Ein hybrides Kommando

Der Organisationsbereich Cyber- und Informationsraum der Bundeswehr

von Christoph Marischka

Ein Denkmal hat sich die in der zweiten Legislaturperiode amtierende Verteidigungsministerin von der Leyen auf jeden Fall gesetzt: Mit der Abteilung Cyber- und Informationsraum (CIR) im Bundesministerium für Verteidigung (BMVg) und einem identisch benannten Kommando in Bonn wurde de facto eine neue »Teilstreitkraft« der Bundeswehr ins Leben gerufen, auch wenn dieser Begriff im deutschen Diskurs gerne gemieden wird. Mit einem eigenen Inspekteur, der dem Kommando vorsteht, ist dieser Organisationsbereich den Teilstreitkräften Heer, Marine und Luftwaffe sowie der Streitkräftebasis und dem Sanitätsdienst gleichgestellt. Entsprechend erklärte von der Leyen den „Cyber- und Informationsraum" anlässlich der Aufstellung des neuen Kommandos „neben Land, Luft, See und Weltraum" nicht nur zur „sicherheitspolitische[n] Domäne", sondern auch zum neuen „Operationsraum für die Bundeswehr".[1] Mit einer Zielgröße von 15.000 militärischen und zivilen Dienstposten liegt die neue Teilstreitkraft auch im Umfang nur knapp hinter dem der Deutschen Marine.

Dabei handelte es sich in einem ersten Schritt vor allem um eine Umstrukturierung. Im Tagesbefehl vom 17. September 2015, mit dem ein Aufbaustab für das neue Kommando ins Leben gerufen wurde, schrieb von der Leyen: „Die Bundeswehr hat bereits gute Fähigkeiten im Cyber-Raum und in der Informationstechnologie (IT) – diese sind aber organisatorisch verstreut." Die etwa 13.700 Dienstposten, die dem neuen Kommando zum 30. Juni 2017 unterstellt wurden, setzten sich fast ausschließlich aus den bereits bestehenden Truppengattungen Fernmeldetruppen, elektronische Kampfführung (EloKa), Geoinformationswesen und Operative Kommunikation zusammen. Entsprechend wurden dem Kommando etwa 5.500 Dienstposten aus dem Bereich Militärisches Nachrichtenwesen, 5.500 aus der IT-Cybersecurity, 650 vom Zentrum für Geoinformationswesen der Bundeswehr und 850 Dienstposten für Operative Kommunikation zugeordnet.[2] Das Kommando besteht zunächst aus 260 Dienstposten, bis spätestens 2023 sollen es jedoch 700-800 werden.

Eine Besonderheit des Organisationsbereiches CIR besteht darin, dass der entsprechenden Abteilung im BMVg (nicht aber dem Kommando CIR) auch die unternehmerische Steuerung der BWI GmbH mit 3.500 bis 4.000 Mitarbeiter*innen obliegt. Die BWI GmbH wurde 2006 von der Bundeswehr gemeinsam mit den Firmen Siemens und IBM gegründet und führte als Öffentlich-Private Partnerschaft die Modernisierung und Vereinheitlichung der »nicht-militärischen« Informationstechnologie der Bundeswehr durch. Seit 2016 befindet sie sich im alleinigen Besitz des Bundes und ist für den Betrieb der »weißen« (»nicht-militärischen« in Abgrenzung zur »grünen«) IT der Bundeswehr zuständig. Laut Wikipedia betreut sie bundesweit rund 1.200 Liegenschaften der Bundeswehr und betreibt u.a. drei zentrale Rechenzentren und 25 Servicecenter. An etwa 90 Standorten der Bundeswehr ist die GmbH dauerhaft präsent, an zentralen Liegenschaften des Organisationsbereichs CIR sogar sehr umfangreich, in Rheinbach etwa mit 200 Mitarbeiter*innen. „Eine Tendenz zur Hybridisierung der Verteidigung – im Verständnis zivil/militärisch – ist" für die Bundesregierung dennoch „nicht erkennbar".[3]

Die Aufgaben des Kommandos CIR

Dem Kommando CIR unterstehen das Kommando Informationstechnik, das Kommando Strategische Aufklärung sowie das Zentrum für Geoinformationswesen der Bundeswehr.

