Mehr Verantwortung für den Cyberspace – aber wie?

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 Rüstungskontroll-vorschläge.

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.

Cyberangriffen ist breit und 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 einen 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 Beispiele sind die Erpressungssoftware WannaCry und Bad Rabbit. Diese Aktionen richten erheblichen ökonomischen oder psychologischen Schaden an, gelten aber nicht als unmittelbare Kriegshandlung.

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

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 Cyberpolitik 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

Domäne für Soldaten, nicht nur ein Netzwerk für Spione.

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

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]

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

offensive Operationspotenziale, Cyberdoktrinen und die Funktion damit belasteter 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 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

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.

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. 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. 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. 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. www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf (Stand: 26.4.2019).

6 U. S. Joint Chiefs of Staff (2018): „Cyberspace Operations“, Joint Publication 3-12, 8. Juni 2018,

S. II-5. 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“. media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf (Stand: 26.4.2019).

9 „Information Security Doctrine of the Russian Federation“. 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. 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. 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. 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. 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 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.

Autor

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.

neuneck@ifsh.de

Lesen Sie auch:

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

"Erste Erfolge in der Cyberdiplomatie sind bereits sichtbar"
Matthias Friese

Cyberwar: die digitale Front - ein Angriff auf Freiheit und Demokratie?
Ethik und Militär 02/2014

Alle Ausgaben

Mehr Informationen zum zebis

Militärbischofs für die Deutsche Bundeswehr am Institut für Theologie und Frieden (ithf) errichtet.