Cyberwar und Inforaum

Die NATO und der Krieg auf dem fünften Schlachtfeld

von Thomas Gruber

„Der erste Schuss im nächsten großen Krieg wird im Web fallen". Rex Hughes, Sicherheitsberater der NATO im Bereich der Cyber-Verteidigung, weiß die zentrale Bedeutung der Cyber-Kriegsführung für die Mitglieder des Nordatlantikbündnisses in Szene zu setzen.[1] Neben klassischen militärischen Schauplätzen wie dem Krieg zu Land, in der Luft, im Meer und im Weltall wird der Cyberspace innerhalb der NATO längst als neues fünftes Schlachtfeld gehandelt. Der Begriff Cyberwar bezeichnet dabei kriegerische Aktionen im virtuellen Raum. Diese neuen Angriffstaktiken umfassen unter anderem Attacken auf feindliche Infrastruktur über das Internet, das Einschleusen fehlerhafter Hardware in Kommunikationsnetze und die gezielte Störung elektronischer Geräte durch Mikrowellen- oder elektromagnetische Strahlung.[2] Das Bedrohungsszenario, dem sich die NATO-Verbündeten bei der Thematisierung des Cyberkriegs bedienen, reicht von der bloßen industriellen oder diplomatischen Spionage bis zur vollständigen Sabotage kritischer ziviler und militärischer Infrastruktur. Die politischen und militärischen Entscheidungsträger_innen suggerieren, dass Cyberangriffe auf Krankenhäuser, Kraftwerke oder Kriegsgerät – vor allem jene, die über das Internet erfolgen – äußerst niedrigschwellig, „kostengünstig und effektiv"[3] und daher auch von Staaten mit begrenzten militärischen Mitteln oder Hacker_innenkollektiven durchführbar sind. Suleyman Anil, der Leiter des NATO-Zentrums zur Reaktion auf Computerzwischenfälle, konstatiert: „Cyberverteidigung wird nun in den höchsten Rängen zusammen mit der Raketenabwehr und der Energiesicherheit in einem Atemzug genannt".[4] Dass allerdings eine Struktur zur Cyberverteidigung auf NATO-Seite jemals ohne die gleichzeitige Planung von Cyberangriffen gedacht wird, ist höchst unwahrscheinlich – denn innerhalb der NATO dominiert folgende Auffassung zum „Wert" solcher Offensivkapazitäten: „[K]ann irgendeine militärische Macht glaubwürdig versichern, dass sie zukunftsweisende Fähigkeiten besitzt, wenn sich in ihrem Arsenal nicht auch offensive Cyberoperationen befinden?"[5]

Öffentliche Darstellung und Kooperationsstrukturen

Angriffe im Informationsraum werden auf Seite der NATO umfassend als Verteidigungsfall dargestellt. Ebenso defensiv orientiert berichtet auch die westliche Presse vornehmlich von Cyberangriffen auf NATO-Verbündete durch russische und chinesische Hacker_innen oder durch politische Aktivist_innen (wie das Kollektiv Anonymous). Die einzelnen Ziele der Angriffe auf die jeweilige Staats- und Wirtschaftsordnung sind dabei in klare Feindbilder abgegrenzt: Chinesische Angreifer_innen beschränken sich demnach auf die Wirtschaftsspionage,[6] russische Hacks dagegen auf die politische Vergeltung gegenüber einzelnen Staaten oder NATO-Strukturen[7] und aktivistische Hacker_innen zielen aus ideologischen Gründen auf die Offenlegung von empfindlichen Staatsgeheimnissen ab.[8] Gegen die erdrückende Flut von Cyberattacken kann sich die NATO also als Retterin – und zu gegebener Zeit gar als Rächerin – der westlichen Werte- und Wirtschaftsunion hervortun. Doch für schlagkräftige Wehrhaftigkeit werden Strukturen und Technologie benötigt, Personal muss ausgebildet, eingestellt und Stellen müssen verstetigt werden – kurz: Der Verteidigungsetat der einzelnen NATO-Staaten wird entsprechend erhöht und es entstehen nationale und transnationale Kompetenzzentren zum Cyberwar. Dabei zeichnet sich auf Seiten der Staatsregierungen und deren Bündnissen ein Ringen um die Kontrolle des virtuellen Raumes ab. Waren gezielte Großangriffe im Cyberspace vor 10 bis 15 Jahren noch den mächtigen und reichen Staaten oder Konzernen vorbehalten, bangen diese nun zunehmend um ihren exklusiven Status und befürchten gegenüber Kleinstgruppen gekonnter Hacker_innen Informations- und Raumverluste im Cyberkrieg hinnehmen zu müssen.

