Strategien im Cyberkrieg

Verschiedene Perspektiven auf das fünfte Schlachtfeld

von Thomas Gruber

Viel hat sich in den letzten zwei Jahren im Diskurs über den virtuellen Raum (auf Englisch auch Cyberspace) getan. Kaum eine Tageszeitung, kaum ein Politblog, die nicht irgendwo das Thema „Cyber“ behandeln würden – oft in so Unheil verkündenden Kombinationen wie „Cyberkrieg“, „Cyberangriff“ oder gar „Cyberterrorismus“. Kein Mensch kann sich angeblich mehr vor der unsichtbaren virtuellen Bedrohung sicher fühlen, dringen Hacker_innen doch inzwischen schon in die am besten abgeschotteten Netzwerke wie die von Banken und Geheimdiensten ein. Mit zwei aktuellen Beispielen wird in der Presse derzeit die allgegenwärtige Gefahr eines existenzbedrohenden Hacks begründet: Seit Anfang des Jahres wird von vermehrten Angriffen auf Banken berichtet. Nachdem die Zentralbank Bangladeschs im Februar um 81 Millionen US-Dollar erleichtert wurde, soll hinter den Attacken nun System stecken und es müssen weitere Angriffe auf Banken befürchtet werden.[1] Außerdem wurde im August bekannt, dass der US-Geheimdienst NSA[2] erfolgreich gehackt wurde. Zu allem Überfluss war das Opfer die „Equation Group“, ein Zusammenschluss äußerst versierter Hacker_innen, die vermutlich an der Entwicklung der mächtigsten invasiven Programme der NSA beteiligt sind.[3]

Die politische Antwort auf die neue Gefahr aus dem Cyberspace ist überwiegend militärisch und geheimdienstlich-polizeilich geprägt. Dies lässt sich vor allem an der Hochrüstung westlicher Akteur_innen im virtuellen Raum erahnen: Die NATO betont Gipfeltreffen um Gipfeltreffen die zentrale Bedeutung einer schlagkräftigen Cybertruppe und betreibt eigens dafür ein NATO-Kompetenzzentrum zur Cyberabwehr (*CCDOE*);[4] nationale (in Deutschland vorwiegend Landespolizeien) und supranationale polizeiliche Institutionen erhalten erhebliche Mittel und Machtbefugnisse im Kampf gegen die Cyberkriminalität;[5] und die Bundeswehr schafft mit dem *Kommando Cyber- und Informationsraum* einen eigenen Organisationsbereich für die deutsche Beteiligung am Cyberkrieg.[6]

Die Analyse von Aktionen im Cyberspace ist derzeit also äußerst populär – sei es in der Presse, der Politik oder aus einer militärischen Perspektive. Und obwohl sich professionelle Cyberattacken meist gegen Konzerne oder staatliche Institutionen richten, wird in der öffentlichen Diskussion ebenso häufig von einer Gefahr für Privatpersonen und die Zivilgesellschaft gesprochen. Grund genug, einen genaueren Blick auf die Akteur_innen zu werfen, die sich im virtuellen Raum bewegen und wie der Cyberspace aus verschiedenen Ansichten thematisiert wird.

Cyberwar in Militär und Politik

Wo sich, wie im virtuellen Raum, Angriff und Verteidigung, Täter_innen und Opfer definieren lassen, ist die militärische Elite nicht weit, um ein neues, sie selbst legitimierendes Schlachtfeld zu generieren. Für das Militär ist es dabei wünschenswert, wenn die kriegerischen Aktionen im Zusammenspiel mit wirtschaftlichen und polizeilichen Interessen einzelner Nationalstaaten laufen, weil so der Rechtfertigungszwang auf die Staatsregierungen übergeht. Im Cyberwar ist diese Agenda äußerst erfolgreich: Cyberangriffe auf westliche Unternehmen werden zu einer Bedrohung der nationalen Sicherheit, „Cybercrime” wird zu „Cyberterrorismus“ und der_die Feind_in kann angeblich in jedem dunklen Winkel des Internets lauern, das es aufgrund dieser akuten Notlage umfassend zu überwachen gelte.

