Nerd-Offensive

Der Cyberspace als militärischer Operationsraum

von Jürgen Wagner

Logo des Kommando Strategische Aufklärung der Bundeswehr. Quelle: Wikipedia

Um der gewachsenen Bedeutung des Bereiches Rechnung zu tragen, veröffentlichte die Bundeswehr am 26. April 2016 den „Abschlussbericht des Aufbaustabs Cyber- und Informationsraum“, mit dem der Bereich weiter militärisch „erschlossen“ wird. Dabei geht es ganz und gar nicht allein um „Verteidigung“, wie offiziell suggeriert wird. Schon länger hat die Bundeswehr damit begonnen, sich auch Offensivkapazitäten zuzulegen.

Militärischer Operationsraum

Im „Abschlussbericht des Aufbaustabs Cyber- und Informationsraum“ wird der Bereich als fünfte Bundeswehr-Streitkräftekategorie etabliert: „Der dargestellte strategische Kontext zeigt die militärische Relevanz des CIR [Cyber- und Informationsraum] als eigene Dimension neben Land, Luft, See und Weltraum auf. Dieser ist umfassend Rechnung zu tragen.“ Bis Oktober 2016 soll hierfür in einer Grundbefähigung im Verteidigungsministerium eine eigene Abteilung „Cyber/IT“ (CIT) geschaffen und ein militärischer Organisationsbereich für den Cyber- und Informationsraum bis spätestens April 2017 aufgestellt werden, dem ein eigener Inspektor vorstehen soll. Der CIT werden dann fast 14.000 bislang über verschiedene Abteilungen verstreute Dienstposten angehören. Im Abschlussbericht des Aufbaustabs Cyber- und Informationsraum heißt es dazu: „Mit dem Aufbau des militärischen Organisationsbereiches CIR soll der Cyber- und Informationsraum als Operationsraum bzw. militärische Dimension angemessen abgebildet werden. […] Dazu wandern in einem ersten Schritt ca. 13.700 Dienstposten mit ihren Aufgaben zum Organisationsbereich CIR. Darüber hinaus werden ca. 300 Dienstposten für die Führungsfähigkeit des KdoCIR, die Aufstellung eines Zentrum Cyber-Sicherheit der Bundeswehr und die Stärkung der Aufgabe Computer Netzwerk Operationen herangezogen.“

Offensivkapazitäten & Rekrutierung

Schon 2009 meldete der Spiegel (7.2.) die Bundeswehr sei dabei, eine „Abteilung Informations- und Computernetzwerkoperationen“ genannte Hackertruppe mit 76 Soldaten für Cyberangriffe aufzustellen: „Die Bundeswehr wappnet sich mit einer bislang nicht bekannten Einheit für künftige Internet-Konflikte. […] Die Soldaten, die sich vor allem aus den Fachbereichen für Informatik an den Bundeswehruniversitäten rekrutieren, beschäftigen sich dabei auch mit den neuesten Methoden, in fremde Netzwerke einzudringen, sie auszukundschaften, sie zu manipulieren oder zu zerstören – digitale Angriffe auf fremde Server und Netze inklusive.“

Mittlerweile sind die diesbezüglichen Bemühungen noch deutlich weiter fortgeschritten. Bei dem nun veröffentlichten Abschlussbericht Cyber- und Informationsraum handelt es sich nach Eigenangaben um „ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung“. Dieses geheime Dokument vom 16. April 2015, das u.a. von Netzpolitik.org (30.7.2015) eingehend analysiert wurde, veranschaulicht, dass es bei all diesen Bemühungen tatsächlich auch darum geht, sich Offensivkapazitäten zu verschaffen. Explizit heißt es in der Leitlinie Cyber-„Verteidigung“: „Offensive Cyber-Fähigkeiten der Bundeswehr sind als unterstützendes, komplementäres oder substituierendes Wirkmittel anzusehen. Sie haben zum Einen das Potenzial, in der Regel nicht-letal und mit hoher Präzision auf gegnerische Ziele zu wirken, zum Anderen kann diese Wirkung im Gegensatz zu kinetischen Wirkmitteln unter Umständen sogar reversibel sein. Offensive Cyber-Fähigkeiten der Bundeswehr haben grundsätzlich das Potenzial, das Wirkspektrum der Bundeswehr in multinationalen Einsätzen signifikant zu erweitern.“

Zu diesem Zweck will die Bundeswehr nun verstärkt IT-Fachkräfte rekrutieren; gesucht seien aktuell „eher Nerds als Sportskanonen“, fasst es tagesschau.de (26.4.2016) zusammen. Hierfür startete die Bundeswehr im Rahmen des „Projekts Digitale Kräfte“ eine massive Rekrutierungskampagne (siehe auch IMI-Standpunkt 2016/16b), deren Details die Bundeswehr zeitgleich mit der Vorstellung des neuen Cyberkonzeptes auf einer Folie veranschaulichte: „rund 60 Kampagnentage“; „Mitte März Plakate-Kampagnenauftakt im CeBIT-Umfeld“; „3 verschiedene Sprüchemotive (unter dem Aspekt ‚Sinnstiftung‘)“; „ 5 IT-Berufswelt-Botschafter/Botschafterinnen (unter dem Aspekt ‚Qualifizierung‘)“; „Anzeigen in 25 Printtiteln“; „knapp 18.000 Plakat-Flächen“; „45 Online-Banner“; „YouTube- und Facebook-Einsatz über die gesamte Kampagnenlaufzeit“; „Kosten 3,6 Mio. Euro“.

„Cyber-Gedöns“

Logo des Chaos Computer Club. Quelle: Wikipedia

Die Bundeswehr rüstet sich ganz offensichtlich für den Kampf um den Cyber- und Informationsraum. Scharf geht deshalb u.a. Frank Rieger vom Chaos Computer Club auf „Internationale Politik und Gesellschaft“ (2.5.2016) mit den Plänen des Verteidigungsministeriums ins Gericht: „Der Versuch, das Feld zu militarisieren und zu ‚vergeheimdienstlichen‘ geht am Kern des Problems vorbei: schlechte Software, mangelnde Ausbildung und fehlende Haftungsregeln für Unternehmen. Zu glauben, man könne hier mit militärischen Mitteln irgendetwas anderes als eine Eskalation bewirken, ist naiv. Die Lage fasste ein Bundeswehr-General mir gegenüber auf einer Veranstaltung treffend zusammen: ‚Solange ich über das Bundeswehr-Logistiksystem nicht einmal zuverlässig Toilettenpapier bestellen kann, brauche ich auch kein Cyber-Gedöns.‘“

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen