Übung ein anspruchsvolles, realistisches Szenario, das unsere Cyberverteidiger auf echte Cyberherausforderungen vorbereitet. Industrie und Wissenschaft beteiligen sich ebenfalls an der Cyber Coalition.

Ein weiteres Beispiel für Übungen im Zusammenhang mit der NATO, die für die Industrie offen sind, ist die Übung Locked Shields 2019. Sie wird jährlich durch das NATO Cooperative Cyber Defence Centre of Excellence organisiert und fand in diesem Jahr vom 8. bis 12. April statt.

Diese Übung ermöglicht es Cybersicherheitsexperten, ihre Fähigkeiten zur Verteidigung nationaler IT-Systeme und kritischer Infrastrukturen bei Echtzeitangriffen zu verbessern. Der Fokus liegt auf realistischen Szenarien, modernsten Technologien und der Simulation der gesamten Komplexität eines massiven Cybervorfalls, einschließlich von Aspekten strategischer Entscheidungsfindung, des Rechts und der Kommunikation.

Die diesjährige Übung wurde in Zusammenarbeit mit den estnischen und finnischen Streitkräften, dem Europäischen Kommando der Vereinigten Staaten, dem Nationalen Sicherheitsforschungsinstitut der Republik Korea, der Technischen Universität Tallinn und einer organisiert, Vertreter der Industrie waren maßgeblich daran beteiligt.

Zur Person

***Generalmajor José Luis Triguero de la Torre** trat 1975 in die Spanische Luftwaffenakademie ein ein. Er hat mehr als 35 Jahre Erfahrung in der Spezifikation, Entwicklung, Beschaffung, Implementierung und Steuerung von bedeutenden CIS- und C2-Systemen auf verschiedenen Verantwortungsebenen. Zudem verfügt er über umfangreiche Kenntnisse im Bereich Cyberabwehr. Im März 2016 übernahm Generalmajor Triguero del Torre den Posten des Direktors NATO Headquarters Consultation, Command and Control Staff (NHQC3S) im NATO-Hauptquartier.*

Der gebürtige Madrilene ist verheiratet, hat drei erwachsene Söhne und eine Enkelin.

Die NATO betrachtet – wie Sie eben erwähnten – die Cyberverteidigung als Teil der kollektiven Verteidigung und erklärt, dass eine Berufung auf Artikel 5 von Fall zu Fall erfolgen kann. Einige Leute sagen, dass es einen andauernden Cyberkrieg zwischen Mitgliedstaaten und feindlichen Mächten gibt, einschließlich staatlicher und nicht staatlicher Akteure. Wie weit sind wir also von einem Artikel-5-Szenario entfernt?

Das Hauptaugenmerk der NATO auf dem Gebiet der Cyberverteidigung liegt auf dem Schutz ihrer eigenen Netze (einschließlich Operationen und Missionen) und der Verbesserung der Resilienz im gesamten Bündnis. Wir sind uns natürlich bewusst, dass der Cyberspace in vielerlei Hinsicht eine Herausforderung darstellt. Es gibt heute keine militärische Operation, keinen militärischen Konflikt ohne eine Cyberdimension.

Wir sind uns auch bewusst, dass der Cyberraum für den Versuch genutzt wurde, sich in politisch-demokratische Prozesse innerhalb des Bündnisses einzumischen. Dies ist einer der Gründe, warum wir unsere Cyberabwehr, die Widerstandsfähigkeit unserer Cybernetzwerke und die Sensibilität der Alliierten deutlich verbessert haben und warum die Alliierten entschieden haben, dass Cyberangriffe Artikel 5 auslösen können.

Zur Frage, wie weit wir von einem Artikel-5-Szenario entfernt sind: Ich halte es nicht für angebracht, darüber zu spekulieren, welche Art von Cyberangriff den Artikel 5 auslösen würde. Jede Entscheidung, sich auf Artikel 5 zu berufen, und die mögliche Reaktion der Allianz wären abhängig vom Kontext und würden auf einer politische Entscheidung basieren. Die Antwort der Allianz könnte diplomatische und wirtschaftliche Sanktionen, Cyberreaktionen oder sogar den Einsatz konventioneller Streitkräfte umfassen, je nach Art und Folgen des Angriffs. Aber was auch immer die Antwort sein mag, die NATO wird weiterhin dem Grundsatz der Zurückhaltung folgen. Und im Einklang mit dem Völkerrecht handeln.

Um sich nun einer anderen Dimension der Sicherheit zuzuwenden: Dialog wird zusammen mit Abschreckung oft als eine der beiden Seiten derselben Medaille wahrgenommen. Welche Möglichkeiten zur Förderung eines neuen Dialogs bietet der Cyberspace?

Dialog ist auf allen Gebieten wichtig. Transparenz hat für unser Bündnis Priorität, und unsere Bürger verdienen es, zu wissen, was wir tun.

Was auch immer die Antwort auf einen Cyberangriff sein mag, die NATO wird weiterhin dem Grundsatz der Zurückhaltung folgen. Und im Einklang mit dem Völkerrecht handeln

Der Cyberspace bietet viele Möglichkeiten für den Dialog. Über die Online-Welt können die Alliierten sofort miteinander kommunizieren und die breite Öffentlichkeit sowie Medienorganisationen erreichen.

Die NATO unterstützt auch Bemühungen, wie etwa bei den Vereinten Nationen und der OSZE, um Frieden und Sicherheit im Cyberspace aufrechtzuerhalten, die Stabilität zu fördern und das Konfliktrisiko zu verringern.

Herr Generalmajor, wir bedanken uns für das Interview!

„ERSTE ERFOLGE IN DER CYBERDIPLOMATIE SIND BEREITS SICHTBAR“

Interview mit ***Kapitän zur See Matthias Friese***

Die Teilnehmerstaaten der OSZE haben ja bereits vor Jahren – 2013 und zuletzt 2016 – eine Reihe von Vertrauensbildenden Maßnahmen in Bezug auf die Cybersicherheit beschlossen. In letzter Zeit hört man aber immer wieder von Cyberattacken, die ihren Ursprung in Teilnehmerstaaten der OSZE haben. Nicht wenige reden gar von einem Cyberkrieg. Versagt die Cyberdiplomatie?

Nein! Ich verstehe zwar durchaus die kritische Herangehensweise an den Begriff „Cyberdiplomatie“, denn die Vorfälle, von denen man hört, sind durchaus sehr problematisch. Dennoch zeigen sie meines Erachtens sehr deutlich, dass wir mehr Cyberdiplomatie brauchen und nicht, dass sie gescheitert ist. Gerade im Angesicht der Tatsache, dass Cyberangriffe auf technischer Ebene stattfinden, ist es elementar wichtig, auf politischer Ebene Kontakte und Kommunikationsmöglichkeiten zu haben. Diese bietet eben die OSZE. Lassen Sie mich dazu von den 2013 und 2016 beschlossenen Vertrauensbildenden Maßnahmen (VBM) nur drei hervorheben, um das etwas genauer zu illustrieren. Nach VBM 3 erklären alle Teilnehmerstaaten, Konsultationen durchzuführen. Das klingt möglicherweise profan, aber es ist – neben technischen Bewertungen – eben von zentraler Bedeutung, auf politischer Ebene miteinander zu reden, um Spannungen oder Konflikte sich nicht weiter verschärfen zu lassen. Daher ist die hier gezeigte Dialogbereitschaft sehr wichtig. Auf ihr aufbauend wird es dann in VBM 8 schon konkreter. Danach ist es gelungen, ein Cyber-Kontaktpunktenetzwerk (Point-of-Contact Network) aufzubauen, und heute haben bereits 54 Staaten ihre nationalen Cyberverantwortlichen nominiert. Dieses Netzwerk bietet eine schnelle Kommunikationsmöglichkeit von Staat zu Staat, um bei etwaigen Zwischenfällen im Bereich Cyber beziehungsweise Informations- und Kommunikationstechnologie, die einzelne oder mehrere OSZE-Teilnehmerstaaten betreffen, zügig auf politischer Ebene reagieren zu können. Das Auswärtige Amt fördert übrigens mit finanziellen Mitteln den weiteren Ausbau dieses Kontaktpunktenetzwerks nach VBM 8.

Es ist elementar wichtig, auf politischer Ebene Kontakte und Kommunikationsmöglichkeiten zu haben. Diese bietet die OSZE

Eine wichtige Ergänzung zur Implementierung dieser politischen Konsultationen verbirgt sich hinter VBM 13 (Nutzung gesicherter und autorisierter Kommunikationskanäle). Hier ist beabsichtigt, das bereits bestehende OSZE-Kommunikationsnetz (OSCE Communication Network), das seit langer Zeit erfolgreich für Informationsaustausch in der konventionellen Rüstungskontrolle genutzt wird, für Cybersicherheit mitzunutzen. Dieses Netzwerk besteht physisch aus extra abgesicherten Terminals zum Austausch sensibler Daten und Informationen zwischen den OSZE-Teilnehmerstaaten. Das Forum für Sicherheitskooperation hat der Mitnutzung zugestimmt. Jetzt wird die praktische Ausgestaltung erarbeitet.

Alles in allem sieht man, dass die OSZE konkret an einer Verbesserung beziehungsweise Vertiefung und praktischen Umsetzung der internationalen Cyberdiplomatie arbeitet und erste Erfolge hier bereits sichtbar sind.

Nun beruhen jedoch die beschlossenen VBM zur Transparenz, Zusammenarbeit und Stabilität sämtlich auf Freiwilligkeit – sind also rechtlich unverbindlich. Ist dies hinreichend, um zu gewährleisten, dass im Cyberspace kein Konflikt entsteht, der sich zu einem konventionellen Krieg entwickeln kann?

Ich denke, hier lohnt es sich, ein wenig weiter auszuholen: Die OSZE ist eine regionale Sicherheitsorganisation nach Kapitel VIII der Charta der Vereinten Nationen (VN). Ihr Zweck ist komplementär zum Ziel der VN, Streitigkeiten und Konflikte friedlich beizulegen. Hierzu hat die OSZE schon vor geraumer Zeit sogenannte transnationale Bedrohungen, beispielsweise transnationalen Terrorismus oder organisierte Kriminalität, identifiziert und fördert Dialog und Zusammenarbeit auf regionaler Ebene gegen diese Bedrohungen. Cybersicherheit ist 2012 als eine neuere Form der transnationalen Bedrohungen hinzugekommen. Im Kern geht es darum, durch Vertrauensbildung auf regionaler Ebene zu verhindern, dass Spannungen oder Krisen zwischen Staaten zu Konflikten eskalieren. Diese Gefahr besteht sehr konkret durch Cyberattacken. Wird ein Staat, der sich gerade in politisch zunehmenden Spannungen mit einem anderen befindet, im Cyberraum angegriffen, besteht durch fehlende oder ungenaue Attribution, den Beweis der Urheberschaft des Angriffs, oft eine akute Eskalationsgefahr, da möglicherweise vorschnell der Angriff diesem anderen Staat zur Last gelegt wird. Dies soll durch die Vertrauensbildung, Transparenz und Kommunikation zwischen den Teilnehmerstaaten der OSZE verhindert werden.

Zur Frage der Freiwilligkeit muss man vielleicht sagen: Es gehört zum Wesenskern einer Vertrauensbildenden Maßnahme, dass diese aus freier Entscheidung beiderseitig vereinbart wird. Insofern hat es schon einiges an Gewicht, wenn der Ministerrat der OSZE, das heißt konkret alle 57 Außenminister der Teilnehmerstaaten, einstimmig die Entscheidung des Ständigen Rates 1202 zu den Cyber-VBM gebilligt und alle Teilnehmerstaaten zur weiteren praktischen Implementierung der VBM ermutigt haben. So ist dies ja geschehen auf dem OSZE-Ministerrat 2016 – übrigens in Hamburg unter deutschem Vorsitz.

Die Freiwilligkeit der Staaten ist also insofern kein Manko, sondern extrem wichtig, um Vertrauen aufzubauen und zu vertiefen.

Viele Experten bezweifeln, dass effektive Rüstungskontrolle im Cyberspace überhaupt möglich sei. Es ist ja auch nur schwer möglich, Computerwürmer und Softwareschwachstellen so zu zählen wie Panzer und Raketen. Wie wird in der OSZE diese Problematik diskutiert?

Zugegeben: Das ist durchaus richtig und beschreibt die Problematik der Cybersphäre ziemlich gut. Umso wichtiger ist es, Möglichkeiten zur Konfliktverhütung im Cyberraum zu suchen, und hier können die Erfahrungen aus der konventionellen Rüstungskontrolle nur hilfreich sein. Man sollte Rüstungskontrolle nicht nur als „in Stein gemeißeltes" Vertragswerk betrachten und nur dessen Effektivität beurteilen. Viel eher sollte man sie als fortwährenden Prozess verstehen, in welchem verschiedene Parteien aufeinander zugehen, sich austauschen und bestenfalls letztendlich kooperieren. Schauen wir auf die Entwicklung der klassischen Rüstungskontrolle im OSZE- Bereich, so ist diese ja auch erst langsam entstanden. Damals wurde im Rahmen der KSZE in einem ersten Schritt die Grundlage gelegt, indem die einzelnen Staaten für Transparenz sorgten. So hat man durch den gegenseitigen Austausch eigener Daten, Absichten und Pläne allmählich eine Vertrauensbasis geschaffen; manchmal auch unterlegt durch Verifikationsregime. Darauf aufbauend war es möglich, konkrete Maßnahmen und

Die Freiwilligkeit der Staaten ist kein Manko, sondern extrem wichtig, um Vertrauen aufzubauen und zu vertiefen

Mechanismen zur Rüstungskontrolle und sogar Abrüstung auszuhandeln und zu vereinbaren. Ganz Ähnliches wird nun in der OSZE im Bereich Cyber versucht, das ja sicherheitspolitisch ein relativ neues Feld ist. Regelmäßig informieren OSZE- Teilnehmerstaaten über nationale Entwicklungen im Bereich Cyber, zum Beispiel neue Cyberstrategien, Gesetzgebung und Aktivitäten. Auch auf die Gefahr hin, dass ich mich wiederhole: Auf der politischen Ebene ist es von herausragender Wichtigkeit, miteinander zu reden, um Vertrauen zu schaffen und darauf aufbauend überhaupt erst konkrete Maßnahmen zu vereinbaren.

Derzeit wird in Deutschland ja die Option von staatlich ausgeführten Hackbacks offen diskutiert. Können sie einschätzen, ob diese Option auf dem „Austausch bewährter Verfahren“ nach VBM 15 beruht? Haben überhaupt schon Teilnehmerstaaten ihre Erfahrungen in der aktiven Cyberabwehr im Rahmen der OSZE geschildert?

Mit Sicherheit nicht. Konkrete (technische) Gefahrenabwehr bleibt Verantwortung und Aufgabe der einzelnen Staaten, die dazu über geeignete Instrumente und Einrichtungen verfügen – meist im Bereich der Innenministerien und Sicherheitsbehörden –, welche mit Sicherheit auf ihrer Ebene wiederum international vernetzt sind. Jedenfalls gibt es in der OSZE keine gemeinsame Planung oder Koordination oder Austausch zu aktiver (praktischer) Cyberabwehr. Die VBM 15 zielt auf einen besseren Schutz der Vulnerabilitäten von Staaten, insbesondere den Schutz von kritischen Infrastrukturen. Dazu sollen unter anderem der Austausch von Informationen, Erfahrungen und bewährter Praxis dienen sowie ein gemeinsames Verständnis über die Gravität beziehungsweise die Bedeutung von Cyberzwischenfällen.

Wann ist denn mit einem völkerrechtlich verbindlichen Cyberwaffenbegrenzungs- oder besser: -verbotsvertrag zu rechnen?

Nun, da fragen Sie ein wenig über den Rahmen der OSZE hinaus. Die Federführung in einem solchen Prozess läge bei den VN. Zu Cyber hat der VN-Generalsekretär seit 2004 sogenannte Governmental Groups of Experts (GGE) zur Entwicklung von Cybernormen einberufen. Die letzte GGE lief sogar unter deutschem Vorsitz. Demnächst beginnen in New York sogar zwei hochrangige Gremien die weitere Arbeit: eine GGE, bestehend aus 25 hochrangigen Experten, sowie eine Open-ended Working Group, zu der alle VN-Staaten beitragen können. Die Bundesrepublik Deutschland wird sich sehr aktiv an beiden Gremien beteiligen. Daran erkennt man die Absicht, internationale Normen für diese neue Herausforderung zu schaffen, aber man weiß auch, dass dabei „ein dickes Brett zu bohren ist“, das viel Zeit benötigen wird. Neu ist, dass die GGE plant, frühzeitig im Prozess die Erfahrungen beziehungsweise Arbeit von regionalen Sicherheitsorganisationen kennenzulernen. Vielleicht erleben wir hier also einen Beitrag der OSZE zum Entstehen internationaler Normen. Zuerst wird die GGE übrigens mit der OSZE sprechen, die Termine dafür sind bereits vereinbart. Die Arbeit der OSZE zur Vertrauensbildung im Cyberbereich haben ohnehin international Modellcharakter, denn zum Beispiel das ASEAN Regional Forum (ARF) hat 2018 mit der Entwicklung von Cyber-VBM im südostasiatischen Raum auf der Basis der Entscheidung 1202 des Ständigen Rates begonnen.

Man sieht also, und das ist mein Credo, internationale sicherheitspolitische Zusammenarbeit braucht Zeit und vor allem gegenseitiges Vertrauen sowie Organisationen wie die OSZE. Dies ist eine wichtige Grundlage für eine friedliche internationale Ordnung, ob „analog“ oder digital.

Herr Kapitän, herzlichen Dank für dieses Gespräch!

Zur Person

Kapitän zur See Diplom-Ingenieur Matthias Friese
Militärpolitischer Berater, Ständige Vertretung Deutschlands bei der OSZE, unter anderem zuständig für Cyber. Verwendungen im Bereich Marineflieger einschließlich Kommandeur. Admiralstabslehrgang. Referent in der Militärpolitikabteilung und im Büro des Parlamentarischen Staatssekretärs im BMVg sowie im Planungsstab des Verteidigungsministers. Studienleiter an der Bundesakademie für Sicherheitspolitik. Stellvertretender Kommandeur Landeskommando BAYERN und Standortältester München.
Veröffentlichungen zur Sicherheitspolitik, zu Afghanistan und zur Marine (geschichte).

ADIC – Agentur für Innovation in der Cybersicherheit / Agency for Innovation in Cybersecurity
Ursprünglich als „Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien“ gegründet.
Originally founded as "Agency for Disruptive Innovations in Cybersecurity and Key Technologies".

ARPANET – Advanced Research Projects Agency Network
Durch die US Air Force ab 1968 betriebenes dezentrales Computernetzwerk. Vorläufer des Internets.
Decentralized computer network operated by the US Air Force since 1968. Forerunner of the internet.

ASEAN – Verband südostasiatischer Nationen / Association of Southeast Asian Nations

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe / Federal Office of Civil Protection and Disaster Assistance

BSI – Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

CERT - Computer Emergency Response Team

CyberAZ – Cyber Abwehrzentrum / Cyber Defense Center

DARPA -Organisation für Forschungsprojekte der Verteidigung; Behörde des US Verteidigungsministeriums / Defense Advanced Research Project Agency; Agency of the US Department of Defense

DoS/DDoS – Denial of Service/Distributed Denial of Service (deutsch: Verweigerung des Dienstes/ verteilte Verweigerung des Dienstes)
Nichtverfügbarkeit eines Internetdienstes, meist durch Überlastung der Datenleitung
Unavailability of an Internet service, usually due to overloading of the data line

GGE – UN-Gruppe von Regierungssachverständigen / Group of Governmental Experts

Hackback
Wörtlich „Zurückhacken“, virtueller Gegenangriff
Literally, virtual counterattack

IKT/ICT – Informations- und Kommunikationstechnologie / Information and Communications Technology

IoT – Internet der Dinge / Internet of Things

KdoCIR – Kommando Cyber- und Informationsraum / Cyber and Information Domain Service

KRITIS-Verordnung
Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz
Ordinance on the Determination of Critical Infrastructures under the BSI Act

NCDA – Nationale Cyber Verteidigungsbehörde. In Deutschland ist dies das BSI. / National Cyberdefence Authority. In Germany the BSI.

NCIRC – NATO-Reaktionsfähigkeit bei Computerereignissen / NATO Computer Incident Response Capability
Teil der NATO Communications and Information Agency zum Schutz von NATO-Netzwerkstrukturen.
Part of the NATO Communications and Information Agency for the protection of NATO's network structures.

