Kommando Cyber- und Informationsraum

Strukturen für den geheimdienstlichen Dauerkrieg

von Christoph Marischka

Im April 2017 wurde das *Kommando Cyber- und Informationsraum* unter Führung eines eigenen Generalinspekteurs der Bundeswehr in Bonn aufgestellt. Zum 1. Juli 2017 werden diesem gut 13.000 Dienststellen an 27 Standorten unterstellt, womit neben Heer, Luftwaffe und Marine de facto eine weitere Teilstreitkraft entsteht. Darüber hinaus ist die *Abteilung Cyber- und Informationstechnik* im Bundesverteidigungsministerium für die unternehmerische Steuerung der bundeswehreigenen *BWI Informationstechnik GmbH* zuständig, welche die Bundeswehr mit knapp 3.400 Mitarbeiter_innen an insgesamt 98 Standorten unterstützt. Das ist das Ergebnis der Antwort der Bundesregierung auf eine Kleine Anfrage (Bundestags-Drucksache 18/11688) der Bundestagsabgeordneten Sevim Dagdelen aus Duisburg. Die Abgeordnete hatte die Anfrage auf den Weg gebracht, weil zentrale Elemente der Cyber-Truppe in NRW, insbesondere im Raum Köln-Bonn, stationiert sind.

NRW als Zentrum des Cyber- und Informationsraumes

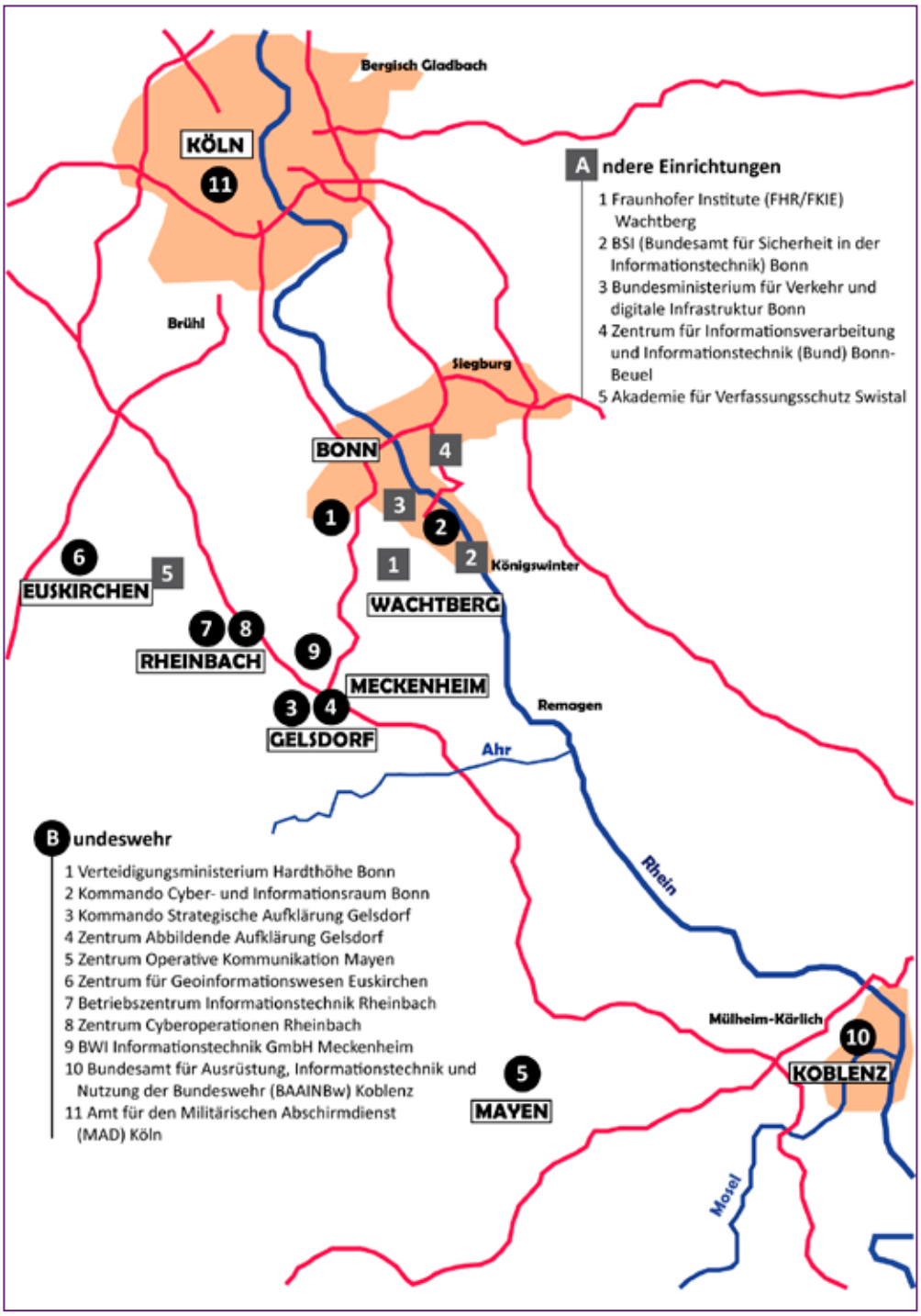
Neben dem *Kommando Informationstechnik* der Bundeswehr in Bonn und den diesem unterstellten Einheiten – darunter v.a. das *Betriebszentrum Informationstechnik* in Rheinbach sowie insgesamt sechs *Informationstechnikbataillone* in Rheinland-Pfalz, Bayern, Brandenburg und Thüringen – setzt sich der Organisationsbereich Cyber- und Informationsraum v.a. aus dem *Kommando Strategische Aufklärung* in Gelsdorf (Kreis Ahrweiler) und diesem unterstellten Einheiten zusammen. Dem Kommando Strategische Aufklärung sind u.a. das für die Satellitenaufklärung zuständige *Zentrum Abbildende Aufklärung* (ebenfalls in Gelsdorf), das *Zentrum Operative Kommunikation* (Mayen), das *Zentrum für Geoinformationswesen* in Euskirchen sowie vier *Bataillone für Elektronische Kampfführung* in Schleswig-Holstein, Niedersachsen, Rheinland-Pfalz und Hessen unterstellt. Obwohl diese Einheiten dem militärischen Nachrichtenwesen zugeordnet werden, haben viele davon neben der Aufklärung auch den Auftrag, zu „wirken". So zählt es zu den Aufgaben der Elektronischen Kampfführung, „durch eigene Störmaßnahmen gegnerischen Kräften die Nutzung des elektromagnetischen Spektrums zu verwehren". Das Zentrum Operative Kommunikation soll nicht nur „die Lage im Informationsumfeld mit ihren Möglichkeiten und Risiken ... analysieren", sondern zu seinen Aufgaben gehört laut Bundesregierung auch, „durch zielgerichtete Informationsaktivitäten geplante Wirkungen in diesem Umfeld zu erzielen und diese mit wissenschaftlichen Methoden zu messen" – früher nannte sich das Psychologische Kriegsführung. Auch das dem Kommando Strategische Aufklärung unterstellte *Zentrum Cyberoperationen* in Rheinbach „klärt auf und wirkt in der Dimension CIR [Cyber- und Informationsraum]". Diese Einheit war bereits in der Vergangenheit unter der Bezeichnung *Computernetzwerkoperationen* (CNO) für offensive Cyber-Operationen zuständig und wird das auch in Zukunft sein.