Diese Entwicklung zeichnet sich auch in den großen militärischen Strategien ab, die im Laufe des Jahres von der NATO, der EU und dem deutschen Verteidigungsministeriums entwickelt wurden. Die Ergebnisse des NATO-Gipfels in Warschau, die Formulierungen zur EU-Globalstrategie, das Weißbuch der Bundeswehr, sie alle schlagen in Sachen Cyberstrategie in dieselbe Kerbe: Der Cyberwar ist eine reale Bedrohung der Gegenwart und die militärischen Strukturen der westlichen Großmächte sind für diese Art von Kriegsführung nicht ausreichend gerüstet. Cyberattacken sind eine Gefahr für mittelständische Unternehmen sowie für Großkonzerne, für ganze Wirtschaftssysteme, ja sogar die staatliche Ordnung und damit auch die Zivilgesellschaft. Der virtuelle Raum ist das Schlachtfeld der Zukunft. Um die Wehrhaftigkeit der westlichen Großmächte gegen gut verborgene Kleingruppen von Hacker_innen zu gewährleisten, müssen neue Geschäftsfelder und Abteilungen für die militärischen und polizeilichen Institutionen der Bundesrepublik, der EU und der NATO geschaffen werden, die einen regen Austausch pflegen.

Für eine schlagkräftige Cybertruppe wird außerdem das modernste Equipment benötigt. Schon im Prozess der strategischen Ausarbeitung werden auf BRD-, EU- und NATO-Ebene die Weichen für sogenannte *Private-Public-Partnerships* (PPPs) in Sachen Cybersicherheit gelegt (siehe folgender Abschnitt). So sollen westliche IT-Sicherheitskonzerne die unterversorgten militärischen Einrichtungen für satte Gewinne mit der modernsten Spionage- und Cyberabwehrtechnologie bestücken.

Bedeutung für die Wirtschaft

Die Privatwirtschaft nimmt in der politischen Diskussion über den Cyberwar eine besondere Rolle ein. Sie ist – wie beispielsweise Banken und produzierendes Gewerbe – sowohl Opfer von Cyberattacken, als auch – im Falle der IT-Sicherheitsindustrie – Profiteurin des Cyberkriegs. Die größten Unterschiede der deutschen, der EU- und der NATO-Strategie im Cyberwar werden gerade in der Rolle, die privatwirtschaftliche Akteur_innen dort einnehmen, deutlich. Auf dem NATO-Gipfel im Juli 2016 werden Cyberattacken noch ausschließlich im Kontext von kriegerischen Handlungen betrachtet: „Wir […] erkennen den virtuellen Raum als ein Operationsgebiet an, in dem sich die NATO genauso effektiv verteidigen muss, wie sie es bereits in der Luft, an Land und zur See tut.“[7] Im Weißbuch der Bundeswehr werden Cyberattacken auf deutsche Unternehmen und staatliche Strukturen mit einer Gefahr für die Zivilgesellschaft in einem Atemzug genannt: „Die wachsende und sämtliche Lebensbereiche durchdringende Digitalisierung […] macht Staat, Gesellschaft und Wirtschaft […] besonders verwundbar für Cyberangriffe und erfordert unmittelbare Gefahrenabwehr”.[8] Und die EU-Globalstrategie bittet eher in einem

Quelle: Korpus der Zeitung „Die Zeit". Erstellt mithilfe des Digitalen Wörterbuchs der Deutschen Sprache (DWDS).

Appell um breite Zusammenarbeit: „Kooperation und Informationsaustausch zwischen den Mitgliedstaaten, den Institutionen, dem privaten Sektor und der Zivilgesellschaft können eine gemeinsame Kultur der Cybersicherheit fördern und zur besseren Verteidigungsbereitschaft gegen mögliche Störungen und Attacken im Cyberraum beitragen."[9]

In den Fragen, woher die nötige Technologie für die zu gewährleistende Cybersicherheit denn nun genommen werden soll und ob für den Schutz von Banken und Konzernen vor Cyberattacken auch Steuergelder verwendet werden sollen, sind sich alle drei Papiere dann jedoch wieder sehr ähnlich: Mit Geldern des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI), der EU-Kommission und der NATO wurden jeweils Zusammenschlüsse aus Unternehmen der IT-Sicherheitsbranche und Behörden gebildet, die die Grundlage für Großprojekte im Rahmen von PPPs darstellen sollen. Auf Bundesebene sorgt die *Allianz für Cybersicherheit* für die nötige Nähe zwischen staatlichen Institutionen und privaten Unternehmen: „Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland" soll die Allianz „die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen […] stärken". Inzwischen gehören dem Verbund fast 2000 Institutionen an – eine bunte Mischung aus Behörden, Sicherheitsunternehmen, sogenannte „Betreiber kritischer Infrastruktur" und „Institutionen im besonderen staatlichen Interesse".[10] Die EU-Kommission bringt die verschiedenen Akteur_innen über die *öffentlich-private Partnerschaft zur Cybersicherheit* zusammen: Das von der EU-Kommission gestartete Projekt soll die größten europäischen IT-Sicherheitskonzerne mit „regionalen [und] nationalen Behörden" verkuppeln, um „Europa besser gegen Cyberattacken auszurüsten und die Wettbewerbsfähigkeit des europäischen Cybersicherheits-Sektors zu verbessern". Die Partnerschaft soll bis zum Jahr 2020 „Investitionen von 1,8 Milliarden Euro anlocken".[11] Auch die NATO gibt der Industrie Schützenhilfe mittels der NATO Industry Cyber Partnership (NICP)[12]: Um zu lernen, „Cyberattacken besser zu verhindern, auf sie zu reagieren und sich von ihnen erholen zu können, […] werden wir als Teil einer offenen, transparenten und für beide Seiten gewinnbringenden Partnerschaft mit der Industrie zusammenarbeiten".

