Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet von Aaron Lye (Universität Bremen und FIfF) und *Wenn Big Data tödlich ist – Globale Überwachung und Drohnenkrieg* von Norbert Schepers (Rosa-Luxemburg-Stiftung, Bremen). Die Moderation hatten Eva Böller (Bremische Stiftung für Rüstungskonversion und Friedensforschung) und Barbara Heller (Bremer Friedensforum). Das Cyberpeace-Forum wurde organisiert vom Bremer Friedensforum, von der Bremischen Stiftung für Rüstungskonversion und Friedensforschung, vom Cyberpeace-Team Bremen, von der Bremer Regionalgruppe des FIfF und von der GEW Bremen. Die Podiumsdiskussion am Freitag wurde außerdem mitorganisiert vom DGB Bremen-Elbe-Weser. Die Veranstaltung wurde dankenswerterweise unterstützt von der Universität Bremen, der Hochschule Bremerhaven, dem AStA der Hochschule Bremen, dem Arbeitskreis Hochschulpolitik sowie vom Forum Friedenspsychologie.

Ich habe das Cyberpeace-Forum als Anregung zur Nachahmung relativ ausführlich beschrieben. Eine derartige Veranstaltung kann ein Publikum weit jenseits der an Informatik und Gesellschaft im engeren Sinne Interessierten erreichen und bietet die Chance zu Kooperationen mit Hochschuleinrichtungen, mit Gewerkschaften und mit Organisationen der Friedensbewegung. Im Falle des Cyberpeace-Teams Bremen wird die Kooperation auch fortgesetzt durch einzelne Veranstaltungen von April bis Juni 2017 mit dem Aufgreifen und Vertiefen der Vorträge von Norbert Schepers am 27. April und von Aaron Lye am 29. Juni sowie am 30. Mai mit einer Protestveranstaltung gegen die Konferenz und Messe *Undersea Defense Technology* in den Bremer Messehallen. Und im Herbst gibt es vielleicht das zweite Cyberpeace-Forum. Weitere Informationen lassen sich auf der Webseite *https://cyberpeace.fiff.de/Kampagne/CyberpeaceForum* finden. Insbesondere kann man dort auch Flyer und Plakat anschauen und das ziemlich beachtliche Medienecho nachvollziehen.

Von den fünf Vorträgen liegen drei in schriftlicher Fassung vor, die nachfolgend abgedruckt sind. Meinen eigenen Vortrag habe ich nicht verschriftlicht, weil ich auf der FIfFKon 2016 einen ganz ähnlichen Vortrag gehalten habe, der in der FIfF-Kommunikation 1/2017 nachzulesen ist.

Rolf Gössner

Cyberkrieg und Völkerrecht

Anlässlich der digitalen Aufrüstung der Bundeswehr im „Cyber- und Informationsraum"

Gegenwärtig wird die Bundeswehr mit einem neuen Kommando Cyber- und Informationsraum *aufgerüstet, das Anfang April 2017 in Dienst gestellt wurde – ergänzt von einem Forschungszentrum an der Bundeswehr-Universität in München.[1] Mit dieser digitalen Kampftruppe mit (geplant) fast 14.000 Dienstposten wird der „Cyber-Raum" zum potentiellen Kriegsgebiet erklärt, beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – bislang übrigens ohne Parlamentsbeteiligung, ohne demokratische Kontrolle und ohne gesetzliche Grundlagen.*

Diese Militarisierung des Internets und des gesamten Cyberraums dient nach Plänen des Bundesverteidigungsministeriums sowohl der Verteidigung gegen Cyberattacken von außen als auch eigener Cyberangriffe auf andere Staaten und deren IT-Systeme (laut *Geheimer Strategischer Leitlinie Cyber-Verteidigung* des Bundesverteidigungsministeriums von 2015).[2] Erstmals spielt im *Weißbuch zur Sicherheitspolitik 2016* der Krieg im Cyberraum eine gewichtige Rolle – inklusive Cyberkämpfer.innen.[3] Das bedeutet: Auch die Bundeswehr entwickelt Cyberwaffen, um in fremde IT-Systeme einbrechen und dort Manipulationen vornehmen oder diese zerstören zu können.

