Jürgen Altmann und Dietrich Meyer-Ebrecht

Angriff und Verteidigung in der *Ära des Cyberkriegs*

Abendveranstaltung von W&F und BICC, 26. Januar 2018, Bonn

Die zunehmende Bedeutung des Cyberraums als *fünftem Kriegsschauplatz* war das Thema einer öffentlichen Diskussionsveranstaltung, die die Zeitschrift *Wissenschaft und Frieden* auf ihrer Jahrestagung in Zusammenarbeit mit dem Internationalen Konversionszentrum Bonn (BICC) am 26. Januar 2018 in Bonn ausrichtete. Der etwas sperrige Titel des Abends: *Ambivalenzen zwischen Angriff und Verteidigung in der ‚Ära des Cyberkriegs' – Theorie und Praxis der digitalen Strategie der Bundeswehr*. Der Anlass, dieses Thema zu wählen, war die Brisanz einer nun schon etwas zurückliegenden Nachricht, dass die Bundeswehr (Bw) eine eigenständige Einheit für Operationen im digitalen Raum, dem Cyber- und Informationsraum, in der Bundeswehrsprache kurz CIR, aufbaut. Auf dem Podium diskutierten Prof. Dr. Hans-Jörg Kreowski, Informatiker, Universität Bremen, Vorstandsmitglied des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Generalmajor Michael Vetter, Erster Stellvertretender Inspekteur und Chef des Stabes des Kommandos Cyber- und Informationsraum (CIR) in Bonn, und Prof. Dr. Matthew Smith, Informatiker, Universität Bonn und Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKI), Wachtberg. Die Podiums- und anschließende Plenumsdiskussion moderierte Prof. Dr. Hartwig Hummel, Universität Düsseldorf, Vorstandsmitglied des Arbeitskreises Friedens- und Konfliktforschung (AFK) und von W&F. Das Podium widmete sich verschiedenen Aspekten des militärischen Engagements im Cyber- und Informationsraum und seinen Auswirkungen.

Prof. Kreowski stellte zunächst einige Fakten zusammen. Der neue Organisationsbereich *Cyber- und Informationsraum* (CIR) der Bundeswehr befindet sich mit rund 13.500 Dienstposten seit 2016 im Aufbau, die offizielle Indienststellung war im April 2017. Überwiegend werden vorhandene Abteilungen unter einem Dach zusammengeführt, die neben Heer, Marine und Luftwaffe eine neue Teilstreitkraft bilden. Unterstützt wird dieser Prozess durch massive Nachwuchswerbung und mit der Einrichtung eines Master-Studiengangs IT-Sicherheit an der Bundeswehr-Universität München.

Neben defensiven Aufgaben wird die neue Teilstreitkraft auch offensive Aufgaben haben und sich am weltweiten Cyberkriegswettrüsten (bei dem es vorwiegend um eine Stärkung der offensiven Fähigkeiten geht) beteiligen. Kreowski stellt die Frage, wie sich das mit dem Verteidigungsauftrag der Bundeswehr verträgt. Ebenso sei fraglich, ob die Vermischung militärischer Cyberverteidigung mit ziviler Cyberabwehr verfassungsgemäß ist. Denn Cyberangriffe, die geheim gehaltene Sicherheitslücken und Schwachstellen nutzen, erfordern ganz andere Kompetenzen als eine Cyberverteidigung, bei der es darum geht, vor allem zum Schutz der Zivilgesellschaft Sicherheitslücken zu schließen und Schwachstellen zu beheben. Um im *Darknet* Know-how über Eingriffsmöglichkeiten, wie z. B. *Zero-Day-Exploits*, anzukaufen, erhielte die neue Teilstreitkraft ein dreistelliges Millionenbudget (was vom nachfolgenden Redner bestritten wurde). In kontraproduktiver Weise würde dieses Wissen der zivilen Datenverarbeitung vorenthalten.

