Bereit für den Cyberkrieg

Weser-Kurier, 23.08.19

bzeichen des neuen Kommandos Cyber- und Informationsraum ist in Bonn beim Dienstappell an einem Barett zu sehen.

FOTO: INA FASSBENDER/DPA

VON NORBERT HOLST

Bremen. Es war der bislang schwerste Cyberangriff mit politischem Hintergrund in Deutschland: Im Januar 2015 drangen Hacker in das Netz des Bundestags ein. Es folgten Angriffswellen gegen zahlreiche Parlamentarier, darunter auch das Abgeordnetenbüro von Bundeskanzlerin Angela Merkel. Mithilfe eines sogenannten Trojaners konnten die Angreifer rund 16 Gigabyte an Daten abzweigen, teilweise fielen sensible Dokumente und vertrauliche Mails in ihre Hände.

Es waren offenbar Profis am Werk: Mehrere Wochen brauchten die Experten des Bundesamtes für Sicherheit in der Informationstechnik (BSI), um die Angriffe zu stoppen. Die Attacke wurde sogar zu einem Fall für den Generalbundesanwalt. Doch die Täter wurden bis heute nicht entdeckt. Manche Experten sehen aber starke Indizien, dass der russische Geheimdienst GRU und eine Hackergruppe namens „ATP 28" hinter dem Angriff standen. „ATP 28" soll auch hinter Cyberangriffen auf die Verteidigungsministerien von mehreren Nato-Ländern und europäischen Rüstungsunternehmen stecken.

Die Hackerangriffe von 2015 hätten die Bemühungen der Bundeswehr erheblich forciert, ein eigenes „IT-Kommando" auf die Beine zu stellen, sagt Oberst a. D. Jürgen Schick. Er referierte im Schütting auf Einladung der Bremer Sektion der Gesellschaft für Sicherheitspolitik. „Im Moment sind wir noch in der Krabbelphase", beschreibt Schick die Fortschritte beim Aufbau des neuen Organisationsbereichs Cyber- und Informationsraum (CIR), für den er selbst bis vor Kurzem tätig war.

Im April 2017 ist das CIR-Kommando von der damaligen Verteidigungsministerin Ursula von der Leyen offiziell in Dienst gestellt worden und ist seitdem eine Teilstreitkraft wie etwa Heer und Marine – mit 13 000 Männern und Frauen. Nun ist es aber keineswegs so, dass die Bundeswehr damit 13 000 Hacker hat. Im CIM sind vielmehr verschiedene Bereiche zusammengeführt worden: Fernmelde-elektronische Aufklärung, militärisches Nachrichtenwesen, IT-Unterstützung, Geoinformationswesen, operative Kommuni-

kation. Know-how und Erkenntnisse dieser in ganz Deutschland verstreuten Dienststellen sollen im Gemeinsamen Lagezentrum des CIR zusammenlaufen. Das Ziel: Immer wieder aufs Neue die Sicherheitslage zu beurteilen. „Das ist das Herz des Kommandos", erläutert Schick. Das soll auch mithilfe von modernster Technologie wie künstlicher Intelligenz und Big Data passieren. „Aber da stehen wir erst am Anfang", gibt der Oberst zu. Erst in zwei Jahren soll der Aufbau des CIR beendet sein.

Schick hält den eingeschlagenen Weg für richtig beziehungsweise alternativlos. „Vor elf, zwölf Jahren war die IT der Bundeswehr total veraltet", erzählt er. Tatsächlich haben die Militärs die neuen Gefahren aus dem Netz erst relativ spät erkannt – das gilt selbst für Länder wie Großbritannien und die USA. Letzteres überrascht besonders, weil die „Erfindung" des Internets auch vom Pentagon kräftig gefördert wurde.

Oberst a. D. Schick. FOTO: KUHAUPT

Gegenwärtig soll es rund 30 Länder geben, die im Cyberbereich massiv aufrüsten. Doch wie muss man sich den Krieg der Zukunft vorstellen? Ein Beispiel für einen erfolgreichen Angriff: 2007 wurden in Estland verschiedene Regierungsstellen lahmgelegt, auch die größte Bank des Landes war nicht mehr erreichbar. Vermutlicher Hintergrund: Es gab zu jener Zeit erhebliche Spannungen zwischen Estland und dem Nachbarn Russland.

Internationales Aufsehen erregte 2010 der Internetwurm „Stuxnet". Das Schadprogramm sollte das iranische Atomprogramm sabotieren. Tatsächlich hat die Attacke wohl größere Schäden angerichtet. Wer hinter dem Sabotageversuch steckte, ist nicht bekannt. Verdächtigt wurden die USA und Israel. Zumal es als sicher gilt, dass nur ein schlagkräftiger Geheimdienst den hochkomplexen Angriff organisiert haben kann. Ein Merkmal der neuen Art der Kriegsführung: Er kennt nur Ziele, keine Täter.

In Fachkreisen gelten auch digitale Angriffe gegen die Infrastruktur eines Landes, wie im Fall von „Stuxnet", als Cyberkrieg. Eine noch weitere Auslegung des Begriffs beinhaltet auch Fake News und Desinformation via Internet, die eine Gesellschaft beeinflussen oder destabilisieren sollen. Ein solcher Fall ist etwa die mutmaßliche Einflussnahme Russlands auf die US-Präsidentschaftswahl vor drei Jahren.

Für Schick ist die Digitalisierung ein „Game Changer", der die militärischen Herausforderungen „total verändert" habe. So könnte eine Kriegsführung in Zukunft immer virtueller werden: „Wo ist die Front?" Es werde auch eine zunehmende Distanz zwischen den Akteuren eines Konflikts geben. „Das Schlachtfeld wird immer leerer", glaubt der Oberst. Und auch die Zunft der Ethiker sei gefragt. Denn im Gegensatz zum konventionellen Krieg gibt es für Auseinandersetzungen im virtuellen Raum keine Art Genfer Konvention. „Darf man nach einem Angriff aus Nordkorea den Hauptspeicher zerschießen?", fragt Schick in die Runde. Die Bundeswehr als Hacker? Der Redner gibt die Antwort selbst: „Das ist rechtlich im Moment noch nicht klar." Andererseits gilt besonders für den Cyberkrieg: Angreifen ist leichter als verteidigen.