Sputnik Deutschland

Der Cyberkrieg bedroht alle – Digitale Rüstungskontrolle statt Aufrüstung gefordert

05.04.2017 (aktualisiert 14:18 06.04.2017)

Die digitale Aufrüstung der konventionellen Armeen bedroht nicht nur IT-Systeme ganzer Staaten, sondern auch die Zivilbevölkerung, wenn zivile Versorgungssysteme getroffen werden. Davor haben am 30. März in Berlin zwei Experten in einer Diskussionsrunde zum Thema Cyberkrieg gewarnt. Sie fordern u.a. völkerrechtliche Grenzen für digitale Waffen.

© AFP 2017/ Gregor Fischer

Die Bundeswehr eröffnet „praktisch ein fünftes Schlachtfeld", indem sie eine komplette digitale Kampfgruppe mit geplant fast 14.000 „Cybersoldaten" aufstellt. Darauf wies am 30. März Rolf Gössner hin. Er ist Rechtsanwalt und Vorstandsmitglied der Internationalen Liga für Menschenrechte und diskutierte in Berlin mit dem Informatiker und Datenschutzexperten Rainer Rehak über das Thema „Aufrüstung zum Cyberkrieg – aktuelle Entwicklung und Gegenentwurf". Dazu hatten das Berliner Haus der Demokratie und Menschenrechte, die Internationale Liga für Menschenrechte, die Humanistische Union und die Redaktion der Zeitschrift Ossietzky gemeinsam eingeladen.

„Mit dieser digitalen Aufrüstung wird neben Land, Luft, Wasser und Weltraum der Cyberraum beziehungsweise das Internet zum potentialen Kriegsgebiet erklärt", betonte Gössner. „Damit beteiligt sich die Bundesrepublik am globalen digitalen Wettrüsten und zwar bislang weitgehend ohne parlamentarische Beteiligung, ohne demokratische Kontrolle und ohne rechtliche Grundlagen."

Die deutschen Cyber-Soldaten sollen den Informationen zufolge nicht nur Attacken von außen abwehren, sondern auch zu eigenen Cyberangriffen auf andere Staaten und deren IT-Infrastruktur befähigt werden. „Im Klartext heißt das also, zum Führen von Cyberkriegen im In- und Ausland", so der Jurist. So sehe es die geheime strategische Leitlinie Cyberverteidigung des Bundesverteidigungsministeriums vor. Auch im neuen Weißbuch zur Sicherheitspolitik 2016 spiele der Krieg im Cyberraum eine „ganz gewichtige Rolle".

Digitale Waffen bedrohen Zivilbevölkerung

Gössner beschrieb, wie das genau aussehen soll: „Die Bundeswehr soll eigene Cyberwaffen entwickeln, um getarnt auch in fremde IT-Systeme einbrechen und diese über Sicherheitslücken, Trojaner, Viren und so weiter ausspähen, manipulieren, fehlsteuern, lahmlegen, schädigen oder zerstören zu können." Er warnte zugleich: „Digitale Waffen sind in einer vernetzten Welt keine Präzisionswaffen und die Streuung, die kann immens sein – und zwar mit gravierenden Folgen für die Zivilbevölkerung, wenn die Gegenangriffe etwa zu lang andauernden Ausfällen der Strom- und Wasserversorgung oder des Krankenhaus-, Gesundheits- oder Verkehrswesens führen."

Rainer Rehak, Datenschutzexperte vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), machte darauf aufmerksam, dass die Spuren digitaler Waffen „sehr viel geringer" und „sehr viel uneindeutiger" seien. „Das heißt, Spuren sind meistens auch kopierbar und man kann da auch sehr viel einfacher falsche Fährten legen." Der Informatiker nannte als Beispiele dafür Hackerangriffe auf den Bundestag und entsprechende Informationen aus dem US-Wahlkampf 2016. Das ließe sich „immer sehr schön politisch ausschlachten, weil es eben nicht ganz klar ist, wo die herkommen". Er beobachte das seit längerer Zeit und habe Standardantworten zur Frage der mutmaßlichen Täter gefunden: „Bis vor ein paar Jahren waren es immer die Chinesen und jetzt seit kurzer Zeit ist es immer Russland."