Schon jetzt existiert übrigens eine kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn (*Computer Netzwerk Operationen*) mit 70/80 Soldaten, die für operative Maßnahmen zuständig ist. Diese Einheit wird nun erweitert und zusammen mit den bereits existierenden IT-Einheiten der Bundeswehr, etwa dem *Kommando Strategische Aufklärung,* in der neuen Organisationseinheit verschmolzen und zentralisiert. Darüber hinaus werden in großen Werbekampagnen neue IT-Fachleute angeworben.[4]

I. „Deutschlands Freiheit wird auch im Cyberraum verteidigt" *(Bundeswehr-Werbung)*

Wir haben es bei dieser digitalen Aufrüstung mit einer operativen Befähigung der Bundeswehr zu tun. Im Klartext: mit der Befähigung auch zur verdeckten Cyberkriegsführung im In- und Ausland – auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen der Bundeswehr im Ausland. Nicht allein militärische Ziele lassen sich damit treffen, sondern – zumindest als „Kollateralschäden" – auch zivile Infrastrukturen. Dies kann zu lang andauernden Ausfällen etwa der Strom- und Wasserversor-

gung, des Gesundheits- oder Verkehrswesens führen und damit die davon betroffene Zivilbevölkerung enorm schädigen.

Spätestens hier stellen sich dringliche Fragen nach der völkerrechtlichen Beurteilung und Regelung dieser Materie: Ab wann ist Cybergewalt zwischen Staaten völkerrechtswidrig, wann ist sie konventionellen bewaffneten Angriffen gleichzusetzen, wie den Urhebern zuzurechnen; inwieweit grenzen Regeln des Völkerrechts dieses digitale Schlachtfeld ein, ist all das überhaupt mit völkerrechtlichen Kategorien zu fassen und zu kontrollieren, oder müssen neue Regeln her – eine Art digitale Konvention? Diese Fragen sollen hier zumindest kursorisch behandelt werden, wobei wir uns im Klaren sein müssen, dass dieser völkerrechtliche Diskurs erst vor wenigen Jahren begonnen hat und noch in vollem Gange ist.

II. Völkerrecht und Menschenrechte gelten auch im Cyberspace und Cyberkrieg

Bislang reguliert und kontrolliert kein international verbindliches Abkommen die Aufrüstung im Cyberspace und den „Krieg der Zukunft". Aber so viel ist klar: Völkerrecht und Menschenrechte gelten auch hier – also auch das völkerrechtliche Gewaltverbot und das Recht zur angemessenen militärischen Selbstverteidigung gegen kriegerische Cyberangriffe von außen.[5]

Artikel 2 der UN-Charta untersagt den Staaten die *Androhung oder Anwendung von Gewalt.* Das bedeutet prinzipiell: Kriegsverbot zwischen Staaten und damit auch Verbot von Cyberkriegen. Jede zwischenstaatliche militärische Cyberoperation, die als Androhung oder Anwendung von Gewalt oder als Akt von *Cyber-Waffengewalt* definiert werden kann, stellt einen Völkerrechtsverstoß dar.