Mit dem *Kommando Cyber- und Informationsraum*, dem *Zentrum Cyberoperationen*, dem *Zentrum für Geoinformationswesen* und dem *Betriebszentrum Informationstechnik* sind zentrale Elemente des Organisationsbereichs Cyber- und Informationsraum im Großraum Köln-Bonn in Nordrhein-Westfalen stationiert, wo auch die *BWI Informationstechnik GmbH* ihren Hauptsitz hat. Die Standorte des *Kommandos Strategische Aufklärung*, das *Zentrum Operative Kommunikation* und die *Auswertezentrale Elektronische Kampfführung* in Rheinland-Pfalz liegen ebenfalls weniger als 100km von Bonn entfernt. Darüber hinaus befinden sich auf dem Wachtberg bei Bonn die *Fraunhofer-Institute für Hochfrequenzphysik und Radartechnik (FHR)* und für *Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)*. Diese gehörten bis zur Überführung in die zivile Fraunhofer-Gesellschaft 2009 der fast ausschließlich im militärischen Auftrag forschenden FGAN (*Forschungsgesellschaft für Angewandte Naturwissenschaften e. V.*) an. Demgegenüber sind die heutigen Fraunhofer-Institute zwar deutlich enger an die zivilen Hochschulen angebunden, ihre finanzielle Förderung und das Auftragsvolumen durch das Bundesverteidigungsministerium haben sich jedoch zwischen 2007 und 2016 zum Teil drastisch (tw. bis um den Faktor 5) erhöht. Dies gilt insbesondere für die Auftragsforschung am Fraunhofer FKIE, das zahlreiche Fragestellungen behandelt, die für die Cyberverteidigung von Relevanz sind. Auf die Frage, an welchen dieser Forschungsprojekte neben den Instituten die Bundeswehr, die BWI GmbH oder die *Universität Bonn* beteiligt gewesen sei, gibt sich die Bundesregierung mit Verweis auf das „im Wissenschaftsbereich übliche Selbststeuerungsrecht von Forschungsinstituten" unwissend. Zugleich deklariert sie die Auflistung der Forschungsprojekte im Auftrag des Verteidigungsministeriums als „Verschlussache – nur für den Dienstgebrauch", da sie „einen weitgehenden Rückschluss auf die Gesamtstrategie der Bundeswehr bei Technologievorhaben erlaubt." Die Institute auf dem Wachtberg, an denen zahlreiche Studierende und Doktorand_innen der Hochschule Bonn verkehren, verfügen über „zwei separate Anbindungen zum Bundeswehr-Netz", darunter eine „aktive Daten-Direkt-Verbindung" zur Generalmajor Freiherr von Gersdorff Kaserne in Euskirchen.