Auf nationaler Ebene befassen sich traditionell meist Geheimdienste mit der Abwehr und der Durchführung von Cyberattacken (so beispielsweise im Falle der USA die National Security Agency und in Deutschland der Bundesnachrichtendienst). Der „Vorteil", solch intransparent agierende Organisationen zu unterhalten, ist die Möglichkeit, selbst klandestine Spionage oder Sabotage-Angriffe durchführen zu können, ohne diese öffentlich thematisieren zu müssen. Nicht immer ist allerdings ein geheimer Schlagabtausch im Cyberspace politisch erwünscht: Es kann aus nationaler und geopolitischer Sicht durchaus sinnvoll sein, einen Cyberangriff als Kriegsakt zu stilisieren. Denn würde eine Cyberattacke als vollwertige kriegerische Aktion gegen einen NATO-Staat klassifiziert, so ließe sich daraufhin der in einer Politik der militärischen Eskalierung oft ersehnte Bündnisfall ausrufen. Auf dem NATO-Gipfel in Wales 2014 wurde konstatiert: „Ein Beschluss darüber, wann ein Cyber-Angriff zur Erklärung des Bündnisfalls nach Artikel 5 führen würde, wäre vom Nordatlantikrat fallweise zu fassen."[9] Mit ebendieser Prämisse arbeitet auch das 2008 in Estland gegründete Kompetenzzentrum für Cyberabwehr der NATO.[10] Nach eigener Auffassung soll es die „Fähigkeit [...] bieten, Bündnismitglieder auf Verlangen bei der Abwehr eines Cyberangriffs zu unterstützen".[11] Auch auf nationaler Ebene entstanden militärische Abteilungen zur Abwehr und zur Durchführung von Cyberangriffen. Die im Jahr 2008 gegründete *Abteilung Informations- und Computernetzwerkoperationen der Bundeswehr* soll neben einer Analyse des Bedrohungspotentials feindlicher Cyberattacken auch die Möglichkeiten offensiver digitaler Kriegsführung durch die Bundeswehr bearbeiten.[12] In Frankreich wurde im Jahr 2009 die regierungsamtliche Cybersicherheitsbehörde *ANSSI* ins Leben gerufen, die sich mit der Sicherheit französischer Informationssysteme befassen soll und dem Sekretariat zur nationalen Verteidigung und Sicherheit unterstellt ist.[13] Das US-amerikanische *United States Cyber Command* entstand im Jahr 2010 und setzt sich unter Führung *United States Strategic Command* mit den Möglichkeiten und Strategien des Cyberwars auseinander.[14]

Neben dem Aufbau eigener Strukturen und der Ausbildung militärischen Personals für Cyberaufgaben greift das NATO-Bündnis vor allem auf bereits bestehende Expertise aus der Privatwirtschaft zurück. Auf dem NATO-Gipfel 2014 in Wales wurde die Gründung einer *NATO Industry Cyber Partnership*

(NICP) beschlossen, die beim Aufbau einer engen Kooperation zwischen dem Nordatlantikbündnis und Unternehmen der Kommunikationsindustrie behilflich sein soll. Bereits knapp zwei Wochen später trafen sich NATO-Vertreter_innen mit Personen aus der Industrie, um die NICP offiziell einzugehen. Das Ziel der NATO innerhalb der NICP besteht in der Akquise von „Expertise" und „Innovation" aus dem privaten Sektor. Koen Gijsbers, Geschäftsleiter der *NATO Communications and Information Agency* (NCIA), fügt hinzu: „Hier geht es um ein Bündnis mit der Industrie und der Schlüssel zu diesem Bündnis ist Vertrauen – sensible Informationen miteinander auszutauschen, um auf Bedrohungen reagieren zu können".[15] Zum einen erhoffen sich die NATO-Funktionär_innen also technologische und innovative Unterstützung von den kollaborierenden Unternehmen, zum anderen sollen sensible Informationen (wie beispielsweise Kommunikationsdaten oder Schwachstellen in den eigenen Sicherheitssystemen) von den Konzernen an die militärischen Akteur_innen weitergegeben werden. Dass dabei erhebliche Summen an die beteiligten IT-Sicherheits- und Kommunikationsunternehmen fließen werden, ist selbstverständlich. Sie verkaufen an die NATO neben den neuesten Angriffs- und Verteidigungsschemata im Cyberwar auch private Daten ihrer Kunden, oder zumindest Wege, diese zu akquirieren.[16]

NATO-Aktionen im Cyberwar

Die Aktionen der NATO-Staaten im Cyberwar werden öffentlichkeitswirksam verkauft. Die Berichte umfassen militärische Übungen wie beispielsweise einen simulierten Großangriff auf Computernetzwerke im NATO-Kompetenzzentrum in Tallinn – bei dem Methoden zur Cyberverteidigung eine ebenso große Rolle spielten wie Angriffsschemata im Cyberspace[17] – oder die Einbettung von Cyberkonzepten in die Großübung Trident Juncture im Jahr 2015. Trident Juncture behandelte eine Intervention in einer Region in Afrika, in der zwei Kleinstaaten um den Zugang zu Trinkwasser streiten und die es nach NATO-Maßstäben militärisch zu stabilisieren gilt.[18] In diesem Sinne fanden während der Übung auch Cyberkonzepte ihre offensive Anwendung. Von minder technologisierten Kleinstaaten kann kaum ein Cyberangriff ausgehen, der für die NATO-Verbündeten gefährlich würde. Stattdessen muss sich ein solches Manöver auf Cyberattacken gegen zivile und militärische Infrastruktur, Überwachung, Spionage und die Möglichkeiten der Verbreitung von westlicher Kriegspropaganda – der sogenannten „strategischen Kommunikation" – fokussieren.[19] Offensive Taktiken im Cyberspace werden von NATO-Seite nach alter Manier in ein Verteidigungsszenario eingebettet und als legitime Abschreckungsmanöver gerechtfertigt: „Eine klare Artikulation der Art, wie die NATO offensive Cyberstrategien als Teil jeder defensiven Operation nutzen würde, würde auch die Risikoabschätzungen der Feinde dahingehend ändern, dass sie gezwungen wären zu bedenken, dass jede offensive Aktion, auch wenn sie verdeckt stattfinden sollte, nicht risiko- oder kostenfrei ist."[20]

Eine weitere Möglichkeit, die öffentliche Meinung zu manipulieren, ist die Kopplung geheimdienstlicher Cyberangriffe und offen kommunizierter Cyberabwehr. Denn die westlichen Großmächte können die Herkunft ihrer geheimdienstlichen Cyberattacken weitaus besser verschleiern als Staaten wie der Iran oder China. So wurden beispielsweise im Jahr 2010 mittels des Internetwurms Stuxnet, der vermutlich aus den USA stammt, iranische Atomanlagen angegriffen[21] und die anschließenden Vergeltungsschläge iranischer Hacker_innen in den westlichen Medien als Angriff dargestellt und verurteilt.[22] Da die US-Behörden und -Geheimdienste allerdings nicht offenlegen, auf welcher Grundlage sie die Ursprünge der neuen Cyberangriffe im Iran verorten, ist auch nicht auszuschließen, dass die iranischen Hacks von den USA selbst fingiert wurden. Denn falls auf die US-amerikanischen Cyberangriffe keine militärische oder geheimdienstliche Reaktion aus dem Iran folgt, wäre auch die fälschliche Darstellung eines feindlichen Cyberangriffes denkbar, um den Konflikt zu eskalieren. Während die Sabotage bei Cyberangriffen meist gegen politische Feinde außerhalb des NATO-Bündnisses beschränkt ist, greifen Spionagebemühungen auch unter den NATO-Staaten um sich. Eines der jüngsten Beispiele ist die NSA-Abhöraffäre, die aufgrund der von Edward Snowden geleakten Dokumente im Jahr 2013 an die Öffentlichkeit gelangte: Unter dem Deckmantel der Terrorbekämpfung wurden von den USA global und verdachtsunabhängig Kommunikationswege überwacht, private Kommunikation offengelegt und auch staatliche Institutionen von NATO-Verbündeten sowie Vertretungen der Vereinten Nationen ausspioniert.[23]

Logo des Kompetenzzentrums. Quelle: Wikipedia

Die Auswirkungen des Cyberwar auf die Zivilbevölkerung

Das Bedrohungsszenario, das von der NATO stetig aufrechterhalten wird, birgt neben der Möglichkeit einer Eskalation internationaler Konflikte aber auch eine erhebliche Gefahr für die Zivilgesellschaft. Ziele wie Krankenhäuser oder die Stromversorgung eines Landes stehen sowohl auf der Liste der bei einem Cyberangriff gefährdeten Objekte, als auch auf der Agenda bei Angriffen von Seiten der NATO-Staaten, wie die vermutliche US-amerikanische Attacke auf das iranische Atomprogramm eindrucksvoll zeigt. Die immer weiter reichende Digitalisierung und Technologisierung von Städten bis hin zur Planung sogenannter *Smart Cities* öffnet den neuartigen Cyberattacken sukzessive eine breitere Flanke. Die Absichten, den öffentlichen Nahverkehr zu automatisieren, intelligente Produktionslinien bereitzustellen und die Stromversorgung