Doch nicht jeder Cyberangriff ist schon Cyberkrieg. Die meisten Cyberangriffe finden in Friedenszeiten statt und können grundsätzlich nicht als Kriegshandlung bezeichnet werden, auch wenn sie in feindlicher Absicht durchgeführt werden. Das gilt für Akte der digitalen Informationsmanipulation, Cyberkriminalität, Cyberspionage, Computersabotage und des Cyberterrorismus. In solchen – nicht-militärischen – Fällen von organisierter oder schwerer Kriminalität ist ein militärischer Gegenschlag zur Selbstverteidigung keinesfalls gerechtfertigt. Die Bekämpfung solcher Operationen unterfällt der nationalen „Inneren Sicherheit" und Rechtsprechung, weil es sich bei den Angreifern zumeist um Zivilpersonen, Organisationen, Firmen oder nichtmilitärische staatliche Institutionen handelt. Zuständig zur Sicherung, gezielten Abwehr und Ahndung mit angemessenen, nichtmilitärischen Gegenmaßnahmen sind hier: Nationales Cyber-Abwehrzentrum, Bundesamt für Sicherheit in der Informationstechnik (BSI), Geheimdienste, Bundes- und Länderpolizeibehörden sowie Staatsanwaltschaften/Bundesanwaltschaft und Justiz – die Bundeswehr nur dann, wenn es um Angriffe auf ihre eigene Militär-IT geht. Doch das Bundesverteidigungsministerium erhebt auch zum Schutz anderer staatlicher, kommunaler oder ziviler Netze den Anspruch der kooperativen Zuständigkeit der Bundeswehr für die „gesamtstaatliche Abwehr von Cyber-Angriffen" im Cyber-Raum – eine verfassungsrechtlich zumindest fragwürdige Zuständigkeit.

Wann handelt es sich demgegenüber um „Cyberkrieg", also um „bewaffnete Angriffe" oder um „Cyber-Waffengewalt"? Unter kriegerischen Cyberangriffen versteht man *militärische* IT-Attacken eines Staates auf computergestützte Systeme, kritische Infrastruktur und Netzwerke eines anderen Staates bzw. Landes, um in dessen Systeme einzudringen, diese – über Sicherheitslücken, Trojaner, Viren etc. – auszuspähen, zu manipulieren, zu schädigen, lahmzulegen oder zu zerstören. Angreifer und Angegriffene sind idealtypisch staatliche Akteure, deren Beziehungen durch das Völkerrecht geregelt werden.

Bislang gibt es jedoch keine völkerrechtliche Legal-Definition, wann ein (staatlicher) Cyberangriff als kriegerische Angriffshandlung gilt. Nach (noch) vorherrschender Auffassung in der juristischen Literatur liegt ein solcher Angriff nur dann vor, wenn die zerstörerischen Auswirkungen einer militärischen Cyberattacke mit denen konventioneller Waffengewalt vergleichbar sind – wenn also eine solche Attacke etwa Züge entgleisen, Flugzeuge abstürzen, Kraftwerke explodieren lässt und Menschen verletzt werden oder umkommen. Auch erhebliche Beschädigungen und Zerstörungen können ausreichen. Ob auch rein ökonomische Schädigungen genügen, ist umstritten. Insgesamt besteht aber die Gefahr, dass es aufgrund von Fehlinterpretationen zu verhängnisvollen militärischen Selbstverteidigungsschlägen und damit zu einer gefährlichen und folgenschweren Eskalation kommen kann.

Das Kriegsvölkerrecht beziehungsweise das humanitäre Völkerrecht – also das Recht zum Krieg und das Recht im Krieg – gelten auch im Fall des Cyberkriegs. Das Völkerrecht soll Kriege von vornherein verhindern oder nur in absoluten Ausnahmefällen zulassen, und das Humanitäre Völkerrecht verbietet – zum Schutz der Zivilbevölkerung – exzessive und unverhältnismäßige Handlungen im Kriegsfall.

So ist gemäß Genfer Konventionen verboten und als Kriegsverbrechen einzustufen, wenn ein Staat Cyberattacken gezielt gegen zivile Infrastrukturen (Strom, Wasser, Gesundheit etc.) eines anderen Staates führt und dadurch die Grundversorgung der Zivilbevölkerung unterbrochen oder nachhaltig gestört wird. Das gilt nicht für gezielte Cyberattacken gegen „rein" militärische IT- und Kommunikationssysteme. Problematisch dabei sind allerdings die möglichen, ja wahrscheinlichen *Kollateralschäden*, die bei vernetzten sowie Dual-Use-Systemen insbesondere die Zivilbevölkerung schwer treffen können. Digitale Waffen sind in

einer vernetzten Welt jedenfalls keine Präzisionswaffen, und die Streuwirkung kann immens sein.