Stimmen aus der Forschung und der Presse

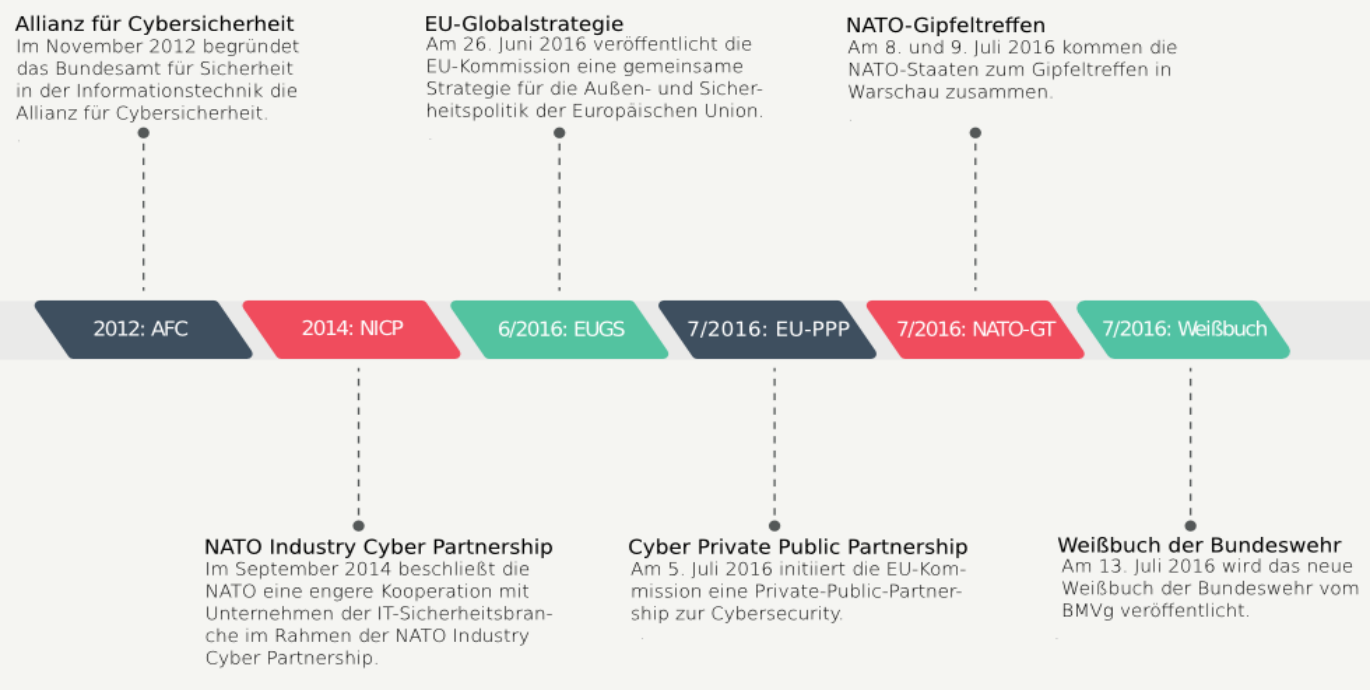
Sehr kritische Worte für die aktuelle politische und militärische Stoßrichtung im Umgang mit Cyberattacken finden sich vor allem in wissenschaftlichen Publikationen wie beispielsweise von der *Stiftung Wissenschaft und Politik* (SWP), die eine „Militarisierung" des „freie[n] Internet[s]" thematisiert[13] und in einer Studie im März 2016 mit „Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik" zur „Sorgfaltsverantwortung im Cyberraum" mahnt[14]. Im virtuellen Raum sei in Friedenszeiten der zivilen Komponente Vorrang gegenüber der militärischen zu geben. Polizeiliche, staatliche und militärische Aktionen im Cyberspace seien transparent zu machen und mit anderen Interessensgruppen der Gesellschaft abzustimmen. In einer Ausgabe des Journals „WeltTrends" zum Cyberwar sprechen Autor_innen von der Konstruktion, der „Erfindung des Cyberwars", welche für die Zivilgesellschaft Bedrohungsszenarien im Cyberraum heraufbeschwört, wie sie „in ähnlicher Form auch schon als Probleme der IT-Sicherheit diskutiert wurden".[15] Eine höchstens strafrechtlich oder im Eigentumsrecht relevante, „verbrecherische" Aktion zu einem militärischen Angriff zu stilisieren sei durchaus bemerkenswert.

Die wissenschaftlichen Arbeiten zum Thema Cyberwar finden allerdings nur bedingt Anklang in der breiten Öffentlichkeit. Sie sind vielmehr als Empfehlungen für Regierungshandeln oder als Denkanstoß für politische Arbeit gedacht. Große Tageszeitungen und öffentlich-rechtliche Sender sind als Schnittstelle zwischen Politik und Gesellschaft dagegen maßgeblich für die Form des öffentlichen Diskurses zu tagesaktuellen Themen verantwortlich. Und so ist es entscheidend, mit welchem Ton die Journalist_innen über den Cyberkrieg berichten und wie sehr sie ihre Darstellung an den großen staatlichen, militärischen und privatwirtschaftlichen Interessensträger_innen orientieren.

Doch sachliche Artikel zum „Krieg im Netz" oder eine fundierte Auseinanderstzung mit der tatsächlichen Bedrohungslage für die Zivilgesellschaft sind in den Mainstream-Medien scheinbar eher unpopulär. Vielmehr überschlagen sich die Meldungen zu immer neuen Angriffen aus dem Nichts – unkontrollierbar und unberechenbar. Die einen sprechen vom „Angriffsziel Deutschland"[16], einer „Gefahr durch Cyber-Angriffe [...] [für] Krankenhäuser oder die Energieversorgung"[17], von „Hackerangriff[en] auf […] deutsche Banken"[18] oder von möglichen Attacken auf „die neuesten und beliebtesten Smartphones"[19]. Keine beruhigenden Worte für die Leser_innen also – Cybercrime, Cyberwar und Cyberterrorismus werden in der Presse zur großen Bedrohung erklärt. Wie die Regierung mit dieser Gefahrenlage umgeht, wird in zumeist wohlwollendem Ton im gleichen Atemzug nachgeliefert: Auf militärischer Seite „[sucht] die Bundeswehr […] IT-Spezialisten für den Krieg im Cyberspace"[20], „Geheimdienste rüsten auf gegen Terror und Cyber-Attacken"[21] und alle polizeilichen und militärischen Bemühungen kommen dann einer „mobile[n] Einsatztruppe gegen Hacker" zugute[22].

Zivilgesellschaftliche Akteur_innen im Cyberkrieg

Zur Angst und Panikmache in Politik und Tagespresse um eine neue kriegerische Bedrohung wird also gleichzeitig eine Lösungsstrategie formuliert: Die Regierung, das Militär, die Geheimdienste – sie alle sollen der Gesellschaft aus der akuten Bedrohungslage mit den nötigen Mitteln helfen. Was die Bürger_innen dabei opfern sollen, sind erhebliche Teile ihrer digitalen Privatsphäre. Wie gut die Rechnung allerdings für die Machteliten in diesem Falle aufgeht, wird erst bei einem genaueren Blick auf die tatsächliche Gefahr von Cyberattacken für die Zivilgesellschaft sichtbar: Bisher besteht in Europa und den USA die größte Cyber-Bedrohung für den Staat, militäri-



Quelle: Selbst erstellte Grafik nach einer Vorlage von freepik.com

sche Strukturen, Unternehmen und die Geheimdienste selbst. Erfolgreiche Angriffe auf die Energieversorgung eines Landes oder andere kritische zivile Infrastruktur wurden bisher nur von westlichen Staaten durchgeführt, die damit die eigentliche Bedrohung für zivilgesellschaftliche Akteur_innen darstellen. So schlagen Bundesregierung, EU-Kommission und NATO ein geschicktes Rad von der aus Steuergeldern getragenen Cybersicherheit ihrer Herrschafts- und Wirtschaftsstruktur hin zur Legitimation vermehrter Überwachung von Privatpersonen.