Kreowski sieht im Aufbau eines Cyberwaffenarsenals eine erhöhte Kriegsgefahr, denn angreifen ist einfacher als verteidigen, die Mittel sind vergleichsweise billig (und wiederverwendbar!). So schwinden die Hemmschwellen, und die Eskalation durch konventionelle Vergeltungsschläge auf Cyberangriffe macht deren Folgen unkalkulierbar. Die vorhersehbare Ausweitung von Kriegen in den digitalen Raum, stellte Kreowski fest, ist völkerrechtswidrig, denn aufgrund der hohen Verletzlichkeit ziviler Infrastrukturen stellt sie in erster Linie eine Bedrohung der Zivilgesellschaft dar.

Dies alles sind Gründe, warum das FIfF mit seiner Kampagne *Cyberpeace statt Cyberwar* die Ächtung jeglicher Form von Cyberwaffen, zumindest jedoch der offensiven, fordert. Das Internet müsse entmilitarisiert werden und allein dem Frieden dienen, anstatt für Ausspähung und militärische Operationen missbraucht zu werden. Konsequent wäre es, eine *Digitale Genfer Konvention* zu schaffen, die Cyberangriffe auf lebenswichtige zivile Infrastrukturen verbietet. Weitere Forderungen der Kampagne sind ein Verbot des Einsatzes konventioneller Waffen als Antwort auf Cyberattacken, international transparente forensische Untersuchungen angeblicher Cyberkriegsangriffe, die Offenlegung und Beseitigung aller Schwachstellen (statt sie für eigene Angriffe zu nutzen) sowie die Sicherung kritischer Infrastrukturen (z. B. durch Entnetzung und Dezentralisierung).

Kreowskis provozierende Fragen stehen im Raum – sie bleiben auch unbeantwortet im Raum stehen, als Generalmajor Vetter das Podium übernimmt und die Perspektive der Bundeswehr einbringt. Vetter spricht über die Digitalisierung im Bereich der Streitkräfte, über die neuen Optionen und auch über die neuen Verwundbarkeiten. Er berichtet über den Aufbau der Cyberstreitkräfte als Segment der nationalen Cybersicherheitsstrategie 2016 der Bundesregierung. Federführend für letztere ist der Bundesminister für Inneres, während die Umsetzung schwerpunktmäßig in den Händen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundeskriminalamtes (BKA) und des Bundesamtes für Verfassungsschutz (BfV) liegt. Die Cyber-Verteidigung obliegt dagegen der Bundeswehr. Geht es um mandatierte Einsätze, ist Cyber-Außenpolitik gefordert. Entsprechend liegt die Verantwortung beim Auswärtigen Amt. Eine völlig neue Herausforderung sei die fehlende Symmetrie zwischen digitaler und materieller Welt. Denn mit vergleichsweise wenig (Software-) Aufwand kann ein immenser materieller Schaden verursacht werden. Abzusehen ist, dass es den „klassischen" Krieg nicht mehr geben wird. Ob ein Krieg als physikalischer beginnt oder als digitaler, in beiden Fällen wird die jeweils andere Komponente alsbald dazukommen und den Krieg zu einem hybriden machen.

Hierauf muss die Bundeswehr vorbereitet sein, betont Vetter. Sie hat jetzt alle diesbezüglichen Aktivitäten in einer Abteilung, dem Kommando CIR mit derzeit 13.500 SoldatInnen und zivilen Angestellten, gebündelt. Das Kommando soll auf knapp 15.000 Personen wachsen. Zuständig ist das Kommando für den Schutz

der bundeswehreigenen IT-Systeme sowie der Satelliten-, Richtfunk- und terrestrischen Kommunikations-Infrastrukturen. Dazu betreibt es ein *Cyber Security Operations Center*, ähnlich wie die Telekom; es stellt mobile Einsatzgruppen (CERT) und beschäftigt Cyber-Forensiker. Weiterhin ist das CIR zuständig für das militärische Nachrichtenwesen. Dazu gehören die Aufklärung über Aktivitäten der Streitkräfte anderer Staaten, eine Krisenfrüherkennung, die Bereitstellung von 3D-Geo-Information sowie von Wetter- und Klimadaten. Viele dieser Aufgaben sind die bisherigen, neu ist jedoch, dass alle diese Aktivitäten – auf Anforderung verschiedener ziviler Behörden – in den Rahmen einer gesamtstaatlichen Cybersicherheit eingeordnet sind.