III. Staatlich-militärische Reaktionen auf Cyberkriegshandlungen

Im Falle eines Cyberangriffs gegen einen Staat, der einem konventionellen bewaffneten Angriff gleichgesetzt werden kann, ist der angegriffene Staat nach Artikel 51 UN-Charta berechtigt, sein Recht auf angemessene Selbstverteidigung und Gefahrenabwehr auszuüben. Der angegriffene Staat darf dann gegenüber einem klar identifizierten Angreifer(staat) Selbstverteidigungsmaßnahmen im Cyberspace oder aber in der realen Welt durchführen. Die USA nehmen jedenfalls für sich in Anspruch, auch mit konventioneller militärischer Gewalt, also mit Raketen, Bomben und Granaten auf solche Cyberattacken zu reagieren.

Die Gegenmaßnahmen müssen zwar zur Abwehr des erlittenen, aber noch andauernden – also gegenwärtigen – Angriffs erforderlich und angemessen sein (Verhältnismäßigkeitsgrundsatz). Da die Streuwirkung eines Gegenangriffs jedoch immens sein kann, ist die Verhältnismäßigkeit von vornherein fraglich.

Da bewaffnete Auslandseinsätze der Bundeswehr dem sogenannten Parlamentsvorbehalt unterliegen, müsste ein solcher offensiver Cyber-Selbstverteidigungseinsatz der Bundeswehr im oder gegen das Ausland vom Bundestag genehmigt werden, genauso wie sonstige Kampfeinsätze im Ausland. Ob der Bundestag jedoch in der Lage ist, seine demokratische Kontrollfunktion vollumfänglich auszuüben und die Mittel und Folgen solcher Digitaleinsätze abzuschätzen, ist mehr als fraglich.

Ab wann und wie jeweils auf Cyberkriegsoperationen konkret reagiert werden soll, wird von Seiten der NATO und der Bundeswehr geheim gehalten, um „unberechenbar" zu bleiben und das Gegenschlagsrisiko unkalkulierbar zu machen (Abschreckungseffekt). Auch der UN-Sicherheitsrat könnte die Gewaltanwendung im Cyberspace oder Sanktionen als Gegenmaßnahme beschließen und ihren Vollzug delegieren. Und die NATO könnte den Bündnisfall erklären, sobald ein Mitglied angegriffen wird.

IV. Völkerrechtsrelevante Probleme bei der Beurteilung von Cyber-Operationen

1. Risiko einer Fehlzuordnung: Bei Cyberattacken und im Cyberkrieg gibt es keine Armeen, die sich gegenüberstehen und keine Soldaten in Uniform – stattdessen kommen etwa Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz, also Software, die keine Uniform oder Staatsabzeichen trägt. Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben – um etwa unter falscher Flagge Konflikte zu schüren oder Kriegsgründe zu produzieren.

So ist einerseits nur schwer herauszufinden, ob es sich bei IT-Angriffen um zivil-kriminelle und wirtschaftliche oder um geheimdienstliche und militärische Operationen handelt. Andererseits hat der angegriffene Staat das Problem, die eigentlichen Urheber oder Angreifer zweifelsfrei zu identifizieren, um überhaupt rechtmäßig, angemessen und zielgenau durch die richtigen Institutionen reagieren bzw. sein Selbstverteidigungsrecht ausüben zu können. Hier besteht die Gefahr, dass es zu vorschnellen militärischen Selbstverteidigungsschlägen kommt – und damit zu einer gefährlichen und folgenschweren Eskalation. Die Beweisführung ist jedenfalls in aller Regel äußerst schwierig. Der Internationale Gerichtshof verlangt eine klare Beweislage, denn es gibt kein Recht auf Selbstverteidigung ins Blaue hinein oder aufgrund bloßer Indizien; ein Gegenschlag ohne klar identifizierbaren Aggressor ist völkerrechtswidrig.

