Thomas Reinhold

Die Bundeswehr zieht ins Cyberfeld

Nun ist offiziell, was sich bereits seit einem Jahr in der Diskussion zum neuen „Weißbuch" der Bundeswehr abgezeichnet hat: Die Truppe soll künftig einen Organisationsbereich „Cyber und Informationsraum" erhalten, der Heer, Marine und Luftwaffe sowie dem Sanitätsdienst gleichgestellt ist. Dieser soll 13700 Stellen umfassen, wobei etwa 12800 bereits bestehende Dienstposten dem Cyberbereich zugewiesen werden, so sehen es die Konzepte des Aufbaustabs vor.

Damit folgt die Bundesregierung einem internationalen Trend, den Cyberspace als weitere militärische Domäne zu begreifen. Die Nato stellt seit Mitte Juni Cyberattacken auf eine Stufe mit konventionellen militärischen Aggressionen. Das heißt auch: Angriffe über Datennetze könnten künftig den Bündnisfall auslösen.

Einem Bericht des United Nations Institute for Disarmament Research (UNIDIR) von 2013 zufolge betreiben mindestens 47 Staaten nominell militärische Cyber-Programme, darunter zehn Staaten mit einer explizit offensiven Ausrichtung.[1] Daher sieht der Aufbaustab das Wirken der Bundeswehr im Cyberspace als entscheidenden militärischen Entwicklungssprung und bezeichnet ihn in seinem Abschlussbericht sogar als nächsten Schritt nach der Entwicklung des Panzers und der Nuklearwaffen. Denn die IT sei ein zentraler Bestandteil moderner Gesellschaften, deren Sicherung in den vergangenen Jahren zu wenig Aufmerksamkeit erfahren habe. Zudem berichten Medien häufig von schwerwiegenden Cybervorfällen mit hohem wirtschaftlichem Schaden.

IT als militärische Schlüsseltechnologie

Tatsächlich ist es sinnvoll, bei der Bundeswehr die Beschaffung und Entwicklung der IT-Ausrüstung zu optimieren, da gerade diese Technologie nach wie vor von einer enormen Dynamik geprägt ist. Computer und Software veralten innerhalb weniger Jahre, werden inkompatibel, leistungsschwach oder genügen nicht mehr den Herausforderungen durch neue Entwicklungen, wie dem *Internet of things*, der Omnipräsenz mobiler Endgeräte oder der virtuellen Realität. Für die beschleunigte und kontinuierliche Modernisierung der Bundeswehr ist eine zentral geführte, zeitnah kontrollierte und an den aktuellen Erfordernissen ausgerichtete (sogenannte agile) Projektsteuerung mit Hilfsmitteln und Werkzeugen, wie sie in der IT-Wirtschaft und im zivilen Leben üblich sind, daher ein wichtiger Schritt.

Entscheidend ist zudem, dass IT-Personalangelegenheiten künftig zentral im Verteidigungsministerium verwaltet werden. Denn IT-Fachkräfte werden auf dem freien Markt, der nicht an feste und einheitliche Tarifvereinbarungen gebunden ist, schwer umworben. So sollen in den nächsten Jahren zum einen Wege aus der freien Wirtschaft und in sie zurück geebnet werden sowie Möglichkeiten für unkonventionelle Karrierewege bei der Bundeswehr geschaffen werden, um Fachpersonal zu akquirieren und zu halten. Zum anderen wird verstärkt auf die

1 Vgl. UNIDIR, The Cyber Index – International Security Trends and Realities, Genf 2013.

massive Förderung von IT an den Ausbildungseinrichtungen der Bundeswehr gesetzt.[2]

Diese Maßnahmen werden sich jedoch erst in einigen Jahren in höheren Abschlussquoten niederschlagen. Angesichts der aktuellen Personalstärken wird der neue Cyberbereich vor seinem Start im April 2017 daher wohl in erster Linie verstärkt Ressourcen und Know-how aus der Wirtschaft einkaufen. Das liegt auf der Linie der im letzten Jahr verkündeten Strategie des Verteidigungsministeriums, die eine Stärkung des wehrtechnischen Mittelstandes vorsieht und IT zur nationalen militärischen Schlüsseltechnologie und „wesentliche[n] Säule für die Zukunftsfähigkeit der Bundeswehr im Cyber- und Informationsraum" erklärt.

Die Hacker der Bundeswehr

Gegenüber den schlüssig konzipierten Anpassungen im Verteidigungsministerium erscheinen die Änderungen bei der Bundeswehr angesichts ihrer unklaren strategischen Ausrichtung im Cyberspace zweifelhaft. Ein Großteil ihrer IT-Fähigkeiten ist derzeit in der als Dienstleistungsbereich angelegten Streitkräftebasis zusammengeführt, die das zentrale IT-Betriebszentrum der Bundeswehr und der Führungsunterstützungssysteme betreibt, aber auch den militärischen Nachrichtendienst und die Einheiten der strategischen Aufklärung umfasst. Zusätzlich sind auch in den anderen Teilbereichen der Bundeswehr IT-Fachkräfte vertreten, die für den Betrieb, die Wartung und die Weiterentwicklung der Technik benötigt werden.