Presseberichte zu offensiven Cyberaktionen, die von NATO-Staaten ausgehen, sind selten. Die westlichen Militärstrategien sprechen zwar häufig von der Notwendigkeit offensiver Cyberkapazitäten, die eigentlichen Angriffe werden dann aber im Geheimen durchgeführt. Die Dunkelziffer der von NATO-Staaten iniiterten Cyberattacken dürfte daher dementsprechend hoch sein. So wurden beispielsweise ab dem Jahr 2007 iranische Atomanlagen mittels des Computerwurms *Stuxnet* aus den USA angegriffen, was erst im Jahr 2010 bekannt wurde.[23] Seit Kurzem wird außerdem berichtet, dass die Bundeswehr im Jahr 2015 das afghanische Mobilfunknetz im Zuge einer Geiselbefreiung attackierte.[24] Die beiden Cyberangriffe stellen eine ernsthafte Gefährung der Sicherheit und einen empfindlichen Eingriff in die Privatsphäre der iranischen bzw. der afghanischen Zivilgesellschaft dar.

Das Bedrohungsszenario des Cyberkriegs wird damit zu einer sehr realen Bedrohung für die Zivilgesellschaft. Und so darf das Eifern des Militärs und der Polizeibehörden um Verfügungsgewalt im virtuellen Raum als Signal für Privatpersonen und Gruppierungen verstanden werden, sich dieser anbahnenden staatlichen Kontrolle zu entziehen. Sei es mithilfe einer Verschlüsselung der privaten Kommunikation auf kollektiv organisierten *CryptoParties*, die Unterstützung der Initiative *Freifunk*, die sich für freies, offenes und anonymes Surfen einsetzt oder des antimilitaristischen Kampfes des *Forum Informatiker_innen für Frieden und gesellschaftliche Verantwortung*[25], dessen Mitglieder sich für eine friedliche und am Gemeinwohl orientierte Nutzung der Informationstechnik einsetzen.

Anmerkungen

1 Cyber-Angriff auf weitere Bank, tagesschau.de, 10.09.2016.
2 National Security Agency.
3 Hacker erbeuteten offenbar NSA-Software, Spiegel online, 10.09.2016.
4 NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/, 13.09.2016.
5 European Cybercrime Centre (EC3), europol, 13.09.2016.
6 Cyber- und Informationsraum, in: Europäische Sicherheit & Technik 9/2016, S. 44-47.
7 Warsaw Summit Communiqué, NATO, 13.09.2016, Abschnitt 70. Vom Autor aus dem Englischen übersetzt.
8 Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, pdf, 13.09.2016, S. 36.
9 Shared Vision, Common Action: A Stronger Europe, pdf, 13.09.2016, S. 22. Vom Autor aus dem Englischen übersetzt.
10 Bundesamt für Sicherheit in der Informationstechnik: Allianz für Cybersicherheit, AFC, 14.09.2016.
11 Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats, europa.eu, 14.09.2016. Vom Autor aus dem Englischen übersetzt.
12 NATO Industry Partnership, nato.int, 14.09.2016. Vom Autor aus dem Englischen übersetzt.
13 Einträge auf swp.org zum Thema „Cyber", swp.org, 14.09.2016.
14 Annegret Bendiek: Sorgfaltsverantwortung im Cyberraum, SWP-Studien 2016/S 03, 14.09.2016.
15 Kai Denker: Die Erfindung des Cyberwars, in: WeltTrends 113, S.17-21.
16 Angriffsziel Deutschland, tagesschau.de, 12.09.2016.
17 Die Bundeswehr sucht IT-Spezialisten für den Krieg im Cyberspace, süddeutsche.de, 12.09.2016.
18 Hackerangriff auf dreizehn deutsche Banken, faz.net, 12.09.2016.
19 Sicherheitslücke in 900 Millionen Handys, faz.net, 12.09.2016.
20 Die Bundeswehr sucht IT-Spezialisten für den Krieg im Cyberspace, süddeutsche.de, 12.09.2016.
21 Geheimdienste rüsten auf gegen Terror und Cyber-Attacken, süddeutsche.de, 12.09.2016.
22 Mobile Einsatztruppe gegen Hacker, tagesschau.de, 12.09.2016.
23 Obama ordnete Stuxnet-Attacken an, taz.de, 24.09.2016. Vgl. auch: Stuxnet, Wikipedia, 24.09.2016.
24 Bundeswehr-Hacker knackten afghanisches Mobilfunknetz, Spiegel Online, 24.09.2016.
25 cryptoparty.in; freifunk.net; fiff.de.