2. Dual-Use-Problematik: Auch Cyber-Angriffe, die zielgenau nur auf militärische IT-Infrastrukturen gerichtet sind, können rasch zum Flächenbrand führen, wenn sie sich auf zivile Infrastrukturen ausbreiten, diese lahmlegen oder gar zerstören – etwa Energienetze, Kernkraftwerke, Wasserversorgung oder Krankenhäuser. Der Cyberraum kennt im Zeitalter digitaler Vernetzung und auch der gemischt zivil-militärischen Kooperation keine wirksamen Grenzen – weder nationale und geografische, noch physische oder technische. Dual-Use-IT-Objekte werden schon heute als legitime Ziele militärischer Angriffe gesehen – wobei ohnehin fast die gesamte Cyber-Infrastruktur dem Dual-Use dient, also sowohl zivil als auch militärisch genutzt wird, zumindest nutzbar ist.[6] Mit gravierenden Folgen für die Zivilgesellschaft.

V. Eskalationspotential durch Rechtsauslegung

Dieses technologische Eskalationspotential wird noch erhöht durch eine gefährliche Rechtsauslegung in einem NATO-Dokument, das völkerrechtliche Fragen des Cyberwars bislang am intensivsten behandelt: das *Tallinn Manual – ein Handbuch zur Anwendung des Völkerrechts auf die Cyberkriegsführung (von 2013)*. Zwanzig Rechtsexperten aus verschiedenen NATO-Staaten, auch Deutschland, haben diesen Leitfaden in Kooperation mit dem Internationalen Roten Kreuz und dem Cyber-Kommando der US-Armee erarbeitet. An den 95 Regeln sollen sich alle NATO-Staaten im Fall eines Cyberkriegs orientieren. Sie sind zwar rechtlich nicht bindend, aber richtungweisend.

Die Autoren stammen großteils aus dem Militär oder sind militärnahe Juristen – entsprechend militärfreundlich ist das Dokument auch ausgefallen. Und es offenbart eine *„sehr US-amerikanische Sicht auf das Völkerrecht"* (F. Delerue). So gelten danach selbst solche Operationen als Cyberwar-Angriffe, die bloße wirtschaftlich-finanzielle Schäden eines betroffenen Staates verursachen, wenn diese gewisse (katastrophische) Ausmaße annehmen, etwa ein Börsencrash. Dagegen wäre dann eine gewaltsame, auch konventionelle Selbstverteidigung rechtens, so der Leitfaden, was aber zu einer unkontrollierbaren Eskalation der Auseinandersetzungen führen könnte.

Das NATO-Tallinn-Manual sieht in Regel 15 zudem vor, dass ein Staat sein Recht auf Selbstverteidigung auch präventiv ausüben darf – also bevor überhaupt ein Angriff stattgefunden hat, dieser erst unmittelbar bevorsteht und nicht anders als durch Gewalt abwendbar scheint. Auch hier, wie bei konventionellen militärischen Erstschlägen, besteht hohe Missbrauchsgefahr und die Gefahr folgenreicher Eskalation.[7]

Laut Handbuch gelten zivile Hacker („Hacktivists“) als aktive Kriegsteilnehmer, wenn sie Cyber-Aktionen im Verlauf kriegerischer Konflikte ausführen; sie können daher angegriffen und getötet werden. Selbst das Suchen und Offenlegen von Schwachstellen in Computersystemen des Gegners gilt demnach als kriegerische Handlung. Auf diese Weise wird die Kampfzone praktisch auf Privatpersonen und deren Laptops ausgeweitet.

Auf Cyberangriffe mit konventioneller Waffengewalt antworten solle ein Staat jedoch nur dann, wenn die Attacken Menschenleben gekostet oder massive Schäden am Besitz eines Staates angerichtet hätten (Regel 22). Bei eigenen (Gegen-)Attacken soll besondere Rücksicht auf die Zivilbevölkerung genommen werden. Ebenso wie bei traditioneller Kriegsführung dürfen etwa Krankenhäuser und sonstige medizinische Einrichtungen im Falle eines Cyberkrieges nicht (gezielt) angegriffen werden.