So werden mit Tornados und über Satelliten, kommerziellen wie militärischen, schon seit Längerem Funknetze überwacht. Zuständig dafür war und ist die Truppe für Elektronische Kampfführung (EloKa), jetzt Teil des Kommandos CIR. Zu ihren Aufgaben gehören auch Maßnahmen des Informationskrieges, wie die Beeinflussung der Zivilbevölkerung durch aufbereitete Nachrichten, unterstützt mit Narrativen, die Gegenpositionen beispielsweise zu Taliban- und IS-Narrativen vermitteln. Neu hinzu kommen Fähigkeiten, in gegnerische Netze eindringen zu können, nicht nur zur Aufklärung, sondern auch, um für operative Maßnahmen manipulierend eingreifen zu können. Vetter nennt Beispiele wie die Verhinderung des Auslösens von Sprengfallen per Mobilfunk durch mitgeführte Störsender oder durch gezielte Lahmlegung lokaler Mobilfunknetze. Dies entspräche dem klassischen Kriegsziel, die Luftabwehr auszuschalten (so geschehen z. B. in Serbien), indem Führungs- und Gefechtssysteme gehackt werden.

Solche Angriffe, so betont Vetter (um wenigstens diesen Punkt des Vorredners aufzugreifen), würden streng regelbasiert erfolgen. Für offensive Cyber-Einsätze würden dieselben rechtlichen Voraussetzungen gelten wie für kinetische Angriffe. Für Cyber-Einsätze zur Unterstützung konventioneller Verteidigung und Angriffe (wie z. B. in Afghanistan) werde grundsätzlich ein Mandat des Bundestages vorausgesetzt. Das Grundgesetz sei die eherne Grundlage. Auch würden bei derartigen Einsätzen, wie z. B. dem Blockieren eines Funknetzes, immer Rechtsberater hinzugezogen. Wegen möglicher weitreichender Kollateralschäden würde die rechtliche Prüfung sogar rigoroser ausfallen als bei kinetischen Angriffen. Ein grundsätzliches Problem dabei sei, dass bei Cyberangriffen extrem schnell gehandelt werden muss. Zu diesem Zweck laufen aus allen beteiligten Organisationen – BSI, BKA, BfV und Bw – Informationen über Angriffe in einem 2011 gegründeten Nationalen Cyberabwehrzentrum zusammen. Angestrebt wird, einen gemeinsamen Gefechtsstand für alle diese Organisationen zu schaffen. Die Bundeswehr würde auch im zivilen Bereich tätig werden, zwar nicht initiativ, aber auf Anforderung, wenn beispielsweise Kraftwerke nach einem großflächigen Ausfall wieder ans Netz angeschaltet werden müssen und die zivilen Kräfte dafür nicht ausreichen würden.

Zum besseren Verständnis der Materie liefert Prof. Smith in groben Zügen die technischen Fakten nach, die offensiven Cyberoperationen zugrunde liegen. Ausschlaggebend ist, dass zivile und militärische Informationssysteme unterschiedslos dieselben Hardware- und Softwarekonzepte und teils sogar dieselben Programmsysteme nutzen. Insofern sei eine Grenzziehung zwischen zivilen und militärischen Fragestellungen kaum möglich. Der Weg, nichtautorisiert in fremde Computer und IT-Netze einzudringen, führt über das Ausnutzen von Schwachstellen. Entstehen können sie durch Fehler in Soft- oder Hardware, durch Fehlkonfiguration von Programmen oder unbedacht im Zusammenspiel von Programmbausteinen – unvermeidbar bei der Komplexität heutiger Hardware und Software und der Vielzahl der beteiligten Entwickler. Schwachstellen und geheime Hintertüren können sogar absichtlich eingebaut oder nachträglich eingeschleust werden.