Vorwürfe gegen Russland ohne sichere Beweise

Doch bislang seien alle diese Vorwürfe „unfundiert" gewesen, erklärte Rehak. Die zu den mutmaßlichen Hackerangriffen veröffentlichten Studien zum Beispiel von amerikanischen Geheimdiensten hätten „meistens sehr dünne Beweisböden, die sehr schnell dekonstruiert werden können". „Das heißt nicht, dass doch die Chinesen oder die Russen als Urheber da zu nennen sind", erläuterte der Informatiker, „aber eine Argumentation müsste anders laufen". Es sei aber „sehr problematisch, da von Gewissheiten auszugehen."

Der IT-Experte beschrieb den Cyberkrieg, den Cyberwar, als Angriff auf IT-Sicherheitslücken anderer zu eigenen Zwecken, die entweder direkt oder strategisch sind. Es werde so dafür gesorgt, „dass IT-Systeme nicht das tun, was sie tun sollen, sondern den eigenen Zwecken folgen". Rehak sprach von „Sabotage informationstechnischer Systeme aus der Ferne". Er machte auf das 2013 vorgestellte „Tallinn Manual" aufmerksam, einer Studie im Auftrag der Nato, die „als inoffizielle Doktrin bei Cyberkriegen" gelte.

„Seit einigen Jahren ist es also so, dass laut ‚Tallinn Manual' Cyberangriffe gleichwertig mit physischem Angriff gewertet werden sollen. Das ist nicht offizielle Position, aber es wird als Handlungsoption gehandelt. Es hieße dann aber auch, dass bei Cyberangriffen dann zum Beispiel der Bündnisfall ausgerufen werden könnte, wo dann konkrete physische Rückantworten militärische Natur kommen könnten." Der Informatiker warnte davor, dass so die Gefahr von willkürlichen Reaktionen bestünde.

CIA kann eigene Hackangriffe mit fremden Spuren versehen

Für ihn war bei den jüngsten Wikileaks-Enthüllungen über das Cyberspionageprogramm „Vault7" der CIA interessant, dass der US-Geheimdienst „selber einen Quasi-Werkzeugkasten hat, mit den Eigenschaften verschiedener Hackergruppen und verschiedener Länder". So könne ein eigener Hackerangriff so mit Spuren versehen werden, die auf andere angebliche Quellen dafür ablenken. Diese Enthüllungen beschrieb Rehak so: „Als würde man bei einem Kriminellen in den Schrank schauen und da sieht man dann die ganzen Verkleidungen liegen. Ich habe keinen Zweifel daran, dass zum Beispiel Russland oder China das genauso tun, nur wissen wir hier von mehr. Gerade durch so jemanden wie Edward Snowden, aber auch Jesselyn Radack, Thomas Drake und so weiter. Es gibt einfach mehr Whistleblower an dieser Stelle, deswegen können wir das belegen."

Rechtsanwalt Gössner benannte als kritischen Punkt, dass bisher kein internationales Abkommen die Aufrüstung im Cyberspace reguliert und kontrolliert. Klar sei aber: „Völkerrecht und Menschenrechte gelten auch hier. Also auch das völkerrechtliche Gewaltverbot zum einen und das Recht zur angemessenen militärischen Selbstverteidigung zum anderen." Er fordert unter anderem „eine Art Genfer Konvention für die Cyberwelt". Schwachstellen in IT-Systemen müssten ausfindig gemacht und geschlossen werden und dürften nicht für Cyberangriffe oder —Spionage ausgenutzt werden. Der Jurist sprach sich dafür aus, nur rein defensive militärische Cybermaßnahmen zuzulassen und strikt zu verbieten, dass auf Cyberattacken mit konventionellen Angriffen reagiert wird. Zudem hält er die Cyberrüstungskontrolle ebenso für notwendig wie die internationale Ächtung von Cyberwaffen. Doch er zeigte sich skeptisch: „Leider kann man schon seit längerem eine verhängnisvolle Aufweichung des Völkerrechts beobachten, auch und gerade von Seiten des Westens."

Bolle Selke