Trotz solcher Einschränkungen: Mit der Eingriffsschwellen weit herabsenkenden Rechtsauslegung des NATO-Dokuments werden die Grenzen völkerrechtlich zulässiger Gewaltanwendung im Rahmen des Selbstverteidigungsrechts in problematischer Weise aufgeweicht. Was einflussreiche Völkerrechtler da an Regeln für die NATO zusammengestellt haben, ist geeignet, eine schwere Datenattacke blitzartig in einen echten Krieg mit Raketen, Bomben und Granaten eskalieren zu lassen.

VI. Gegen Aufrüstung und Militarisierung im Cyberbereich – für Ächtung des Cyberkriegs

Mit der Aufrüstung der Bundeswehr zum Cyberkrieg steigen Kriegsbereitschaft und Kriegsgefahr – und davor schützt auch die obligatorische Zustimmung des Bundestags im Einzelfall nur bedingt. Der militärische Einsatz von Cyberwaffen durch Staaten ist – auch wenn er „nur“ zur Selbstverteidigung erfolgt – eine Kriegshandlung mit enormem Eskalationspotential, die die internationale Sicherheit und die Zivilbevölkerung erheblich gefährdet. Das Cyber-Konzept der Bundesregierung für die Bundeswehr verwischt die Grenzen zwischen Krieg und Frieden, Angriff und Defensive, innerer und äußerer Sicherheit, zwischen staatlichen und nichtstaatlichen, militärischen und zivilen, kriminellen und politisch motivierten Angriffen und Zielen, Gegenmaßnahmen und Akteuren; es öffnet dem Missbrauch Tür und Tor und ist letztlich demokratisch kaum zu kontrollieren. Die Bestrebungen der NATO, die hohe Schwelle für einen bewaffneten Angriff herabzusenken sowie die restriktiven Kriterien des Selbstverteidigungsrechts weiter aufzuweichen, sind hochgefährlich. Denn all dies würde das völkerrechtliche Gewaltverbot untergraben und die internationalen Beziehungen gefährden.

Aus diesem Befund sind politische und rechtliche Konsequenzen zu ziehen:

1. Um eine unkontrollierbare Aufrüstungsspirale zu verhindern, müssen international verbindliche Konventionen und ein internationaler Verhaltenskodex geschaffen werden – eine Art Genfer Konvention für die Cyberwelt, mit dem Ziel, eine weitere Militarisierung des Cyberraums zu verhindern. Außerdem bedarf es eines effektiven Schutzes eigener IT-Infrastrukturen, und dazu gehört es, Schwachstellen zu identifizieren und Sicherheitslücken wirksam zu schließen.[8]

2. Auch militärische Cyberfähigkeiten sind auf rein defensive Maßnahmen – also auf Verteidigung – zu beschränken, um die Zivilbevölkerung effektiv zu schützen – flankiert von vertrauensbildenden Maßnahmen im Rahmen einer friedensorientierten Außenpolitik und Diplomatie (Stichwort: *Cyberpeace*). Dazu gehört auch ein striktes Verbot, Cyberattacken mit konventionellen Waffen zu beantworten.

3. Noch wichtiger wären darüber hinaus eine weltweite Rüstungskontrolle, Cyberabrüstung und die völkerrechtliche Ächtung von Cyberspionage und Cyberwaffen sowie

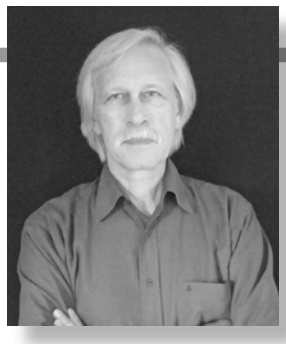
4. die Schaffung einer unabhängigen internationalen Instanz unter dem Dach der UN zur Untersuchung zwischenstaatlicher Cyberattacken und deren angemessener Abwehr.