Smith erläutert, was ein so genannter *Exploit* ist – ein Softwarewerkzeug zur Ausnutzung einer Schwachstelle – und insbesondere ein *Zero-Day-Exploit*. Das ist ein Exploit, der eingesetzt wird, bevor die Schwachstelle aufgedeckt wird und damit erst die Chance zur Entwicklung eines Sicherheits-Updates geboten wird. Der Angreifer kann sich in der Zwischenzeit bereits unentdeckbar eingenistet haben und seine Herrschaft über das System weiter ausbauen. An Exploits arbeiten außer professionellen Entwicklern in militärischer oder geheimdienstlicher Mission unzählige Hacker, die ihr Wissen und ihre Entwicklungen auf einem florierenden Schwarzmarkt anbieten. Dort kann ein Zero-Day-Exploit, zugeschnitten beispielsweise auf Apples iOS, gut und gerne eine Million Euro kosten, und Entwicklungen gegen militärische Systeme können sogar noch sehr viel teurer sein. Solche hochkomplexen Cyberwaffen werfen jedoch noch ein besonderes Problem auf: Sie sind wiederverwendbar, dürfen also keinesfalls Gegnern in die Hände fallen. Sie müssen deshalb einen Selbstzerstörungsmechanismus eingebaut haben (dieser hat bei der bekannt gewordenen Schadsoftware *Stuxnet* offensichtlich nicht funktioniert). Ein eminentes Problem ist die Attribuierung, d. h. die faktische Unmöglichkeit, schnell und zuverlässig den Urheber einer Cyberattacke zu ermitteln. Ein voreiliger Gegenschlag, ausgeführt möglicherweise sogar unter Einsatz konventioneller Waffen, könnte deshalb schnell zu einer Eskalation führen oder, wenn er den Falschen träfe, ungewollt einen neuen Konflikt auslösen. Smith betont zum Abschluss noch einmal, wie vor ihm schon Kreowski, dass militärische und geheimdienstliche Aktivitäten im Cyberraum die Sicherheit ziviler Systeme schwächen, die Gesellschaft gefährden, statt zu schützen, und damit kontraproduktiv im Sinne des Auftrages unserer Bundeswehr sind. Wir müssten auch damit rechnen, dass Cyberangriffe eher zivile Systeme zum Ziel haben könnten als militärische, da letztere vermutlich aufwändiger geschützt werden. Terroristen und Kriminelle würden diese „weiche Flanke“ ohne Skrupel nutzen, wo sich Militärs aus humanitären Gründen noch zurückhalten müssten. Selbst wenn jedoch das primäre Ziel eine militärische Einrichtung wäre, wird ihr Angriff unkalkulierbare Kollateralschäden verursachen, denen wieder vorwiegend zivile Einrichtungen zum Opfer fallen würden.

Die abschließende Diskussion ist engagiert, aber wenig ergiebig hinsichtlich der Klärung der offensichtlich kontroversen Positionen. Zu offensiven Cyberwaffen der Bundeswehr will sich Vetter erwartungsgemäß nicht äußern. Er verweist darauf, dass die empfindlichste Schwachstelle der Mensch sei und deshalb eine Cyber-Awareness entwickelt werden müsse. Dass die Probleme, die militärische Aktivitäten im Cyberraum für die Zivilgesellschaft bringen, damit gelöst werden können, bezweifelt Smith. Bezüglich des Entwurfs von Völkerrechtsregeln im Cyberraum wird das Tallinn-Manual erwähnt (das Richtlinien für den Krieg aufstellt, aber keine Rüstungsbegrenzung behandelt). Vertrauensbildende Maßnahmen seien nötig und z. T. schon in Arbeit. Kreowski weist auf die wichtige Rolle der Prävention mit-

tels Technikfolgenabschätzung hin – mehr Geld sei hierfür nötig, ebenso auch für eine Rüstungskontrollforschung. Ein grundlegendes Problem sei, so Smith, dass Informationstechnologie und informatische Methoden fast unvermeidlich Dual-use-Charakter haben und dass dies zur Bildung einer ausgedehnten Grauzone in Forschung und Industrie führt.