Verlegungsschiff für Transatlantikkabel „Nessie II“. Quelle: Friflash/Wikipedia

über Netze von Kleinkraftwerken (teil)autonom zu steuern, sind nur einzelne Beispiele angreifbarer Infrastruktur, deren Abschaltung in Zukunft ganze Landstriche zum Stillstand zwingen würde und in ein handfestes Chaos stürzen könnte.[24] Die Wahl des Schlachtfeldes ist von ebenso großer gesamtgesellschaftlicher Bedeutung: Bei den meisten Cyberangriffen wird ein vorwiegend zivil verwendeter Kommunikationsweg genutzt – das Internet. Knotenpunkte der Datenübertragung sind vermehrt Ziel von Sabotage- und Spionageaktionen. *TAT-14*, eines der weltweit wichtigsten Transatlantikkabel, wurde in Ägypten mehrmals durchtrennt und in der englischen Küstenstadt Bude vermutlich vom britischen Geheimdienst *GCHQ* angezapft.[25] Auch russischen U-Booten wird von NATO-Seite inzwischen die Fähigkeit attestiert, Transatlantikkabel durchtrennen zu können.[26] Eine weit verbreitete Praxis bei Cyberattacken ist außerdem die Infizierung zahlreicher Computer mit Viren, die anschließend unbemerkt Befehle auf den Privatrechnern ausführen und sie so zu einem kollektiven Netzwerk, einem sogenannten *Botnetz*, machen. Auf diese Weise können beispielsweise Internetseiten und Server von Firmen oder staatlichen Institutionen überlastet werden, indem mehrere tausend Rechner gleichzeitig auf die Webpräsenz zugreifen.[27] Öffentliche Kommunikationswege werden also zu Kriegsschauplätzen, private Technologie zu Waffensystemen und die Zivilgesellschaft steht schließlich im digitalen Kreuzfeuer. Nach Konstanze Kurz wird „die Zivilbevölkerung […] als Geisel genommen und ihre zivile Infrastruktur Schlachtfeld und unreguliertes Operationsgebiet.”[28] Zum einen schürt diese Kriegstaktik das Klima der Angst in der Bevölkerung und erleichtert damit die Legitimation neuer militärischer Aktionen unter dem Deckmantel der nationalen Verteidigung, zum anderen bietet der zivile Sektor eine angenehme moralische Pufferzone bei feindlichen Angriffen.

Im selbsternannten Kampf gegen den Terror wird die Gefahr von in der Mitte der Gesellschaft verdeckt agierenden Terrorzellen instrumentalisiert, um staatliche Überwachungsmechanismen auszuweiten und damit die Privatsphäre der Bürger_innen einzuschränken. Neben der stetigen geheimdienstlichen Überwachung soll nun auch dem Militär ein breiterer Zugriff auf die zivile Kommunikation gewährt werden. Dabei kommen sowohl propagandistische Methoden gegen vermeintliche terroristische Werbung zum Einsatz, als auch komplexe Algorithmen zur automatisierten Analyse staatsgefährdender ziviler Kommunikation. Dass bei einer solchen verdachtsunabhängigen Überwachung auch subversive politische Gruppen in das Raster der Streitkräfte passen, ist kein Novum. Dieser Rhetorik bedienen sich beispielsweise auch die Entscheidungsträger_innen des für Anfang 2017 geplanten *Cyber- und Informationsraum-Kommandos* (CIRK) der Bundeswehr. Rekrutierungsbemühungen terroristischer Gruppierungen wie des IS über die sozialen Netzwerke werden als Angriff auf den Informationsraum gewertet und sollen ebenso aktiv überwacht und offen gelegt werden wie gezielte Cyberangriffe auf deutsche staatliche Institutionen und Unternehmen.[29] Neben der Löschung unliebsamer Inhalte wird der Bundeswehr damit auch die propagandistische Beeinflussung öffentlicher Diskussionen erleichtert, das CIRK kann also auch als Knotenpunkt strategischer Kommunikation fungieren. Dass der Bundeswehr mit der Begründung präventiver Terrorbekämpfung empfindliche Eingriffe in die private Kommunikation von Nutzer_innen sozialer Netzwerke und damit die Privatsphäre deutscher Staatsbürger_innen ermöglicht werden, tut der Planung bisher keinen Abbruch. Die deutsche Beteiligung an der digitalen Aufrüstung der NATO-Streitkräfte ist nicht zu unterschätzen: Neben den überaus präsenten US-amerikanischen Spionagebehörden, wie beispielsweise der NSA oder der US Airforce, kann kaum ein NATO-Staat so umfassende Wachstumsbestrebungen im Cyberkrieg vorweisen wie die Bundesrepublik. Begründet mit der veralteten Technologie der Bundeswehr und dem unmissverständlichen Wunsch der Politik, die deutsche Position in weltweiten Konflikten zu stärken, werden so militärische Umstrukturierungen und damit einhergehende Budgeterhöhungen im Cybersektor durch den parlamentarischen Entscheidungsprozess gewinkt.

Der NATO den virtuellen Raum nehmen!

Das Vorgehen des Nordatlantikbündnisses im Cyberkrieg zeigt vielfältige Parallelen zur übrigen NATO-Kriegsführung auf: Während NATO-Staaten selbst Angriffe planen und durchführen, werden öffentlich nur Verteidigungsszenarien beworben. Außerdem wird die augenscheinliche Einigkeit in Verteidigungsfragen innerhalb der NATO auch von den nationalistischen Aktionen der Einzelstaaten überlagert, die sich gegenseitig misstrauen und ausspionieren. Privatwirtschaftliche Akteur_innen wie IT-Sicherheitsunternehmen, die ursprünglich für die Sicherheit der ihnen anvertrauten Daten sorgen sollten, lassen sich von der NATO kaufen und kompromittieren dabei ihre eigenen Produkte. Allein dieser Umstand zeigt, dass IT-Sicherheit nicht in einem marktwirtschaftlichen Kontext funktionieren kann; die einzige sinnvolle Alternative bleibt quelloffene, kollektiv entwickelte Software, die unabhängig von Markt- und Machtinteressen entsteht. Die wahre Bedrohung für die Zivilgesellschaft, die von der NATO wie von jeder imperialistisch handelnden Militärinstitution ausgeht, fällt gegenüber der ständig präsenten Angst vor feindlichen Cyberattacken kaum ins Gewicht. Doch gerade aus

Smart City. Quelle: pixabay.com

den Angriffen auf die Privatsphäre und der Einbeziehung ziviler Infrastruktur in kriegerische Aktionen gälte es Motivation für vielfältige Formen des Widerstandes und des Protests zu schöpfen. Dass selbst kleine Kollektive von Hacker_innen eine nennenswerte antimilitaristische und antikapitalistische Rolle im digitalen Wettrüsten einnehmen können, wird schon allein durch die offensiven Anfeindungen deutlich, mit denen die NATO aktivistisch motivierte Hacker_innen zu legitimen Zielen im Cyberwar erklärt: „Sogenannte ‚Hacktivists', die sich an Cyberattacken während eines Krieges beteiligen, können legitime militärische Ziele darstellen, obwohl sie Zivilist_innen sind."[30] Hier zeigt sich auch der eigentliche Grund für das von der NATO beschworene Bedrohungsszenario im Cyberraum: Die Sabotage von Kommunikationsnetzen der NATO-Staaten oder die Offenlegung von Staats- und Unternehmensgeheimnissen bedarf im virtuellen Raum keiner schwer beizukommenden Waffentechnologie oder persönlicher Spionage mehr. Gruppen von Hacker_innen, die sich dezidiert friedvoll und jenseits jedweder Großmachtinteressen positionieren, können so der Eroberung des virtuellen Raumes durch macht- und wirtschaftspolitische Interessenträger_innen entgegenstehen. Die wahre Gefahr für eine Zivilgesellschaft geht dagegen nicht von politischen Kleingruppen aus, sie entsteht im internationalen virtuellen Wettrüsten, an dem sich die NATO-Staaten beispiellos beteiligen. Eine Cyberattacke auf wirklich kritische zivile Infrastruktur wie Krankenhäuser oder die Energieversorgung eines Landes benötigt Mittel, die nur den militärischen Großmächten zur Verfügung stehen. Denn im Gegensatz zu großen Teilen der NATO-Kommunikation und der Kommunikation großer Unternehmen oder staatlicher Behörden, sind die Gesundheits- und Energieversorgung meist nicht im Internet vernetzt und muss gezielt über das Einschleusen kompromittierter Hardware oder eigens zu diesem Zweck implementierten Computerviren attackiert werden. In ihren Bemühungen um den Schutz der eigenen militärischen Kommunikationsnetze und den einzelnen nationalen oder wirtschaftlichen Interessen erzeugen die NATO-Staaten also die Gefahr für ihre jeweilige Bevölkerung selbst. Dieser gefährlichen Scheinheiligkeit gilt es gesamtgesellschaftlich entgegen zu wirken und die Argumentation der rüstenden Großmächte muss systematisch dekonstruiert werden.