PKGrG – Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumsgesetz) / Law on the parliamentary control of Federal intelligence service (Control Body Act)

script kiddies
Stereotyp über laienhafte, meist jugendliche Computernutzer, die ohne tiefergehende Computer- und Programmierkenntnisse, meist mittels gekaufter Scripts, in fremde Computersysteme eindringen.
Stereotype about amateur, mostly juvenile computer users, who penetrate without deep computer and programming knowledge, mostly by means of bought scripts, into foreign computer systems.

Stuxnet Worm
Hoch entwickelter Computerwurm, der im Jahre 2010 die Urananreicherungsanlagen im iranischen Natanz zerstörte.
Sophisticated computer worm that destroyed uranium enrichment facilities in Natanz, Iran, in 2010.

TCP/IP – Transmission Control Protocol/Internet Protocol
Internetprotokoll, Basis für die Netzwerkkommunikation im Internet
Basis for network communication on the Internet

VBM/CBM – Vertrauensbildende Maßnahmen / Confidence Building Measures

Zero-Day Exploit
Schwachstelle in einer Computersoftware, für die noch keine Beseitigungsmöglichkeit (Patch/Softwareupdate) besteht
Vulnerability in a computer software for which a removal patch does not yet exist

ZITiS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich / Central office for information technology in the security sector

VORSCHAU / ALLE AUSGABEN

www.ethikundmilitaer.de

Diese und alle anderen Ausgaben von „Ethik und Militär" finden Sie **in Deutsch und Englisch** auf der Homepage des E-Journals.

Die kommende Ausgabe

Nächster Themenschwerpunkt von„Ethik und Militär" **(ab 2.12.2019): Ethische Bildung**

Bisher erschienene Ausgaben von „Ethik und Militär"

2018/2 Europäische Armee
2018/1 Strategic Foresight
2017 Terror
2016 Innere Führung
2015/2 Hybride Kriege
2015/1 Militärmedizinethik
2014/2 Cyberwar
2014/1 Dronen und LAWS

IMPRESSUM

Das E-Journal „Ethik und Militär" mit der ISSN-Nummer 2199-4129 ist ein unentgeltliches, nicht kommerzielles, journalistisch-redaktionell gestaltetes, digitales Angebot des Zentrums für ethische Bildung in den Streitkräften – zebis, Herrengraben 4, 20459 Hamburg.
Direktorin des zebis: Dr. Veronika Bock

Hinweis: Die veröffentlichten Artikel geben nicht unbedingt die Meinung der Redaktion und des Herausgeberkreises wieder.

Herausgeber
Prof. Dr. Andreas Bock, Dr. Veronika Bock,
Prof. Dr. Thomas Elßner, Dr. Johannes Frühbauer,
Prof. Dr. Fred van Iersel, Prof. Dr. Alexander Merkl

Advisory Board
Lothar Bendel, Heinrich Dierkes, Dr. Angela Reinders,
Cornelius Sturm, Kristina Tonn

Redaktion
Jan Peter Gülden
Rüdiger Frank

Verantwortlich gemäß § 55 Abs.2 Rundfunkstaatsvertrag (RStV):
Dr. Veronika Bock, Herrengraben 4, 20459 Hamburg

Kontakt zur Redaktion
Tel.: +49(0)40 - 67 08 59 - 51, Fax 67 08 59 - 3
E-Mail: redaktion@zebis.eu

Diensteanbieter als Rechtsträger des Zentrums für ethische Bildung in den Streitkräften – zebis
Katholische Soldatenseelsorge (KS)

Rechtsform
Anstalt des öffentlichen Rechts

Aufsicht
Katholischer Militärbischof für die
Deutsche Bundeswehr
Am Weidendamm 2, 10117 Berlin

Vertretungsberechtigter Vorstand der KS
Leitender Militärdekan
Msgr. Wolfgang Schilk
Diplom-Kaufmann Wolfgang Wurmb
Am Weidendamm 2
10117 Berlin

Kontakt zur KS
Telefon: +49(0)30 - 20 617 - 500
Telefax: +49(0)30 - 20 617 - 599
Info@Katholische-Soldatenseelsorge.de

Erscheinungsdatum: 1.12.2018

ethikundmilitaer.de

zebis
Zentrum für ethische Bildung in den Streitkräften
Herrengraben 4
20459 Hamburg

Tel. (040) 67 08 59 - 55
Fax (040) 67 08 59 - 59

info@zebis.eu
www.zebis.eu