Ein in den vergangenen Jahren besonders in den Fokus gerückter Teil der Streitkräftebasis ist die seit 2006 bestehende Einheit „Computer Network Operations" (CNO), die mit etwa 60 Dienstposten den offensiven Zugriff auf fremde IT-Systeme trainiert, wenn auch aktuell nur in abgeschlossenen Übungsnetzwerken. Über diese bislang einzige potentiell militärisch offensiv wirkende Bundeswehr-Cyber-Einheit sind nur wenige Details bekannt. Obgleich das Ministerium immer wieder betont, dass selbstverständlich auch Cyber-Einsätze zuvor vom Parlament gebilligt werden müssen, ist es bisher eine genaue Erklärung schuldig geblieben, wozu eine militärische Hacker-Truppe denn strategisch vorgesehen ist. Besonders unklar ist, wie diese effektiv eingesetzt werden soll, wenn sie formal erst nach einer öffentlichen Erlaubnis durch den Bundestag damit beginnen darf, fremde IT-Netze auszuspähen und in diese einzudringen.

Anders formuliert: Wenn die Bundeswehr auch im Cyberspace offensiv agieren will, wer übernimmt dann die im Vorfeld notwendige weitreichende Aufklärung potentieller Ziele? Welche verdeckten Kooperationen mit Nachrichtendiensten sind dafür möglicherweise vorgesehen und wo sieht die Bundesregierung die Grenze zwischen Aufklärung und der völkerrechtlich weit schwerwiegenderen Manipulation eines IT-Systems zum Zwecke der Datenspionage?

Technisch ist diese Grenze kaum abzustecken und ihre Einhaltung lässt sich mit Blick auf die potentiell unabwägbaren Konsequenzen eines unautorisierten Zugriffs auf fremde IT-Systeme nur schwer garantieren. Trotz dieser Unklarheiten betont man jedoch die Notwendigkeit, in fremde Netze einzudringen. Daher wird die CNO-Einheit 2017 um 20 Dienstposten aufgestockt und danach weiter ausgebaut. Überdies hat die Bundesregierung bislang nicht geklärt, wie es um einen Einsatz der Bundeswehr zur Cyber-Verteidigung im Inneren bestellt ist und wie mit der problematischen Verzahnung von Nachrichtendiensten und militärischen Einrichtungen oder der zwei-

2 Vgl. Bundesministerium der Verteidigung, Abschlussbericht Aufbaustab Cyber- und Informationsraum, Berlin 2016.

felhaften außenpolitischen Wirkung einer solchen strategischen Zusammenarbeit umgegangen werden soll.

Was sind Cyberwaffen?

Bei alledem kommt insbesondere dem Umgang mit Cyberattacken eine zunehmende außen- und sicherheitspolitische Rolle zu: Über Monate hinweg konnten Eindringlinge im vergangenen Jahr auf das interne Kommunikationssystem des Deutschen Bundestags zugreifen. Vermutlich entwendeten sie über den gesamten Zeitraum interne Daten wie E-Mails, elektronische Dokumente und Zugangsdaten von Bundestagsabgeordneten und deren Mitarbeitern. Dies sorgte zwar für große Aufregung, allerdings anscheinend für keinerlei nach außen gerichtete Reaktion der Bundesregierung.[3]

Im Gegensatz dazu wurde in den USA Ende 2014 der Datendiebstahl bei einer Sony-Tochterfirma trotz völlig unklarer Faktenlage zum Anlass für nahezu unmittelbare Sanktionen gegen nordkoreanische Unternehmen und Einzelpersonen genommen.[4] Der nun geplante zentral geführte militärische Cyberbereich der Bundeswehr scheint sich stark am US-amerikanischen Vorbild zu orientieren, er soll einen Chief Information Officer als nationalen und internationalen Ansprechpartner erhalten. Mit dem US-Cybercommand gibt es dort schon lange eine explizit offensive Cyber-Einheit, die unter Leitung des jeweils amtierenden Direktors der National Security Agency (NSA) steht.

Auch für die Nato gilt Cyber schon seit dem Ministertreffen in Wales 2014[5] als elementarer Bestandteil der strategischen Planungen, und Partnerstaaten haben einen „substanziellen Beitrag zu einem multinationalen Command Element“[6] zu leisten. Während einige Strategen Cyberattacken bereits auf eine Ebene mit konventionellen Waffen heben und sich auch die Option nuklearer Verteidigung vorbehalten wollen, sind Cyberwaffen für andere eine neue, zielgenaue und gering-invasive Möglichkeit der Konfliktaustragung ohne eigene Verluste.