Anmerkungen

1 *Cyberwar: Nato-Staaten rüsten für das fünfte Schlachtfeld*, Spiegel online, 20.04.2016.
2 *Cyberkrieg*, Wikipedia, 20.04.2016.
3 Katrin Suder, Staatssekretärin des BMVg in: BMVg, 20.04.2016.
4 *Das Cooperative Cyber Defence Centre of Excellence der NATO*, Wikipedia, 20.04.2016.
5 Übersetzung des Autors aus dem Englischen; *The Role of Offensive Cyber Operations in NATO's Collective Defence*, NATO CCDCOE, S. 2, 05.05.2016.
6 *Is China still hacking US? This cyber firm says yes*, CNBC, 20.04.2016.
7 *Russische Hacker spionieren angeblich NATO aus*, heise.de, 20.04.2016.
8 *NATO report threatens to 'persecute' Anonymous Hacktivist grouped named as threat by military alliance*, serpent's embrace, 20.04.2016.
9 *Cyber-Kommando für die Bundeswehr*, NDR.de, 05.05.2016
10 *Krieg in der fünften Dimension*, Neue Züricher Zeitung, 20.04.2016.
11 *Das Cooperative Cyber Defence Centre of Excellence der NATO*, Wikipedia, 20.04.2016.
12 *Die Abteilung Informations- und Computernetzwerkoperationen, Cyber-Einheit der Bundeswehr*, Wikipedia, 20.04.2016.
13 *ANSSI, die erste regierungsamtliche Cybersicherheitsbehörde in Frankreich*, Wikipedia, 20.04.2016.
14 *United States Cyber Command*, Wikipedia, 20.04.2016.
15 Übersetzung des Autors aus dem Englischen; *NATO launches Industry Cyber Partnership*, NATO, 21.04.2016.
16 Besonders eindrucksvoll lässt sich diese Entwicklung am Beispiel des IT-Sicherheitskonzerns *RSA* nachvollziehen, der sich eine vorsätzlich implementierte Sicherheitslücke im eigenen Verschlüsselungssystem vom US-Geheimdienst *NSA* mit 10 Millionen Dollar bezahlen ließ: *Exclusive: Secret contract tied NSA and security industry pioneer*, Reuters, 21.04.2016.
17 *Verteidigungsministerin von der Leyen: Angriff der Cyber-Krieger*, Spiegel online, 20.04.2016.
18 *„Trident Juncture 2015": Machtdemonstration gegenüber Russland?*, IMI, 20.04.2016.
19 *Trident Juncture 2015 kicked off*, NATO, 20.04.2016.
20 Übersetzung des Autors aus dem Englischen; *The Role of Offensive Cyber Operations in NATO's Collective Defence*, NATO CCDCOE, S. 7, 05.05.2016.
21 *Obama ordnete Stuxnet-Attacken an*, taz.de, 20.04.2016.
22 *DDoS gegen Banken: USA klagen iranische Hacker an*, heise newsticker, 20.04.2016.
23 *Globale Überwachungs- und Spionageaffäre*, Wikipedia, 20.04.2016.
24 vgl. dazu beispielsweise Florian Rötzer: *Smart Cities im Cyberwar*, Westend Verlag, 2015.
25 *Die Kabel-Krake, die alles weiß*, Zeit online, 20.04.2016.
26 *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, New York Times, 20.04.2016.
27 *DDoS und Botnetze*, Wikipedia, 20.04.2016.
28 *High-Tech-Kriege*, Heinrich Böll Stiftung, S.21, 20.04.2016.
29 Katrin Suder in *Streitkräfte und Strategien*, NDR Info, 17.10.2015.
30 Übersetzung des Autors aus dem Englischen; *Tallinn Manual: NATO veröffentlicht Handbuch mit Cyberwar-Regeln*, netzpolitik.org, 05.05.2016.