Onlineoffensive

Die Bundeswehr im Cyber- und Informationsraum

von Thomas Gruber

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. Im April 2016 gab Verteidigungsministerin Ursula von der Leyen bekannt, die Struktur der Bundeswehr bis April 2017 um einen eigenen Organisationsbereich zum Cyber- und Informationsraum (CIR) zu ergänzen.[5] Das Kommando des CIR wird in Bonn Hardthöhe, dem Hauptsitz des BMVg, angesiedelt sein und soll 13.700 vorhandene Dienstposten befehligen. 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 sollen 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") fallen. 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 Bundeswehr-Karriere begeistert werden. Dabei ist das Ziel, die Bundeswehr als moderne Arbeitgeberin mit Möglichkeiten zum Quereinstieg ohne starre Hierarchien darzustellen sowie das angehende Personal durch rührselige nationalistische Aussagen und gute Bezahlung ideologisch und finanziell an sich zu binden. Eine weitere Taktik der Nachwuchsgewinnung, die die Bundeswehr schon in anderen Fachbereichen erfolgreich einsetzt, ist die Anwerbung von Studierenden. An der Bundeswehruniversität München entsteht zu diesem Zweck beispielsweise der Masterstudiengang „Cyber-Sicherheit", der ab 2018 jährlich 70 Absolvent_innen für eine anschließende Bundeswehrlaufbahn liefern soll.[9] In diesem Rahmen wird die Bundeswehruniversität um ein Forschungszentrum zur Cybersicherheit, 11 neue W3-Professuren und knapp 70 neue Stellen im Mittelbau und dem wissenschaftsstützenden Personal ergänzt. Neben der Neugewinnung von Personal sieht das BMVg außerdem die Gründung einer „Cyber-Reserve" vor, die aus ausscheidenden Berufs- und Zeitsoldat_innen, Freiwilligen Zivilist_innen oder Seiteneinsteiger_innen aus MINT-Berufen besteht und die Schlagkräftigkeit des CIR erhöhen soll.

Deutsche Strategien im Cyberkrieg und Darstellung in der Öffentlichkeit

Mit dem Organisationsbereich Cyber- und Informationsraum der Bundeswehr entsteht also ein neuer militärischer Akteur, der auf den deutschen Arbeitsmarkt drängt. Wie sieht aber die operative Strategie des CIR aus? Welche Einsatzgebiete gibt es? Die Aufgaben der deutschen Streitkräfte im Cyber- und Informationsraum werden in der öffentlichen Darstellung meist auf defensive Aktionen beschränkt – es gelte, der Verteidigung von „Staat, Wirtschaft und Gesellschaft" zu dienen. Zur Entwicklung wirksamer Verteidigungskonzepte müssten zwar auch Cyberattacken erforscht und verstanden werden, diese würden aber keinem Angriffszweck dienen. Sollte zur Landesverteidigung doch einmal eine offensive Nutzung der Cyber-Konzepte vonnöten sein, so seien diese laut Katrin Suder, der zuständigen Staatssekretärin des BMVg, wie jeder andere militärische Angriff der Bundeswehr auch durch ein Mandat des Bundestages zu legitimieren.[10] Diese Versuche, damit auch im Cyber- und Informationsraum über eine deutsche Politik der militärischen Zurückhaltung zu sprechen, wirken aufgrund der militärischen Strategiepapiere und des tatsächlichen Vorgehens von Bundeswehr und BMVg nahezu lächerlich. Während öffentlich ausufernd über das destruktive Potential von Cyberangriffen berichtet wird, die noch dazu nur schwer nachzuverfolgen sind, sind ebendiese Eigenschaften natürlich auch äußerst interessant für das deutsche Militär. Und so wird im Weißbuch der Bundeswehr 2016 zum Thema Cyber- und Informationsraum von „offensive[n] Hochwertfähigkeiten, die es zu beüben und weiterzuentwickeln gilt"[11] gesprochen.

