erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Thomas Gruber

Die Marschrichtung im Cyber- und Informationsraum

Im April 2017 wurde das neue Kommando Cyber- und Informationsraum (CIR) *am Standort Bonn aufgestellt. Mit ihm existiert nun die Führungsstruktur für den militärischen Bereich Cyber- und Informationsraum, der voraussichtlich 2021 personell vervollständigt wird. Knapp 14.000 SoldatInnen sollen dann an verschiedenen deutschen Standorten arbeiten, bisher sind es etwa 12.500. Die Bundeswehr muss sich innerhalb kurzer Zeit um mehr als 1.000 IT-Fachkräfte, bevorzugt mit militärischer Ausbildung, bemühen – keine leichte Aufgabe.*

Doch auch ohne die volle Truppenstärke ist der neue Organisationsbereich bereits einsatzfähig: Zum Großteil wurden bereits bestehende Kommandos und deren untergeordnete Bataillone dem Kommando CIR unterstellt. In den Arbeitsbereich CIR fallen nun beispielsweise die psychologische Kriegsführung *(Zentrum Operative Kommunikation der Bundeswehr)*, die Störung feindlicher und Sicherung eigener Kommunikationsnetze *(Bataillone Elektronische Kampfführung)*, die Vernetzung und technische Ausstattung der Kriegseinheiten *(Kommando Informationstechnik der Bundeswehr)* sowie Angriff und Verteidigung im Cyberraum (*Computer Netzwerk Operationen*, bald: *Zentrum Cyberoperationen*).

Die genaue Struktur des neuen Organisationsbereichs und die Zielsetzung der Bundeswehr im Cyber- und Informationsraum sind unter anderem dem Abschlussbericht *Aufbaustab Cyber- und Informationsraum*[1], der *Strategischen Leitlinie Cyber-Verteidigung* des Bundesministeriums der Verteidigung (BMVg)[2] und dem *Weißbuch der Bundeswehr 2016*[3] zu entnehmen. Einen kurzen Überblick geben beispielsweise die Artikel *Es cybert bei der Bundeswehr*[4] und *Onlineoffensive*[5]. Jene thematischen Umrisse sollen im Folgenden um einige Gedanken zur deutschen Strategie im Cyber- und Informationsraum ergänzt werden, die während der FIfFKon 2017 angeregt wurden.[6]

Werbung, Wirkung, Widerstand

Die Aussetzung der Wehrpflicht ab dem Jahr 2011 beschränkt die Bundeswehr in ihrer wichtigsten Ressource: SoldatInnen. Gleichzeitig steigt die Zahl der deutschen Kriegseinsätze und damit auch der benötigten Truppenkontingente. In diese Zeit fällt nun noch der Aufbau des neuen Cyberkommandos – der Personalmangel ist programmiert. Das Gegenmittel der Wahl ist für das BMVg großflächige, bundesweite, zielgruppenorientierte Werbung. Von der Plakatkampagne „Mach, was wirklich zählt" über Werbeveranstaltungen in Schulen, auf Jobmessen und in Arbeitsagenturen bis zu YouTube-Serien („Die Rekruten", „Mali") – die Bundeswehr ist inzwischen omnipräsent. Zunehmend versucht sie dabei auch „Erstkontakt" zu jungen Menschen noch weit jenseits des Rekrutierungsalters aufzunehmen: Eigene Websites für Jugendliche, Werbung in Jugendmagazinen, gezielte Postsendungen, Abenteuercamps und vieles, vieles mehr. Etwa 35 Millionen Euro kostet die Nachwuchswerbung für das deutsche Militär jährlich. Immer dabei: Ein starker Fokus auf den neuen Organisationsbereich CIR. So macht beispielsweise das *Projekt Digitale Kräfte* zur Gewinnung von IT-Fachpersonal gut ein Viertel der Kosten der gesamten „Mach, was wirklich zählt"-Kampagne aus; in den vergangenen Jahren war die Bundeswehr wiederholt auf der Computerspiele-Messe *gamescom* mit einem Stand vertreten, 2017 sogar mit einer eigenen *Challenge-App* für Mobilgeräte; und im Rahmen der sogenannten *Cyber-Days* und eines *IT-Camps* gab es neben einer möglichst spannenden Übung und Lagerleben auch noch eine abschließende LAN-Party für die TeilnehmerInnen.

