Grundrechte-Report 2018 – Zur Lage der Bürger- und Menschenrechte in Deutschland.
Herausgeber: Till Müller-Heidelberg, Marei Pelzer, Martin Heiming, Cara Röhner, Rolf Gössner, Matthias Fahrner, Helmut Pollähne und Maria Seitz. Fischer Taschenbuch Verlag, Frankfurt/M., Juni 2018, ISBN 978-3-596-70189-6, 240 Seiten, 10.99 Euro.

Der Grundrechte-Report 2018 ist ein gemeinsames Projekt von:
Humanistischer Union, vereinigt mit der Gustav Heinemann-Initiative • Bundesarbeitskreis Kritischer Juragruppen • Internationale Liga für Menschenrechte • Komitee für Grundrechte und Demokratie • Neue Richtervereinigung • PRO ASYL • Republikanischer Anwältinnen- und Anwälteverein • Vereinigung Demokratischer Juristinnen und Juristen

Rolf Gössner

„Deutschlands Freiheit wird auch im Cyberraum verteidigt“

Aufrüstung der Bundeswehr zum „Cyberkrieg“

Die Bundeswehr ist 2017 mit einem neuen „*Kommando Cyber- und Informationsraum“* aufgerüstet worden. Mit dieser digitalen Kampftruppe mit (geplant) etwa 15.000 Dienstposten beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – ohne Parlamentsbeteiligung, demokratische Kontrolle und gesetzliche Grundlagen.

Schon bisher existierte eine geheim agierende IT-Einheit für operative Maßnahmen in Rheinbach bei Bonn (*„Computer Netzwerk Operationen“*) mit etwa 70/80 Soldaten. Sie wird nun mit weiteren IT-Einheiten der Bundeswehr, so dem *Kommando Strategische Aufklärung*, im neuen *„Cyber-Kommando“* zentralisiert. Mithilfe großer Werbekampagnen (*„Deutschlands Freiheit wird auch im Cyberraum verteidigt“)* versucht die Bundeswehr händeringend, externe IT-Fachleute anzuheuern.

Mit dieser digitalen Aufrüstung wird – neben Land, Luft, Wasser und Weltraum – ein fünftes Schlachtfeld, das „Schlachtfeld der Zukunft“, eröffnet und der Cyberraum – also auch das Internet – zum potentiellen Kriegsgebiet erklärt.

Zielvorgabe: Verteidigung – inklusive Befähigung zu Cyber-Angriffen

Sicher ist es legitim, wenn die Bundeswehr geeignete Schutzmaßnahmen ergreift, um sich gegen Cyberattacken aller Art, etwa kriminelle Hackerangriffe nicht staatlicher Akteure, zu verteidigen, die gegen ihre eigene, höchst verwundbare Militär-IT gerichtet sind – angeblich Zigtausende pro Tag. Doch das Verteidigungsministerium gibt sich damit nicht zufrieden, sondern erhebt den Anspruch auf „gesamtstaatliche Sicherheitsvorsorge“. Also auch auf die verfassungsrechtlich fragwürdige (militärische) Abwehr von Cyber-Angriffen auf andere staatliche, kommunale und zivile Netzwerke im Innern des Landes - für die in Friedenszeiten jedoch nicht das Militär, sondern ausschließlich Polizei, Geheimdienste und Justiz zuständig sind sowie speziell das *Bundesamt für Sicherheit in der Informationstechnik* und das *Nationale Cyber-Abwehrzentrum*.

Doch es kommt noch härter: Denn die Bundeswehr soll mit ihrer verharmlosend *„Cyber- und Informationsraum“* genannten Kampftruppe nicht nur Cyberattacken abwehren können, sondern auch zu eigenen Cyberangriffen auf andere Staaten und deren IT-Systeme befähigt werden. So sehen es die geheime *„Strategische Leitlinie Cyber-Verteidigung“* und das *„Weißbuch 2016“* des Verteidigungsministeriums vor. Im Klartext: Die Bundeswehr entwickelt Cyberwaffen und –kapazitäten, um in fremde IT-Systeme eindringen und diese ausforschen zu können; darüber hinaus wird sie zu militärischen Cyberangriffen auf Infrastrukturen anderer Staaten befähigt, um diese manipulieren, lahmlegen oder zerstören zu können – mit möglicherweise großem physischen Schadens- und Verletzungspotential, vergleichbar dem konventioneller Waffen. Bei derartigen militärischen Cyber-Angriffen auf die IT-Struktur eines anderen Staates handelt es sich um Cyberkriegshandlungen bzw. „Cyberkrieg“ im engeren Sinne.