Aufwertung des Militärischen Nachrichtenwesens

Obwohl ein auch offensiv wirkendes militärisches Nachrichtenwesen im Kommando Strategische Aufklärung bereits zuvor existierte, erfährt dieses als wesentliches Element der Teilstreitkraft Cyber- und Informationsraum eine massive Aufwertung. Dies ist umso problematischer, als von der Bundesregierung keine klare Unterscheidung zwischen ziviler „Cyberabwehr" und militärischer „Cyberverteidigung" getroffen wird. So werden in die „Erstellung eines gesamtstaatlichen Lagebilds im Cyber- und Informationsraum" laut Bundesregierung „alle dem KdoCIR [Kommando Cyber- und Informationsraum] unterstehenden Einheiten einbezogen". Auf die Frage, [anhand] welcher Kriterien ... innerhalb der ‚gesamtstaatlichen Cybersicherheit' jene ‚Verteidigungsaspekte' identifiziert [werden], deren Bewältigung ‚durchgängig wahrzunehmende Aufgabe' der Bundeswehr" sind, und wie „die praktische Aufgabenteilung zwischen der Bundeswehr und zivilen Behörden

bei der Gewährleistung von Cybersicherheit“ stattfindet, antwortet die Bundesregierung nicht. Letztlich legt sie der Aufgabenteilung das Prinzip zugrunde: Was die Bundeswehr macht ist Verteidigung, weil es die Bundeswehr macht, und damit legal. Dabei behält sie sich vor, mit den „vorhandenen defensiven und offensiven Fähigkeiten“ auch gegen nicht-militärische Angriffe vorzugehen („zur Abwehr von (militärischen) Cyberangriffen“). Somit geht mit der Aufstellung des Organisationsbereichs Cyber- und Informationsbereich eine kontinuierliche Einbeziehung des militärischen Nachrichtenwesens in die Erstellung eines gesamtstaatlichen Lagebildes einher, während zugleich der Einsatz offensiver Cyberkapazitäten der Bundeswehr gegen nichtmilitärische Angriffe zur Option wird. Cyberverteidigung wird damit zum Dauerzustand, der Verteidigungsauftrag der Bundeswehr weiter entgrenzt und der Einsatz des militärischen Nachrichtenwesens im Inland zum Normalfall. Für keine dem Kommando Cyber- und Informationsraum unterstehende Einheit wollte sich die Bundesregierung festlegen, dass diese „nur tätig werden dürfen, sofern ein Angriff durch einen staatlichen Gegner erfolgt und/oder explizit auf Infrastrukturen der Bundeswehr zielt“.



Hybride Strategie

Mit dem Organisationsbereich Cyber- und Informationsraum wird eine neue Teilstreitkraft ins Leben gerufen, die ihre Wurzeln im militärischen Nachrichtenwesen hat und zukünftig eng und alltäglich in die zivile Cybersicherheit eingebunden werden soll. Diese Struktur verfügt über offensive wie defensive Kapazitäten (zur Aufklärung und „Wirkung“, – wie das im Militärsprech heißt) und für keine dieser Kapazitäten will die Bundesregierung ausschließen, dass sie auch gegen nichtmilitärische Gegner zum Einsatz kommen kann. Mit dem *Zentrum Operative Informationen* ist dabei auch eine Institution beteiligt, welche die gezielte Beeinflussung der öffentlichen Meinung (in den Einsatzgebieten) zum Ziel hat. Militärisches Nachrichtenwesen, Satellitenaufklärung, Cyberverteidigung und Psychologische Kriegsführung werden so künftig unter einheitlichem Kommando zusammengefasst. Einbezogen in diese zugleich weit gefasste und rechtlich nicht eingehegte Cyberverteidigung sind die über 3.000 zivilen (aber überwiegend auf Bundeswehrstandorten tätigen) Mitarbeiter der BWI Informationstechnik GmbH. Außerdem profitieren die vermeintlich zivilen Fraunhofer-Institute auf dem Wachtberg bei Bonn, die direkt an die Bundeswehr IT-Infrastruktur angebunden sind und umfassende Grundfinanzierung und Forschungsaufträge für die Bundeswehr erhalten. An diesen Forschungsprojekten sind zwar nach unserer Kenntnis auch Angehörige der Universität Bonn beteiligt, zugleich wird der Öffentlichkeit eine Einsicht in die Forschungsprojekte an Fraunhofer FKIE und FHR verwehrt. Der genauere Einblick in die neue Teilstreitkraft („Organisationsbereich“) Cyber- und Informationsraum veranschaulicht die immer weitere Ausdehnung und Entgrenzung des Verteidigungsfalls und den Kompetenzzuwachs der militärischen Nachrichtendienste im zivilen Alltag. Cybersicherheit kann nur zivil erreicht werden, ihre weitere Militarisierung heizt eine Aufrüstungsspirale an und zeugt von der Bereitschaft der Bundesregierung, selbst zunehmend hybride Strategien zu verfolgen.