

Alle Freiheit im Cyberraum

Bundeswehr startet dritte Stufe ihrer Werbekampagne. Neue Truppengattung mit über 13.000 Soldaten soll Onlinekrieg führen. **Von Jörg Kronauer**

Seit Dienstag ist es offiziell: Die Bundeswehr bekommt eine neue Truppengattung für den Cyberkrieg. »Cyber- und Informationsraum«, kurz: CIR, nennt sich die neue Teilstreitkraft, die in Zukunft den Kampf im World Wide Web führen soll, also – wie Militärs es ausdrücken – in der »fünften Dimension« neben Land, See, Luft und Weltraum. 13.500 Dienstposten, ein »Zentrum für Cybersicherheit der Bundeswehr« und ein »Zentrum Cyberoperationen« wird die Cyberstreitkraft umfassen, die einem neuen Kommando in Bonn, dem Kdo CIR, untersteht. Zum 1. April 2017 soll es soweit sein: Dann wird ein neuer Inspekteur die Führung des Kdo CIR übernehmen, ganz so, wie Inspektoren jeweils an der Spitze von Heer, Marine, Luftwaffe, Streitkräftebasis und Sanitätsdienst stehen. Das Verteidigungsministerium richtet dafür an beiden Dienstsitzen, in Bonn und in Berlin, eine neue Abteilung »Cyber/IT (CIT)« ein. Im CIR sollen sämtliche bisherigen Cyberaktivitäten der Bundeswehr gebündelt werden.

Wie sieht er aus, der Krieg der Zukunft, den der CIR führen können soll? Er wird, so heißt es im zuständigen Ministerium, natürlich nur der Verteidigung dienen, also genauso defensiv sein wie alles, was die Bundeswehr schon seit Jahren am Hindukusch, am Horn von Afrika oder in Mali treibt. Cyberverteidigung ist, glaubt man der Bundeswehr, dringend nötig: Allein im vergangenen Jahr habe es in der Bundeswehr 7.200 »Infektionen mit Schadsoftware« gegeben, außerdem eine hohe zweistellige Zahl »ambitionierter« Hackerangriffe; darüber hinaus habe man täglich im Durchschnitt 6.500 leichte Attacken auf die IT-Netze des Bundes insgesamt registriert. Braucht man, um all das abzuwehren, denn aber wirklich eine 13.500 Mann starke Truppe von IT-Soldaten? Nun, es geht natürlich nicht nur um die Abwehr von Hacker-

angriffen: Bei Bedarf soll der CIR auch »offensiv verteidigen« können, also zu Cyberangriffen in der Lage sein.

Mit der Option, auch Angriffe zu führen, begibt die Bundeswehr sich auf ein besonders heikles Terrain. Der bekannteste bisherige Fall ist der Angriff auf die iranischen Zentrifugen gewesen, die laut Auffassung der westlichen Mächte dem Bau von Atomwaffen dienen. Die Zentrifugen wurden dabei weitgehend zerstört; solche Attacken können physische Folgen haben wie jeder andere militärische Angriff auch. Kann aber eine Truppe, die derlei Manöver in den verborgenen Weiten des Cyberraums führt, noch zuverlässig demokratisch kontrolliert werden? Aber natürlich, bekräftigt das Verteidigungsministerium: Man werde vor jeder Maßnahme

einen Parlamentsbeschluss einholen. Regierungsberater sind da weniger optimistisch. Glaubt man der Stiftung Wissenschaft und Politik (SWP), dann bestehen sogar in der Truppe erhebliche Zweifel. »Selbst in der Bundeswehr« gebe es »Befürchtungen«, dass der CIR »eine ähnliche Entwicklung nehmen könnte wie das United States Cyber Command«, warnte die SWP im März: »Dieses ist keinerlei parlamentarischer Kontrolle unterworfen und arbeitet eng mit der NSA zusammen. Es besteht die Sorge«, fuhr der Thinktank fort, der CIR sei womöglich »nicht mit dem traditionellen Verständnis vom »Bürger in Uniform« in Einklang zu bringen«.

Unwägbar Gefahren gibt es beim Cyberkrieg zuhauf. Man könne Ziele im Internet kaum mit der notwendigen Prä-

zision attackieren, warnte ein Sprecher des Chaos Computer Clubs schon im Juli: »Tatsächlich besitzen digitale Angriffe den Charakter von Streubomben« – sie stellen »ein hohes Risiko für weite Bereiche der Zivilbevölkerung dar«. Jede Attacke provoziere Gegenschläge, die gleichfalls »schwerwiegende unbeabsichtigte Schäden verursachen« könnten, warnt auch die SWP.

Die Bundeswehr schlägt sich derweil mit eher praktischen Problemen herum. Eines der größeren besteht darin, dass man für den Cyberkrieg hochqualifizierte Hacker braucht. Im März hat sie unter dem Titel »Projekt Digitale Kräfte« die dritte Stufe dieser Kampagne gestartet: »Deutschlands Freiheit wird auch im Cyberraum verteidigt«, behauptet sie nun.



Krieg in »Neuland«: Ursula von der Leyen (CDU) entdeckt das Internet im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr in Euskirchen (Nordrhein-Westfalen), 17. Juli 2015