Eine solche Offensiv-Befähigung dürfte Art. 26 Abs. 1 GG tangieren, der *„Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören, insbesondere die Führung eines Angriffskrieges vorzubereiten“,* für verfassungswidrig erklärt. Denn mit der Militarisierung des Internets und des gesamten Cyberraums werden Vorbereitungen getroffen zur Entwicklung von Cyberwaffen und zum Führen von „Cyberkriegen“ - auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen im Ausland, etwa in Afghanistan oder Mali.

Doch selbst wenn es sich „nur“ um militärische Cybergewalt zur reinen Selbstverteidigung gegen Militärattacken von außen handeln würde, wäre das zwar völkerrechtlich prinzipiell zulässig, doch schon höchst riskant. Denn von militärisch-digitalen Gegenschlägen wären nicht nur militärische Ziele wie Militär-IT und Waffensysteme betroffen, sondern – zumindest als „Kollateralschäden“ – auch kritische zivile Infrastrukturen. Schließlich sind digitale Waffen in einer vernetzten Welt keineswegs Präzisionswaffen und die Streuwirkung kann immens sein - mit lebensbedrohlichen Folgen für die Zivilbevölkerung: etwa durch lang andauernde Ausfälle der Strom- und Wasserversorgung, des Krankenhaus-, Gesundheits- oder Verkehrswesens – ein glatter Verstoß gegen das Humanitäre Völkerrecht.

Gefährliches Eskalationspotential

Zusätzlich zu solchen Auswirkungen von Cyberangriffen kommen noch weitere, kaum zu lösende Probleme und Gefahren einer Militarisierung des Internets hinzu:

Erstens besteht die Gefahr, dass es zu vorschnellen militärischen Selbstverteidigungsschlägen kommt und damit zu einer folgenschweren Eskalation - etwa aufgrund von Fehlinterpretationen bei der Frage, ob es sich bei einem Cyberangriff um kriegerische oder nichtmilitärische Attacken handelt. Derzeit ist im Völkerrecht nicht klar und verbindlich definiert, wann ein staatlicher Cyberangriff als kriegerisch zu gelten hat. NATO wie Bundeswehr behalten sich ausdrücklich vor, im Einzelfall zu entscheiden, ab wann es sich um einen solchen Angriff handelt und wie darauf reagiert wird. Warum das so ist, verrät ein Oberstleutnant im Verteidigungsministerium: *„weil wir hier auch ein Stück weit unberechenbar bleiben wollen und müssen“ (https://www.bmvg.de)*. Diese Unberechenbarkeit hinsichtlich Anlass und Art eines Gegenschlags diene auch der Abschreckung. Das grenzt jedoch an Willkür und dürfte mit völkerrechtlichen Verpflichtungen zum Schutz der Zivilbevölkerung kaum vereinbar sein!

Zweitens: Im Cyberkrieg gibt es keine Armeen, die sich gegenüberstehen und keine Soldaten in Uniform. Stattdessen kommen Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz – Software also, die keine Uniform oder Staatsabzeichen trägt. Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben. Ein militärischer Gegenschlag zur Selbstverteidigung ohne klar identifizierbaren Aggressor, also ins Blaue hinein, wäre aber völkerrechtswidrig, so der Internationale Gerichtshof.

Und drittens: Diese Probleme werden noch verschärft durch eine gefährliche Rechtsauslegung im „Tallinn Manual“, einem NATO-Handbuch zur Anwendung des internationalen Rechts auf

kriegerische Cyberangriffe (2013). An den darin aufgelisteten 95 Regeln sollen sich alle NATO-Staaten, auch die Bundeswehr, im Fall eines Cyberkriegs zumindest orientieren. Was ist daran so gefährlich? Nur zwei Beispiele:

Nach „Tallinn Manual" gelten selbst solche Operationen als Cyberkriegsangriffe, die bloße wirtschaftlich-finanzielle Schäden eines Staates verursachen, wenn diese gewisse Ausmaße annehmen - wie etwa ein Börsencrash. Dagegen wäre dann eine militärische, auch konventionelle Selbstverteidigung mit Kriegswaffen rechtens, was zu einer unkontrollierbaren Eskalation der Auseinandersetzungen führen kann.

Das Manual sieht zudem vor, dass ein Staat sein völkerrechtlich verbrieftes Recht auf angemessene Selbstverteidigung sogar präventiv ausüben darf, bevor überhaupt ein digitaler Angriff stattgefunden hat. Wie bei konventionellen Militär-Erstschlägen besteht hier hohe Missbrauchsgefahr.

Cyber-Peace statt Aufrüstung zum Cyberkrieg

Was da einflussreiche, zumeist militärnahe Völkerrechtler an Regeln zusammengestellt haben, ist geeignet, die hohen völkerrechtlichen Eingriffsschwellen für bewaffnete Gewaltanwendung zwischen Staaten weit herabzusenken, die restriktiven Kriterien des Selbstverteidigungsrechts und das völkerrechtliche Gewaltverbot aufzuweichen. So kann eine schwere Datenattacke blitzartig zu einem echten Krieg mit Raketen, Bomben und Granaten eskalieren – unter erheblicher Gefährdung von Zivilbevölkerung und internationaler Sicherheit.

All dies bedeutet: Mit der Aufrüstung zum Cyberkrieg steigen Eskalationspotentiale, Kriegsbereitschaft und Kriegsgefahr – und davor schützt auch die obligatorische Zustimmung des Bundestags zu Militäreinsätzen nur bedingt. Denn das Cyber-Konzept für die Bundeswehr wird letztlich demokratisch kaum zu kontrollieren sein.

Aus diesem Befund sind politische und rechtliche Konsequenzen zu ziehen: Keine digitale Aufrüstung der Bundeswehr zum Cyberkrieg, Verzicht auf offensive Cyberwaffen – stattdessen ausschließlich defensive Cybersicherheitsstrategie zur Selbstverteidigung, flankiert von vertrauensbildenden Maßnahmen im Rahmen einer friedensorientierten Außenpolitik und Diplomatie („Cyberpeace"). Auf internationaler Ebene: Schaffung einer Art Genfer Konventionen für die Cyberwelt, weltweite Cyberabrüstung, völkerrechtliche Ächtung von Cyberwaffen sowie Errichtung einer unabhängigen UN-Instanz zur Untersuchung zwischenstaatlicher Cyberattacken und deren angemessener Abwehr.

Literatur

Abschlussbericht Aufbaustab Cyber- und Informationsraum (2016) sowie Dossier Cyber-Verteidigung, siehe Bundesverteidigungsministerium: www.bmvg.de

(Geheime) Strategische Leitlinie Cyber-Verteidigung (2015); dok. in: Netzpolitik.org

NATO, Tallinn-Manual – Handbuch zur Anwendung des Internationalen Rechts auf die Cyberkriegsführung (Cambridge u.a. 2013); Erweiterung: „Tallin 2.0".

Gössner, Rolf, Dr. jur., Rechtsanwalt, Publizist und parlamentarischer Berater. Vorstandsmitglied der Internationalen Liga für Menschenrechte. Seit 2007 stellv. Richter am Staatsgerichtshof der Freien Hansestadt Bremen. Mithrsg. des *Grundrechte-Reports* und der Zweiwochenschrift *Ossietzky*, Mitglied der Jury zur Verleihung des Negativpreises „BigBrotherAward" sowie der Carl-von-Ossietzky-Medaille (Liga); Sachverständiger in Gesetzgebungsverfahren des Bundestages und von Landtagen. Auszeichnung mit der Theodor-Heuss-Medaille, dem Kölner Karlspreis für engagierte Publizistik und dem Bremer Kultur- und Friedenspreis. Veröffentlichungen u.a. *Menschenrechte in Zeiten des Terrors* (2007), *Geheime Informanten. V-Leute des Verfassungsschutzes: Neonazis im Dienst des Staates* (Neuauflage als ebook 2012). Herausgeber von: *Mutige Aufklärer im digitalen Zeitalter* (2015) und *Mutige Lebensretter und Aufklärer in Zeiten von Flucht und Abschottung* (2017). Internet: www.rolf-goessner.de .