Dieser Beitrag ist die überarbeitete Fassung eines Vortrags, den der Autor während des Cyberpeace-Forums am 12. Nov. 2016 im Bremer Haus der Wissenschaft gehalten hat.

Anmerkungen

1 Abschlussbericht Aufbaustab Cyber- und Informationsraum vom April 2016 sowie Dossier Cyber-Verteidigung, siehe Website des Bundesverteidigungsministeriums: https://www.bmvg.de

2 http://www.spiegel.de/politik/deutschland/bundesregierung-stellt-weissbuch-zur-sicherheitspolitik-vor-a-1102759.html ; https://netzpolitik.org/2016/weissbuch-zur-sicherheitspolitik-bundeswehr-geht-in-die-cyberoffensive/ ; https://netzpolitik.org/2015/geheime-cyber-



Rolf Gössner

Dr. **Rolf Gössner** ist Rechtsanwalt, Publizist und Vorstandsmitglied der *Internationalen Liga für Menschenrechte (www.ilmr.de)*. Seit 2007 stellv. Richter am Staatsgerichtshof der Freien Hansestadt Bremen. Sachverständiger in Gesetzgebungsverfahren des Bundestags und von Landtagen. Mitherausgeber des jährlich erscheinenden *Grundrechte-Report. Zur Lage der Bürger und Menschenrechte in Deutschland* (Fischer-TB). Mitglied in der Jury zur Verleihung des Negativpreises *BigBrotherAwards*. Autor und Herausgeber zahlreicher Bücher zum Thema *Innere Sicherheit und Bürgerrechte*, zuletzt: *Mutige Aufklärer im digitalen Zeitalter*, Ossietzky Verlag, Dähre 2015 sowie Gössner/Schuhler: *Terror. Wo er herrührt. Wozu er missbraucht wird. Wie er zu überwinden ist*, isw-spezial 29, München, Dez. 2016 *(www.isw-muenchen.de)*.

leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/

3 *https://www.heise.de/newsticker/meldung/Bundeswehr-Weissbuch-Planspiele-fuer-den-Krieg-im-Cyberraum-3270870.html m. w. N.*

4 *Die Bundeswehr sucht händeringend IT-Fachkräfte; auch an Hochschulen und Universitäten rekrutiert sie und entwickelt neue Karrierepfade. Plakataktion der Bundeswehr: „Deutschlands Freiheit wird auch im Cyberraum verteidigt", so lautet ein Slogan der Kampagne; vgl. Süddeutsche.de 2.4.2016.*

5 *http://www.spiegel.de/netzwelt/netzpolitik/ist-ein-cyberkrieg-ein-krieg-a-841096.html*

6 *Cordula Droege, Ist Cyberwar ein Krieg? In: Spiegel-online 2.7.2012.*

7 *Beispiel: der Computerwurm Stuxnet gegen das iranische Atomprogramm (2010) – gemäß Tallinn-Manual wäre dies als kriegerischer Akt zu werten, also als völkerrechtswidriger Angriffskrieg. Nicht aber, wenn dieser Angriff von den USA gestartet wird: Dann gilt der digitale Übergriff mit steuerndem Sabotage-Schadprogramm nur noch als „Akt der vorbeugenden Selbstverteidigung" gegen das iranische Atomprogramm, bevor damit Atomwaffen produziert werden können. (Die Urheberschaft von Stuxnet ist nicht eindeutig geklärt, es gibt aber starke Anhaltspunkte dafür, dass der Wurm eine Entwicklung des US-Geheimdienstes NSA in Zusammenarbeit mit Israel ist.) https://de.wikipedia.org/wiki/Stuxnet m. w. N.*

8 *Stattdessen werden aber IT-Sicherheitslücken, die für Cyberattacken nutzbar sind, als Angriffsoptionen offen und geheim gehalten, anstatt sie zum Schutz der eigenen Zivilbevölkerung aufzudecken und zu beseitigen. Auf diese Weise werden die Möglichkeiten zur Computerspionage und -kriminalität, zu Cyberterrorismus und -krieg gefördert.*

Thomas Gruber

Onlineoffensive: Die Bundeswehr im Cyber- und Informationsraum

Die Gefährdung der Zivilgesellschaft durch Attacken im Cyberraum war im vergangenen Jahr ein äußerst präsentes Thema in der deutschen Presse. Die Angriffsszenarien reichten dabei von einer wirtschaftlichen Bedrohung durch „Hackerangriff[e] auf […] deutsche Banken"[1] bis hin zu einer existenziellen Gefahr für das Individuum „durch Cyber-Angriffe […] [auf] Krankenhäuser oder die Energieversorgung"[2]. Oft sind die Herkunft und die Intention der Attacken unbekannt – militärische Einheiten bestimmter Staaten oder Staatenbündnisse könnten geopolitische Interessen verfolgen, nationale Geheimdienste könnten Spionage betreiben oder kriminelle Organisationen könnten privatwirtschaftliche Akteur.innen anvisieren. Diese Unsicherheit eignet sich allerdings gut für den Aufbau und die Festigung von Feindbildern; die Sprache wird dabei suggestiver: „Warnung vor russischen Cyberattacken: Angriffsziel Deutschland"[3] oder „Massiver Hacker-Angriff auf Thyssen-Krupp – waren es Chinesen?"[4]

Bundeswehrstrukturen für den Cyberkrieg

Dieses Klima der Verunsicherung und der Bedrohung nutzen auch die Bundesregierung und das Bundesministerium für Verteidigung (BMVg), um die Ausweitung von militärischen Befugnissen im Cyberraum und die dementsprechende Aufrüstung der Bundeswehr zu rechtfertigen. Am 1. April 2017 ist die Struktur der Bundeswehr in diesem Zug um einen eigenen Organisationsbereich zum Cyber- und Informationsraum (CIR) gewachsen.[5] Das Kommando des CIR ist in Bonn Hardthöhe, dem Hauptsitz des BMVg, angesiedelt und befehligt 13.500 vorhandene Dienstposten. Die Aufgabenbereiche bestehen neben der Administration, Organisation und Bereitstellung von IT-Struktur vor allem in den verschiedenen Aspekten der Kriegsführung im Cyber- und Informationsraum. So fallen unter den neuen Organisationsbereich beispielsweise die psychologische Kriegsführung („operative Kommunikation"), die Störung feindlicher und Sicherung eigener Kommunikationsnetze („elektronische Kampfführung"), die Vernetzung und technische Ausstattung der Kriegseinheiten („Führungsunterstützung") sowie Angriff und Verteidigung im Cyberraum („Cyber-Operationen"). Neben den bereits bestehenden Stellen werden außerdem 300 neue geschaffen, von denen 230 auf die Führung des Organisationsbereiches, 40 auf den Fachbereich *Cybersicherheit* und 20 auf die Verbesserung von Cyber-Operationen entfallen.

Um die Funktionalität des neuen Organisationsbereiches gewährleisten zu können, fehlt der Bundeswehr allerdings vor allem eines: qualifiziertes Personal. Denn während der Verteidigungshaushalt jährlich immer großzügiger ausfällt, muss nach Wegfall der Wehrpflicht erheblich nachgeholfen werden, um das deutsche Militär als attraktiven Arbeitgeber darzustellen. Die Bundeswehr steigt mit riesigen Werbekampagnen, Kompromissbereitschaft und mit starkem Fokus auf ihre Zielgruppen in den Wettbewerb auf dem Arbeitsmarkt ein. Im Falle des Cyber- und Informationsraumes sind diese Bemühungen beispielsweise am Projekt *Digitale Kräfte* erkennbar, das mit 3,6 Millionen Euro Finanzierung[6] einen großen Teil der 12,5 Millionen Euro schweren Werbekampagne *Mach, was wirklich zählt*[7] der Bundeswehr ausmacht. Mithilfe von großflächigen Plakataktionen, Netzwerk-Sessions, auf Karrieremessen und in Jobcentern sollen IT-affine Personen, Gamer.innen und *Nerds*[8] für eine