Nord-Eingangsbereich der Bundeswehr-Universität München. Quelle: High Contrast via Wikimedia

Wie diese „Hochwertfähigkeiten" verwendet werden, zeigt beispielsweise die seit kurzem bekannte Attacke der Gruppe Computer Netzwerk Operationen, die im CIR zukünftig zum Zentrum Cyber-Operationen ausgebaut wird[12]: Bereits im Jahr 2015 attackierten deutsche Soldat_innen das afghanische Mobilfunknetz, um an Informationen zu einer Geiselnahme zu gelangen. Da dieser Einsatz weder ein Bundestagsmandat hatte, noch öffentlich gemacht wurde, ist zu vermuten, dass bei weitem nicht alle offensiven Cyberaktionen durch die vorgesehenen Kontrollinstanzen gehen. Außer im Rahmen eines Militäreinsatzes soll die Bundeswehr auch verstärkt in die zivile Kommunikation eindringen. Im Abschlussbericht zum Aufbaustab des CIR ist diesbezüglich von einer verstärkten Zusammenarbeit des BMVg mit dem Bundesministerium des Inneren (BMI) die Rede, in deren Rahmen „gemeinsam ein neues Verständnis über die intensivere Kooperation und auch Beitragsfähigkeit der Bundeswehr […] auch in Friedenszeiten"[13] entwickelt werden soll. Nach den militärischen Publikationen ist außerdem der Begriff der Landesverteidigung ein äußerst biegsamer: So seien nicht nur militärische Attacken ein Grund für ein Eingreifen der Bundeswehr, sondern auch Wirtschaftsspionage oder Rekrutierungsbemühungen terroristischer Gruppierungen in sozialen Netzwerken. Gleichzeitig, so wird allerdings betont, sollen die sonst für solche Aufgaben zuständigen Polizeien und Geheimdienste nicht in ihren Kompetenzen beschnitten werden, sondern eine „Überlappung" mit den Arbeitsbereichen der Bundeswehr stattfinden.

Bewertung und Bedeutung

Die Darstellung von Seiten des Staates und der Bundeswehr behandelt Cyberattacken auf staatliche Institutionen oder privatwirtschaftliche Unternehmen wie militärische Angriffe auf das eigene Land. So bekommen Probleme der IT-Sicherheit oder allenfalls kriminelle Aktionen wie Wirtschaftsspionage und Eigentumsdelikte im Cyberraum schnell eine militärische Bedeutung.[14] Die Zivilgesellschaft wird dabei als zu schützendes Objekt vereinnahmt, um auf dieser Grundlage das bestehende Wirtschafts- und Herrschaftssystem im Cyberraum zu verteidigen. Zu diesem Zweck werden der Bundeswehr erhebliche finanzielle und personelle Kapazitäten sowie weitreichende Befugnisse im Cyber- und Informationsraum zur Verfügung gestellt. Da die Bundeswehr dabei in einem vorwiegend zivil genutzten Raum agiert, wird empfindlich in die digitale Privatsphäre einzelner Personen oder Personengruppen eingegriffen. So gerät die Zivilgesellschaft auch im virtuellen Raum zunehmend ins Kreuzfeuer staatlicher und militärischer Akteur_innen.

Die aktuellen Versuche, mit der sich die Bundeswehr neben Polizeien und Geheimdiensten Verfügungsgewalt im Cyber- und Informationsraum verschaffen will, können als zusätzliches Alarmsignal für zivilgesellschaftliche Akteur_innen verstanden werden. Ob Privatpersonen, aktivistische Gruppen oder politische Vereinigungen – es gilt sowohl, eigene kritische Daten zu schützen, als auch den virtuellen Raum gegen staatlichen und militärischen Angriff zu verteidigen und wieder zivil zu vereinnahmen.

Anmerkungen

1 Hackerangriff auf dreizehn deutsche Banken, faz.net, 5.1.2017.
2 Die Bundeswehr sucht IT-Spezialisten für den Krieg im Cyberspace, sueddeutsche.de, 5.1.2017.
3 Warnung vor russischen Cyberattacken: Angriffsziel Deutschland, tagesschau.de, 5.1.2017.
4 Massiver Hacker-Angriff auf Thyssen-Krupp - waren es Chinesen?, derwesten.de, 5.1.2017.
5 Abschlussbericht Aufbaustab Cyber- und Informationsraum, pdf, 5.1.2017.
6 Folien CIR, pdf, 5.1.2017.
7 "Mach, was wirklich zählt": So viel kostet die Bundeswehr-Werbung, fr-online.de, 5.1.2017.
8 Abschlussbericht CIR, S. 32.
9 Größtes Forschungszentrum für Cyber entsteht, unibw.de, 5.1.2017.
10 Mandatierung, Attribution und offensive Fähigkeiten? Anhörung zur Bundeswehr im „Cyberraum", netzpolitik.org, 5.1.2017.
11 Weißbuch der Bundeswehr 2016, pdf, S.93, 5.1.2017.
12 Entführte Deutsche Bundeswehr-Hacker knackten afghanisches Mobilfunknetz, spiegel.de, 5.1.2017.
13 Abschlussbericht CIR, S. 37.
14 Kai Denker: Die Erfindung des Cyberwars, in: WeltTrends 113, S. 17-21.