Die Werbeoffensive der Bundeswehr hat in den letzten Jahren durchaus Wirkung erzielt. 2017 vermeldete das Verteidigungsministerium begeistert, dass es „im Sendezeitraum der Serie *Die Rekruten* […] 40 Prozent mehr Zugriffe auf die Karriere-Website, ein Viertel mehr Anrufe bei der Karriere-Hotline und 21 Prozent mehr Bewerbungen bei Mannschaften und Unteroffizieren"[7]gab. Auch danach stieg das Interesse am SoldatInnenberuf weiter: Im ersten Halbjahr 2017 gab es beim deutschen Militär fast so viele Einstellungen wie im ganzen Jahr 2016.[8] Die *Castenow*-Werbeagentur, welche den Auftrag des Verteidigungsministeriums bekommen hat, erhält seitdem einen Preis der Werbebranche nach dem anderen.[9]

Die Sprüche (wie „Deutschlands Freiheit wird auch im Cyberraum verteidigt" und „Wir kämpfen auch dafür, dass du gegen uns sein kannst") und die Maßnahmen der Nachwuchswerbung sind oftmals sehr forsch bis provokativ – und das ist ohne Frage auch Kal-

Abbildung 1: Kind mit Waffe am Tag der Bundeswehr 2016 in Stetten am kalten Markt (Quelle: DFG-VK)[10,11]

kül, um die Bundeswehr wieder mehr zum öffentlichen Gesprächsthema zu machen. Allerdings hat dies in den letzten Jahren auch vermehrt zu Diskurs und Widerstand geführt, den sich das Verteidigungsministerium keineswegs so gewünscht haben dürfte. Nach dem *Tag der Bundeswehr 2016* gingen Fotos durch die Presse, auf denen Kinder – teilweise vermutlich noch im Grundschulalter – mit Handfeuerwaffen (siehe Abbildung 1) und auf Panzern zu sehen sind; die Kampagne *Schulfrei für die Bundeswehr* begleitet seit 2010 den Einsatz von Jugendoffizieren an deutschen Schulen mit vielfältigem Protest; Bundeswehrplakate werden regelmäßig zerstört oder kreativ umgestaltet (siehe Abbildung 2); wiederholt brandet die Diskussion darüber auf, ob die Bundeswehr mit jährlich über 1.000 rekrutierten Minderjährigen gegen die UN-Kinderrechtskonvention verstoße; und vieles mehr. Gerade der Anschein von Spiel und Spaß, den die Bundeswehr auch bei der Anwerbung von IT-Fachkräften für den CIR vermitteln will, und der krasse Gegensatz des tatsächlichen militärischen Wirkens heizen die öffentliche Diskussion derzeit immer wieder an.