Zu optimistisch wäre die Erwartung gewesen, dass sich die Podiumsteilnehmer in der Diskussion näher gekommen wären. Deutlich wird vielmehr, wie groß die Kluft zwischen den Positionen von Militärs und Zivilgesellschaft ist und wie wichtig es ist, dass die Zivilgesellschaft Gegenmodelle entwickelt – wie Kreowski abschließend noch einmal unterstreicht – und sich für ihre politische Durchsetzung einsetzt.

Eine Audiodatei der Veranstaltung ist verfügbar unter *https://nc.bicc.de/index.php/s/W4JfTsjDnQ4nFiv.*

Der Beitrag erschien zunächst in Wissenschaft & Frieden 1/2018. Wir danken für die freundliche Genehmigung zum Wiederabdruck.

Wissenschaft & Frieden 1/2018 „USA – eine Inventur“

Ein Jahr nach dem Amtsantritt von US-Präsident Donald Trump konzentrierte sich die Berichterstattung stark auf seine Person, seine Kapriolen, seine Tweets und seinen Gesichtsausdruck. Selbst seine geistige Zurechnungsfähigkeit wurde angezweifelt. Diese Art der Wahrnehmung seiner Präsidentschaft ist unangemessen: Sie lenkt den Blick der Öffentlichkeit noch mehr auf seine Person und lenkt damit ab von Trumps Politik und den Fakten, die er damit schafft. Gleichzeitig unterstellt sie, mit seinem Amtsantritt habe sich in den USA alles geändert.

W&F 1/2018 zeigt Kontinuitäten der US-Politik auf, u. a. in der Innen-, Außen-, Militär- und Rüstungspolitik, aber auch die Folgen der Politik unter Trump: Mehr für Rüstung und weniger für Entwicklungshilfe und Vereinte Nationen, Abschottung gegen die Migration aus dem Süden, wachsender rechter Populismus und Rassismus im Inneren der USA.

Im Einzelnen schreiben:

- *Andrew Lichterman*: Der militärisch-industrielle Komplex
- *William D. Hartung*: Mehr als eine Billion Dollar. Das Budget der USA für Militär, Rüstung und Verteidigung
- *Otfried Nassauer*: „Tailored Deterrence“. Eine Nuklearpolitik für Donald Trump
- *Simon Schulze*: Ein Jahr Präsident Trump. Mehr Rüstung, weniger Vereinte Nationen
- *Christine Ahn* und *Tae Lim*: Korea, Nordostasien und Trump
- *Joachim Guilliard*: Washingtons Nahost-Politik
- *Jürgen Wagner*: Trump oder Brexit? Ursachen und Ausprägungen des EU-Rüstungsschubs
- *Bill Fletcher jr.*: „America First“ und der rechte Populismus
- *Olaf Miemiec*: Rechter Populismus. Die Mär von der „autoritären Internationale“
- *Meztli Yoalli Rodríguez Aguilera* und *Mirna Yazmín Estrella Vega*: US-Grenzregime und Rassismus. Migration aus und durch Mexiko
- *Svenja Boberg*, *Tim Schatto-Eckrodt* und *Lena Frischlich*: Fabricated News. Der Einfluss von Fake News auf die politische Einstellung

Außerhalb des Schwerpunktes geht es um

- das Völkerrecht versus Atomwaffen (*Bernd Hahnfeld*)
- Martin Luther King als Gegner des Vietnamkrieges (*Karlheinz Lipp*)
- den Weg der badischen Kirche zur Kirche des Gerechten Friedens (*Theodor Ziegler*) sowie
- Putins Wiederwahl und die Verantwortung des Westens (*August Pradetto*)

Unter dem Titel *Deutsche Waffen, deutsches Geld – morden mit in aller Welt*, beleuchtet die kommentierte Presseschau den Einsatz deutscher Panzer im Krieg der Türkei gegen die Kurden und Syrien.

Wissenschaft & Frieden, 1/2018: „USA – Eine Inventur“, 9,00 € Inland, EU plus 3,00 € Porto.

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bitte um Vorkasse: Sparkasse KölnBonn
DE86 3705 0198 0048 0007 72, SWIFT-BIC: COLSDE33XXX

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7, 35037 Marburg, E-Mail: *vertrieb@wissenschaft-und-frieden.de*, *www.wissenschaft-und-frieden.de*