Diese Entwicklungen ignorieren jedoch vollkommen, dass international gegenwärtig keinerlei Einigkeit herrscht, was Cyberwaffen eigentlich sind und wie militärische Angriffe über den Cyberspace völkerrechtlich zu bewerten sind. Selbst in der Frage nach Grenzen und nationaler Souveränität im Cyberspace gibt es fundamental unterschiedliche Sichtweisen.[7] Das vom Nato-Exzellenz-Zentrum Cooperative Cyber Defence Centre of Excellence (CCDCOE) erarbeitete Tallinn-Manual wagt einen ersten Vorstoß, indem es etablierte Regeln der internationalen Sicherheit auf den Cyberspace überträgt und anwendet. Ähnliche Fragen werden von Expertengruppen der UNO sowie der OSZE diskutiert.

Dabei werfen die spezifischen Gegebenheiten des Cyberspace einige Komplikationen auf: Zum einen muss laut Artikel 51 der UN-Charta ein Angriff erfolgt sein, um das Recht auf nationale Selbstverteidigung geltend machen zu können. Cyberattacken aber lassen sich leicht verschleiern und sind daher nur äußerst aufwendig und zeitintensiv nachzuverfolgen. Eng damit verbunden ist die Frage, welcher Grad und Umfang einer Cyberattacke einem bewaffneten Angriff gleichkommt.

Die vom Tallinn Manual vorgeschlagene Analogie zu Angriffen mit konventionellen Waffen hilft hier nur be-

3 Vgl. Parlakom Hack, www.cyber-peace.org.
4 Vgl. Sony-Pictures-Entertainment-Hack, www.cyber-peace.org.
5 Vgl. Nato, Wales Summit Declaration, 5.9.2014.
6 Vgl. Abschlussbericht Aufbaustab Cyber- und Informationsraum, a.a.O.
7 Vgl. das 2015 von Russland und China vorgeschlagene „Agreement between the Government of the Russian federation and the Government of the People's Republic of China on cooperation in ensuring international information security“, inoffizielle englische Übersetzung auf www.cyber-peace.org.

dingt weiter, da Cyberattacken relevante Beeinträchtigungen anrichten können, ohne dabei konkrete Schäden an Menschen oder Objekten zu verursachen – etwa durch die Störung eines nationalen Bankensystems oder die Manipulation der Stromversorgung. Darüber hinaus bergen Cyberattacken stets das Risiko der ungewollten Beeinträchtigung dritter, ursprünglich nicht zum Ziel gehörender IT-Systeme, wodurch kritische zivile Infrastrukturen geschädigt werden könnten – unter Umständen auch jene unbeteiligter Nationen.

Rüstungskontrolle im Cyberspace

Cyberwaffen werfen aber auch neue Probleme auf, wenn es um international stabilisierende Maßnahmen zur Einhegung militärisch aggressiver Potentiale geht wie die Rüstungs- und Nonproliferationskontrolle. Ein Großteil der klassischen Konzepte solcher Vereinbarungen, die auf einer territorialen Verortung von Waffen oder dem materiellen Umfang von Kriegsmaterial basieren, versagt angesichts der Virtualität und der potentiell beliebigen Kopierbarkeit von Software. Auch die bei der IT-Sicherheit problematische Abgrenzung zwischen gerechtfertigten Verteidigungsmaßnahmen und dem damit einhergehenden Angriffs-Know-how spielt mit Blick auf die außenpolitische Wirkung militärischer Cybermaßnahmen eine entscheidende Rolle.

Vor diesem Hintergrund wäre die Bundesregierung gut beraten, weniger auf den Aufbau militärischer Cyberwaffen zu setzen als vielmehr auf die Stärkung vertrauensbildender Maßnahmen für den Cyberspace – beispielsweise durch eine weitere internationale Vernetzung zur Frühwarnung und Bekämpfung von kritischen Cybervorfällen. In Deutschland dient dazu bislang das Bundesamt für Sicherheit und Informationstechnik (BSI) als oberste Koordinationsinstanz und zentraler Ansprechpartner für ausländische Partner. Statt die Cyber-Sicherheit zu militarisieren, sollte das BSI gestärkt und unter dem Aspekt der Vertrauensbildung von dem fatalen Verdacht befreit werden, Verbindung zu Nachrichtendiensten und Militärs zu unterhalten.

Die Bundesregierung könnte einen entscheidenden Beitrag leisten, indem sie ein klares Bekenntnis zur ausschließlich defensiven Ausrichtung ihrer Cyber-Einheiten abgibt. Aber auch die Informatik ist in ihrer Rolle als Gestalterin der Technologie und der Möglichkeiten von morgen gefragt. Sie könnte beispielsweise einiges zur Behebung der technischen Probleme bei der Rüstungskontrolle beitragen. Beides ist in erster Linie eine Frage des politischen und wissenschaftlichen Willens. Schließlich ist der Cyberspace gerade in der Hinsicht einzigartig, dass er vollständig vom Menschen kontrolliert wird. Daher kann der Mensch ihn auch jederzeit ändern.