Vom Besetzen des zivilen virtuellen Raumes zum Einsatz im Inneren

Der Angriff auf feindliche Computernetzwerke und die Verteidigung der eigenen im Auslandseinsatz ist eine Aufgabe des Organisationsbereichs CIR, viele weitere Arbeitsgebiete liegen allerdings im zivilen virtuellen Raum – vornehmlich auch im Inland. Zu Beginn der Diskussion um eine deutsche Cybertruppe dienten Wirtschaftskriminalität und zwischenstaatliche Spionage als häufig bemühte Motivationsquellen für eine militärische Aufrüstung des virtuellen Raumes. Zunächst konnten jene Ideen noch mit PR-Taktik verwechselt werden – die Bundeswehr als Retterin und Beschützerin der BürgerInnen und der deutschen Wirtschaft. Doch inzwischen wird immer klarer sichtbar, dass das Bedrohungsszenario *Cyberkrieg* auch hervorragend geeignet ist, das heftig umstrittene Konzept eines Inlandseinsatzes der Bundeswehr salonfähiger zu machen. Zumindest zeigen die verschiedenen Strategiedokumente zum CIR, dass der zivile virtuelle Raum zukünftig stärker militärisch durchdrungen und besetzt werden soll[12]: Das BMVg warnt vor „Bedrohungen im Cyber- und Informationsraum", wie etwa dem „Diebstahl und Missbrauch persönlicher Daten oder […] der Wirtschaftsspionage". „Eine besondere Herausforderung" ist weiter die feindliche „Nutzung der digitalen Kommunikation zur Beeinflussung der öffentlichen Meinung", beispielsweise „in sozialen Netzwerken" oder „auf Nachrichtenportalen". In der logischen Konsequenz erklärt das Verteidigungsministerium den Cyber- und Informationsraum neben „Land, Luft, See und Weltraum" zu einem neuen militärischen „Operationsraum"[13]. Die somit beschworene Bedrohungslage, gepaart mit der Definition eines fünften Schlachtfeldes, führt zu einem breiten Aufgabenspektrum für die junge Cybereinheit[14]: Neben dem Schutz der eigenen IT-Systeme und Angriffen auf feindliche Computer- und Kommunikationsnetzwerke soll die Bundeswehr in Zukunft auch zivile kritische IT-Infrastruktur schützen, mit den eigenen Informationen zu einem „gesamtstaatlichen Lagebild" beitragen und „an der Meinungsbildung im Informationsumfeld der Interessensgebiete der Bundeswehr" teilhaben. Das Wort *gesamtstaatlich* scheint sich beim BMVg größter Beliebtheit zu erfreuen. Es ermöglicht, die Bundeswehr in Fragen der zivilen Sicherheit neben Polizeien und Geheimdienste zu stellen und künftige Einsätze bei innerstaatlichen Gefahrenlagen zu rechtfertigen.

Abbildung 2: Beispiel für Adbusting, Bild aus „Was ist Adbusting?" https://sozialrevolutionaere-aktion.com/2018/02/22/was-ist-adbusting

Parlamentsvorbehalt, Solidaritätsklausel, Bündnisfall

Ein weiteres Hauptaugenmerk in Militärstrategien zum Cyber- und Informationsraum liegt auf der Einordnung militärischer Aktionen in die aktuelle Rechts- und Bündnislage. Denn zumindest auf dem Papier gibt es mehr oder minder strikte Voraussetzungen für den Einsatz militärischer Gewalt – so auch bei Angriffen auf Computer- und Kommunikationsnetzwerke. Auf bundesdeutscher Ebene gilt bei Auslandseinsätzen der Bundeswehr der Parlamentsvorbehalt, das heißt, ein deutscher Kriegseinsatz ist nur zulässig[15], wenn der Bundestag dem zustimmt. Nun sollte dies, wenn der Cyber- und Informationsraum schon als neues Schlachtfeld deklariert wird, selbstverständlich auch für den Bundeswehreinsatz im virtuellen Raum gelten. Und in der Tat spricht Katrin Suder, Staatssekretärin des BMVg, davon, dass ein Militäreinsatz im CIR ebenso wie jeder andere vom Bundestag abgesegnet werden müsse.[16] Das ist geschickt formuliert, denn für die zwei derzeit wahrscheinlichsten Angriffsszenarien wird es eben keine gesonderte parlamentarische Entscheidung geben: Entweder werden offensive Aktionen im CIR (so wie es auch aktuell der Fall ist) als Teil eines Auslandseinsatzes deklariert – die Entscheidung des Bundestages über den Gesamteinsatz rechtfertigt damit die militärischen Aktionen im virtuellen Raum. Oder die Bundesregierung ordnet mit der Begründung der Selbstverteidigung oder sonstiger Schutzmaßnahmen einen Cyberangriff an, mit dem Hinweis, dass „Gefahr im Verzug"[17] – für eine Abstimmung im Parlament also keine Zeit – sei.

Eine äußerst wichtige Rolle spielt die Idee des Cyberkrieges auch in westlichen Bündnisstrukturen wie der EU und der NATO. Denn zum einen kann innerhalb der Bündnisse eine allgegenwärtige Bedrohungslage durch angebliche Cyberangriffe aus Russland, China oder durch terroristische Gruppen heraufbeschworen werden, zum anderen hilft das Konzept der Cyberabwehr auch dabei, die rechtliche Schwelle zum Kriegseinsatz zu senken. Besonders deutlich wird dies beispielsweise in der Diskussion um das Vorgehen zur Bündnisverteidigung. Im Falle der NATO betrifft dies den *Bündnisfall* (Art. 5 des Nordatlantikvertrages), in der EU die *Beistandsklausel* (in Art. 42.7 des EU-Vertrages) sowie die *Solidaritätsklausel* (Art. 222 AEUV). Sie alle legitimieren den Einsatz militärischer Mittel von Einzelstaaten zum Zwecke der Verteidigung eines militärisch angegriffenen oder schwer bedrohten

Bündnispartners. Und was vor dem Konzept des Cyberkrieges noch eine vergleichsweise hohe Hürde war, könnte in Zukunft bei Bedarf sehr viel leichter werden. Denn sowohl in Stellungnahmen des EU-Parlaments als auch aus NATO-Kreisen wird immer wieder vernommen, dass die Beistandsverpflichtungen auch im Falle von Cyberangriffen zur Anwendung kommen sollen.[18] Im Extremfall könnte eine Hacking-Attacke damit einen bündnisweiten Kriegseinsatz (auch mit *konventionellen* Waffen) rechtfertigen. Angesichts der Tatsache, dass Polizeien, Sicherheitsfirmen und Militär jährlich zahlreiche Cyberangriffe auf westliche Verwaltungs-, Regierungs- und Sicherheitseinrichtungen verzeichnen, bergen solche Aussagen enormes Eskalationspotential.

Anmerkungen und Referenzen

1 *Abschlussbericht Aufbaustab Cyber- und Informationsraum, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf, 3.1.2018.*
2 *Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/, 3.1.2018.*
3 *Weißbuch der Bundeswehr 2016, https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf, 3.1.2018.*
4 *Es cybert bei der Bundeswehr: Digitales Aufrüsten um jeden Preis mit Gamern und Nerds, https://netzpolitik.org/2016/es-cybert-bei-der-bundeswehr-digitales-aufruesten-um-jeden-preis-mit-gamern-und-nerds/, 3.1.2018.*
5 *Onlineoffensive: Die Bundeswehr im Cyber- und Informationsraum, FIfF-Kommunikation 2/2017, S. 69–71. Abrufbar auch unter: http://www.imi-online.de/2017/04/03/onlineoffensive-die-bundeswehr-im-cyber-und-informationsraum/, 4.1.2018.*
6 *Vortrag „Die Bundeswehr im Cyber- und Informationsraum", FIfFKon 2017, Video fiff.de/r/181031, Vortragsfolien fiff.de/r/181032.*
7 *Werde Soldat, yo!, http://www.zeit.de/politik/deutschland/2017-10/bundeswehr-exclusive-mali-youtube-serie-die-rekruten, 4.1.2018.*
8 *Bewerber-Boom bei der Bundeswehr, http://www.rp-online.de/politik/deutschland/nach-rekruten-werbung-bewerber-boom-bei-der-bundeswehr-aid-1.7034502, 4.1.2018.*
9 *Castenow News, https://www.castenow.de/news/, 4.1.2018.*
10 *Grenze überschritten: Bundeswehr ließ Kinder an Handfeuerwaffen, PM DFG-VK und Netzwerk Friedenskooperative, Stuttgart, 13. Juni 2016, https://www.dfg-vk.de/unsere-themen/anti-militarisierung/grenze-ueberschritten-bundeswehr-liess-kinder-an-handfeuerwaffen.*
11 *Foto: https://www.dropbox.com/sh/nehz7aa5nim25t5/AADmEbzMW4wwP4tqN-5Kk2ita?dl=0*
12 *Weißbuch der Bundeswehr 2016, S. 36–38.*
13 *Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe.*
14 *Abschlussbericht Aufbaustab Cyber- und Informationsraum, S. 13.*
15 *„Zulässig" nach Auffassung der deutschen Regierungen der letzten knapp 20 Jahre. Mithilfe der dabei hartnäckig ignorierten Regelungen im Zwei-plus-Vier-Vertrag (dass von deutschem Boden nur noch Frieden ausgehen darf), der Präambel des Grundgesetzes (Verpflichtung der BRD, dem Frieden der Welt zu dienen) und dem internationalen Völkerrecht (Verbrechen der Aggression) ließe sich durchaus eine grundsätzliche Unzulässigkeit deutscher Auslandseinsätze rechtfertigen.*
16 *Mandatierung, Attribution und offensive Fähigkeiten? Anhörung zur Bundeswehr im „Cyberraum", https://netzpolitik.org/2016/mandatierung-attribution-und-offensive-faehigkeiten-der-verteidigungsausschuss-zur-bundeswehr-im-cyberraum/, 5.2.2018.*
17 *Zur Reichweite des Parlamentsvorbehalts für Streitkräfteeinsätze bei Gefahr im Verzug, https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2015/bvg15-071.html, 5.2.2018.*
18 *Entschließung des Europäischen Parlaments vom 22. November 2012 zu den EU-Klauseln über die gegenseitige Verteidigung und Solidarität: politische und operationelle Dimensionen, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0456&language=DE&ring=A7-2012-0356, 5.2.2018; „Cyberangriffe können Bündnisfall nach Artikel 5 auslösen", https://www.welt.de/politik/article161307855/Cyberangriffe-koennen-Buendnisfall-nach-Artikel-5-ausloesen.html, 5.2.2018.*

Informationsstelle Militarisierung auf der FIfFKon 2017

Die Informationsstelle Militarisierung (IMI) arbeitet seit über 20 Jahren in einem breiten Spektrum friedenspolitischer und antimilitaristischer Themen mit einem starken Fokus auf Deutschland, die EU und die NATO. Wir veröffentlichen Analysen und Studien, stellen RednerInnen auf Demonstrationen, ReferentInnen für Konferenzen und veranstalten jährlich einen Kongress in Tübingen.

In den letzten Jahren haben sich dabei wiederholt Kooperationsmöglichkeiten mit dem FIfF ergeben, die unsere politische Arbeit sehr bereichert haben. Die zunehmende Automatisierung und Algorithmisierung der Kriegsführung sowie ein starkes Drängen militärischer AkteurInnen in den Cyber- und Informationsraum bieten derzeit viele gemeinsame Anknüpfungspunkte. Auch 2017 gab es wieder regen Austausch zwischen FIfF und IMI: etwa über gegenseitig abgedruckte Texte, einen Vortrag des FIfF-Vorstandes Hans-Jörg Kreowski auf dem IMI-Kongress 2017 und einen IMI-Vortrag auf der FIfFKon 2017. Auch war IMI dort Gast am Informationsstand des FIfF.

http://www.imi-online.de *Thomas Gruber, IMI-Beirat*

Thomas Gruber

Thomas Gruber ist Mathematiker und promoviert an der Universität Bremen zum Thema *Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung*. Er ist Stipendiat der *Rosa-Luxemburg-Stiftung* und Mitglied der *Informationsstelle Militarisierung* (IMI) in Tübingen.