Das Kommando Informationstechnik führt vor allem die recht gleichmäßig über die Bundesrepublik verteilten Informationstechnikbataillone, die für den Betrieb sicherer Kommunikationsverbindungen in Deutschland, in den Einsatzländern und zwischen den hiesigen Stäben und den Kräften im Einsatz zuständig sind (militärisch werden diese Aufgaben auch als »Führungsunterstützung« bezeichnet). Während die Kommunikation der Bundeswehr in der Vergangenheit überwiegend auf Kabel- und Richtfunknetzen basierte, haben mit der »Einsatzorientierung« wesentlich verwundbarere und angreifbarere Satellitenverbindungen an Bedeutung gewonnen. „Von Kabelbaukräften zu IT-Spezialisten" übertitelte kreisbote.de sein Portrait des Informationstechnikbataillons 293 in Murnau im Grunde recht treffend.

In dem Artikel wird auch deutlich, dass gerade diese Truppengattung – wenn auch meist mit kleineren Kontingenten – umfangreich an Auslandseinsätzen beteiligt ist. So heißt es alleine zum Murnauer Bataillon im bereits angesprochenen Portrait vom April 2018: „Die Abstellung von zirka 80 Soldaten nach Bosnien-Herzegowina bildete 1999 den Auftakt für die in den folgenden Jahren anstehenden, größeren Auslandseinsätze des Bataillons. Zum gegenwärtigen Zeitpunkt leisten Murnauer Soldatinnen und Soldaten ihren Dienst in Mali, im Irak, Afghanistan, Kosovo und Litauen."[4]

Neben den Informationstechnikbataillonen unterstehen dem Kommando Informationstechnik auch mehrere Dienstposten, die aus dem ehemaligen Beschaffungsamt der Bundeswehr herausgelöst wurden, das zuvor bereits in »Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr« umbenannt wurde.

Deutlich vielfältiger sind die Aufgaben des Kommandos Strategische Aufklärung, das wesentliche Komponenten des militärischen Nachrichtenwesens umfasst und einen klaren räumlichen Schwerpunkt südlich von Bonn aufweist. Der Standort des Kommandos befindet sich recht versteckt in einem Industriegebiet bei Gelsdorf, südlich des Autobahnkreuzes Meckenheim. Hier befand sich bis 2007 das Zentrum für Nachrichtenwesen der Bundeswehr – eine rein militärische Parallelstruktur zum BND –, das mit seinem Bekanntwerden aufgelöst bzw. in das Kommando Strategische Aufklärung umgewandelt wurde.

Das Kommando führt u.a. die Bataillone für Elektronische Kampfführung. Diese haben die Aufgabe, gegnerische Kommunikationsnetze aufzuklären, abzuhören und zu stören.

Auch das Zentrum Cyberoperationen in Rheinbach untersteht dem Kommando Strategische Aufklärung und erfüllt auf der Ebene der Software ähnliche Funktionen wie die elektronische Kampfführung auf der Ebene der Hardware, stützt sich dabei jedoch stärker auf zivile Infrastruktur und Technologie. In Rheinbach befindet sich eine Einheit mit etwa 80 Kräften, die am ehesten dem Bild einer Hacker-Truppe entspricht und

tatsächlich auch schon mit offensiven Cyber-Operationen beauftragt wurde - bekannt wurde ein Angriff auf das afghanische Mobilfunknetz zum Zwecke der Informationsgewinnung. Potentiell bestehen dort jedoch auch Kapazitäten und Fähigkeiten, um »gegnerische« IT-Systeme zu stören oder für Angriffe zu nutzen.

Auf den ersten Blick irritierend, wird auch das Zentrum für Operative Kommunikation in Mayen vom Kommando für Strategische Aufklärung geführt. Dessen Aufgaben bestehen in dem, was landläufig als »Propaganda« bezeichnet wird und von der Bundeswehr selbst in der Vergangenheit »Psychologische Kampfführung« genannt wurde. Zwar wird immer wieder behauptet, die gezielte Beeinflussung der öffentlichen Meinung mit wissenschaftlichen (oft aber auch sehr banalen) Methoden sei auf gegnerische Kräfte und die Bevölkerung in den Einsatzgebieten beschränkt, in der Praxis jedoch erweisen sich die Übergänge als fließend: So gehört zur Operativen Kommunikation auch der Betrieb des eigens für die Truppe bestehenden »Radio Andernach« sowie des Fernsehsenders BwTV, der im Internet auch für die allgemeine Öffentlichkeit präsent ist. Die Aufnahmen der Einsatzkameratrupps des Zentrums für Operative Kommunikation sind formal für die militärische Führungsebene bestimmt, finden in der Praxis jedoch– nach vorangegangener Freigabe – immer wieder ihren Weg in Publikationen des BMVg und auch in Produktionen öffentlicher und privater Sendeanstalten.

Das Zentrum für Geoinformationswesen in Euskirchen untersteht wiederum direkt dem Kommando CIR. Hier werden u.a. Satellitenaufnahmen aufbereitet und für die Führungs- und Einsatzkräften bereitgestellt. Die Bezeichnung der Einrichtung lässt eine historische Fixierung des Militärs auf Karten und die Abbildende Aufklärung vermuten, tatsächlich werden hier allerdings viele Daten verarbeitet, die aus anderen Quellen stammen. U.a. beschäftigt das Zentrum für Geoinformationswesen Ethnolog*innen, die zuvor als Interkulturelle Einsatzberater*innen oder im Rahmen der zivil-militärischen Zusammenarbeit im Ausland im Einsatz waren. In seiner Selbstdarstellung zitiert das Zentrum Majorin Eva Kaufung, eine Geografin, mit der Aussage: „natürlich [sind] auch Informationen wichtig, wie stark die Gegend besiedelt ist, welche Ethnien sind im Land beheimatet oder welche Gesundheitsgefährdungen durch Krankheiten oder Tiere existieren“.[5] Entsprechend wird von der Einrichtung gemeinsam mit zivilen Wissenschaftler*innen und Hochschulen stets an der verbesserten Aufarbeitung und Darstellung von Daten auf zunehmend interaktiven Karten gearbeitet.

Weitere Komponenten: Marktsichtung, Aus- und Fortbildung

Neben den operativen Aufgaben hat der Organisationsbereich weitere Komponenten, die sich insbesondere mit Strategie und Planung, Personalgewinnung, Aus- und Fortbildung sowie technologischen Innovationen beschäftigen und überwiegend von der Abteilung CIR im BMVg erbracht werden.

Zu deren Aufgaben gehört es, beständig den Markt für innovative Dienstleistungen und Technologien zu beobachten und diese auf ihre militärische Relevanz zu überprüfen sowie selbst entsprechende Forschung anzustoßen. Hierzu wurde u.a. ein »Cyber Innovation Hub« der Bundeswehr geschaffen, der als „Schnittstelle zwischen Startup-Szene und Bundeswehr“ fungieren soll.[6] „Wir warten nicht, bis sich ein Start-up bei uns meldet. Wir suchen ganz aktiv die neuen disruptiven Technologien“, so von der Leyen anlässlich der Indienststellung des Kommandos CIR.[7]

Ende August 2018 gab die Bundesregierung darüber hinaus die Gründung zweier Forschungsagenturen bekannt: einer »Agentur für Innovation in der Cybersicherheit« unter gemeinsamer Steuerung des Verteidigungs- und des Bundesinnenministeriums sowie eine »Agentur zur Förderung von Sprunginnovationen«. Als Vorbild für beide Agenturen gilt die Forschungsbehörde DARPA des US-Verteidigungsministeriums, wofür auch die Begründung spricht, die von der Leyen für deren „flexible Struktur“ abgibt: „[W]ir müssen viel schneller sein, wir müssen rausgehen, wir müssen die Startups suchen, die spannende Technologien entwickeln, von denen wir noch nicht wissen, ob sie erfolgreich sein werden[,] und dann werden wir die, die wir interessant finden[,] fördern, wissend, dass ein Großteil vielleicht nicht funktioniert und dann in den Sand gesetzt wird, aber es braucht nur ein goldenes Ei, also eine Technologie, die dann wirklich bahnbrechend ist, dann hat man schon die Investition wieder raus.“[8]

Eigene Forschungsprojekte im Bereich der Informationstechnik gab und gibt das BMVg u.a. am Deutsch-Französischen Forschungsinstitut Saint-Louis (ISL), dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) und bei verschiedenen Fraunhofer-Instituten in Auftrag, insbesondere bei den Fraunhofer-Instituten FHR und FKIE auf dem Wachtberg bei Bonn, die an das Netz der Bundeswehr angeschlossen sind und über eine „aktive Daten-Direkt-Verbindung“ nach Euskirchen verfügen, die als „Anbindung des Fraunhofer-Instituts FKIE an die Simulations- und Testumgebung der Bundeswehr“ dient.[9]

Als besondere »Herausforderung« für den neuen Organisationsbereich galt von Anbeginn der Planung die Gewinnung und Ausbildung des geeigneten Personals. Als Ziel wurde ausgegeben, »Spitzenkräfte« bzw. die »klügsten Köpfe“ zu gewinnen, was jedoch durch die starren Karrierestrukturen und Besoldungsstufen bei der Bundeswehr erschwert sei, da man mit den hohen Löhnen in der freien Wirtschaft schwer konkurrieren könne. Zur Ausbildung eigenen Personals wurde u.a. ein Studiengang »Cyber-Sicherheit« an der Universität der Bundeswehr in München mit elf neuen Professuren und mehreren Laboren in einem eigens errichteten Hochsicherheitsgebäude geschaffen, das ab 2018 jährlich 70 Absolvent*innen hervorbringen soll. Außerdem hat die Bundeswehr u.a. mit den Hochschulen Bremen und Bonn-Rhein-Sieg Kooperationsabkommen geschlossen, die in den jeweiligen Studiengängen (Frauenstudiengang Informatik bzw. Dualer Studiengang Informatik mit Schwerpunkt Informationssicherheit) ein Kontingent an Plätzen für die Bundeswehr reservieren.

Unter dem Arbeitstitel „Cyber-Reserve“ ist außerdem vorgesehen, „Freiwillige, Seiteneinsteigerinnen und Seiteneinsteiger sowie bislang Ungediente aus der gewerblichen IT-Wirtschaft, einschlägigen MINT-Berufen oder ähnlichen Professionen [...], die über Spezialisten-Ausbildungen oder herausragende Fähigkeiten, Fertigkeiten und Kompetenzen in einschlägigen IT-Bereichen bzw. IT-Funktionen verfügen“, zu integrieren.[10] Neben Aufträgen an Unternehmen und Start-ups wolle die Bundeswehr „die richtig harten Nerds, die sich in den Tiefen der Internet-Protokolle auskennen, mit Beraterverträgen an die Bundeswehr binden“. Die „Stars der Branche“ sollten „nicht Soldat werden müssen, um für die Cybertruppe zu arbeiten“, so das ZDF Ende August 2018. Weiter heißt es in dem Bericht: „Ungefähr 8.000 IT-Fachkräfte muss die Bundeswehr innerhalb der nächsten Zeit am freien Markt einkaufen.“[11] Diese Zahl erscheint angesichts einer Zielgröße des CIR von 15.000

Dienstposten, von denen über 13.000 bereits besetzt sind, bemerkenswert hoch. So oder so ist davon auszugehen, dass die Cybertruppe weit mehr als die anderen Teilstreitkräfte auf privatwirtschaftliche Kooperationen und private Angestellte setzen wird.

Hybride Strukturen für einen hybriden Raum

Während man bei den Richtfunknetzen der Bundeswehr womöglich noch von einer rein militärischen Kommunikationsinfrastruktur sprechen kann, stützt sich bereits die kabelgebundene Kommunikation der Bundeswehr überwiegend auf zivile Infrastruktur. Als Ergänzung zur Satellitenkommunikation über das System SATCOMBw, das teilweise von privaten Angestellten des DLR betrieben wird, kauft das BMVg zusätzliche Bandbreite bei zivilen Anbietern, deren Satelliten damit (wie etwa auch die Transatlantikkabel) zu einer zentralen militärischen Infrastruktur und im Kriegsfalle somit auch zu Zielen werden. Die »Verteidigung« der Kommunikationsstruktur der Bundeswehr lässt sich deshalb auch im Friedensfall nicht auf rein militärische Komponenten beschränken, sondern zielt zwangsläufig auf den gesamten »Cyberraum«.

Völlig undurchsichtig und offenbar nicht geklärt ist entsprechend die Aufgabenteilung zwischen zivilen Institutionen der Cybersicherheit und der Cyber-Truppe der Bundeswehr. Tatsächlich lassen sich Cyberkriminalität und Cyberkriegführung in der Praxis kaum unterscheiden – was auch daran liegt, dass (auch) anderen Staaten zumindest unterstellt wird, für Cyber-Angriffe auf privatwirtschaftliche Netzwerke und Unternehmen zurückzugreifen. Bei vielen dieser »Angriffe« ,die häufig in unfassbar hohen Zahlen angegeben werden (z.B. „Bundeswehr zählt zwei Millionen Hackerangriffe [im Jahr 2017]“; waz-online.de vom 23.3.2018) handelt es sich tatsächlich um jenes »Abtasten«, also Suchen nach Schwachstellen, das künftig auch die Bundeswehr vornehmen muss, um sich – wie im »Weißbuch« der Bundeswehr von 2016 vorgesehen – auch auf offensive Cyber-Operationen vorzubereiten. Wie wir sehen, verschwimmen im Cyber- und Informationsraum also zunehmend die Grenzen zwischen Frieden, Krieg und Verteidigungsfall.[12]

Dies gilt umso mehr, als u.a. mit dem Zentrum für Operative Kommunikation auch Komponenten in den Organisationsbereich CIR aufgenommen wurden, die den öffentlichen Diskurs betreffen. Eine klare Abgrenzung zum »Informationsraum« findet hier ebenfalls nicht statt, wodurch selbst die veröffentlichte Meinung zum „Operationsraum der Bundeswehr“ wird.[13] In dieser Domäne wähnt sich zumindest die EU bereits im Krieg. So forderte das Europäische Parlament in einer Entschließung vom 23. November 2016, die „Anerkennung und Enthüllung des russischen Desinformations- und Propagandakriegs“ als „integrale[n] Bestandteil der hybriden Kriegsführung“. Als Konsequenz wurden die Mitgliedsstaaten u.a. aufgefordert, „feindliche Informationsmaßnahmen, die in ihrem Hoheitsgebiet durchgeführt werden oder darauf abzielen, ihre Interessen zu untergraben, aktiv, vorbeugend und gemeinsam zu bekämpfen“.[14]

Angesichts dieser hybriden Auffassung des Informationsraums zwischen ziviler und militärischer Infrastruktur, zwischen Kriminalität, Angriff und Verteidigung(sfall), zwischen Elektronischer Kampfführung, militärischem Nachrichtenwesen und öffentlicher Meinung überrascht es wenig, dass auch die für diesen »Operationsraum« geschaffene Struktur des BMVg mit der Einbindung ziviler Hochschulen, Forschungsinstitute und -agenturen, mit der engen Zusammenarbeit mit Unternehmen und einer auf Beraterverträgen basierenden »Cyber-Reserve« einen sehr hybriden Charakter aufweist. Ob und wann auch zivile Einzelpersonen und z.B. Organisationen der Friedensforschung Gegenstand der Operationsführung des Kommandos CIR werden, ist gegenwärtig nicht absehbar, aber keineswegs auszuschließen.

Barettabzeichen des Kommandos Cyber- und Informationsraum.

Anmerkungen

1 Aufstellung Kommando Cyber- und Informationsraum - KdoCIR - der Bundeswehr. Europäische Sicherheit und Technik, 5.4.2017; esut.de. Die Formulierung der Ministerin lässt offen, ob sie den Weltraum ebenfalls nur als eine »sicherheitspolitische Domäne« oder auch als einen »Operationsraum der Bundeswehr« versteht.
2 Ebd.
3 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Sevim Dağdelen, Christine Buchholz, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE »Strukturen des Organisationsbereichs Cyber- und Informationsraum der Bundeswehr in Nordrhein-Westfalen«. BT-Drucksache 18/12277 vom 9.5.2017.
4 Max-Joseph Kronenbitter: Das Informationstechnikbataillon 293 in Murnau feiert den 60. Geburtstag. kreisbote.de, 17.4.2018.
5 Meldung »Geofaktoren analysieren, beschreiben und bewerten« auf cir.bundeswehr.de, 28.3.2018.
6 Seite »Cyber Innovation Hub« auf bmvg.de; ohne Datum.
7 Meldung »Aufstellung Kommando CIR: Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik« auf bmvg.de, 5.4.2017.
8 Sendung »Streitkräfte und Strategien« des NDR, 28.7.2018 (Sendungsmanuskript).
9 BT-Drucksache 18/12277, op.cit.
10 BMVg (2017): Abschlussbericht Aufbaustab Cyber- und Informationsraum. April 2017.
11 Peter Welchering: Cyber-Nerds verändern die Armee. zdf.de, 30.8.2018.
12 Siehe dazu ausführlich Ingo Ruhmann (2018): Wachsendes Ungleichgewicht – Cyberrüstung und zivile IT-Sicherheit. W&F-Dossier 86, Mai 2018.
13 So erläuterte die damals verantwortliche Staatssekretärin Karin Suder 2015 die „Rolle von Cyber“ in Hinblick auf die geplante Aufstellung des neuen Organisationsbereichs CIR anhand der Aktivitäten des „Islamischen Staates, der sich [sic!] unter anderem mit Hilfe modernster Kommunikationsmittel, Netzwerke, soziale Medien, junge Menschen rekrutiert, informiert, aktiviert und damit eine Terrorherrschaft auch aufgrund dieser modernen Kommunikationsmittel bisher unbekannten Ausmaßes etablieren konnte“ (Sendung »Streitkräfte und Strategien« des NDR, 17.10.2015, Sendungsmanuskript). Damit wurde deutlich, dass zumindest potentiell durch das Kommando CIR auch der Zugang von Akteuren zu zivilen Medien und zum allgemeinen Diskurs reguliert werden soll.
14 Entschließung des Europäischen Parlaments vom 23. November 2016 zu dem Thema »Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken«. Dokument 2016/2030(INI).