BIG BROTHER AWARDS.de 2017

Video der Laudatio von Rolf Gössner unter: https://vimeo.com/216301925#t=1h25m15s

Kurzbegründung: Kategorie Behörden

Bundeswehr und Bundesministerin für Verteidigung Dr. Ursula von der Leyen

Laudator: Dr. Rolf Gössner

Bundeswehr und Bundesministerin für Verteidigung erhalten den BigBrotherAward 2017 in der Kategorie Behörden für die massive digitale Aufrüstung der Bundeswehr mit dem neuen „Kommando Cyber- und Informationsraum“ (KdoCIR). Diese digitale Kampftruppe mit (geplant) fast 14.000 Dienstkräften wird die Bundeswehr fit machen für den Cyberkrieg - auch für militärische Cyberangriffe auf IT-Systeme und kritische Infrastrukturen anderer Staaten. Mit dieser Militarisierung des Internets beteiligt sich die Bundesrepublik am globalen Cyber-Wettrüsten – ohne Parlamentsbeteiligung, ohne demokratische Kontrolle und ohne rechtliche Grundlage.

Laudatio-Langfassung:

BigBrotherAward 2017 – Behörden – Laudator: Dr. Rolf Gössner:

Der BigBrotherAward 2017 in der Kategorie Behörden geht an

die Bundeswehr und die Bundesministerin für Verteidigung,
Dr. Ursula von der Leyen (CDU), als deren Oberbefehlshaberin.

Mit dieser Auszeichnung wagen wir uns erstmals in der 17jährigen Geschichte des Big-BrotherAwards auf militärisches Terrain beziehungsweise Sperrgebiet. Wohingegen Frau von der Leyen schon einschlägig aufgefallen ist - schließlich haben wir sie bereits 2009 in ihrer damaligen Funktion als Familienministerin mit dem Negativpreis bedacht; wir erinnern uns: als „Zensursula“ wegen ihrer Vorstöße zur Inhaltskontrolle und Sperrung von Webseiten. Doch was haben die Verteidigungsministerin und das Militär mit Überwachung, Zensur, überhaupt mit Datensünden zu tun? Weshalb soll ausgerechnet die Bundeswehr mit ihren Panzern, Bomben und Granaten eine auszeichnungswürdige Datenkrake sein – die in jüngerer Zeit eher durch Neonazi-Umtriebe, Gewaltexzesse, Misshandlungen, sexuelle Übergriffe, Mobbing und einen ausgeprägten Korpsgeist aufgefallen ist?

Nun, die heutige Verleihung erfolgt für die massive digitale Aufrüstung der Bundeswehr mit dem neuen „Kommando Cyber- und Informationsraum“ (KdoCIR) - das heißt im Klartext: für die Aufstellung einer kompletten digitalen Kampftruppe mit (geplant) fast 14.000 Dienstkräften, mit eigenem Wappen, Verbandsabzeichen und Fahne - selbst ein Cyber-Marsch wurde eigens für diese Truppe komponiert, die Frau von der Leyen just vor einem Monat (am 5.04.2017) in Bonn in Dienst gestellt hat. Schon bislang existierte eine kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn (*„Computer Netzwerk Operationen“*) mit etwa 70 bis 80 Soldaten, die für operative Maßnahmen zuständig ist. Diese Einheit wird nun mit weiteren IT-Einheiten der Bundeswehr, etwa dem *Kommando Strategische Aufklärung*, in der neuen Cyber-Kampftruppe verschmolzen und zentralisiert. Weitere dringend benötigte IT-Fachleute versucht die Bundeswehr mithilfe großer Werbekampagnen anzuheuern.

Mit dieser digitalen Aufrüstung wird - neben Land, Luft, Wasser und Weltraum - ein fünftes Schlachtfeld, das sogenannte "Schlachtfeld der Zukunft" eröffnet und der Cyberraum - man kann auch sagen: das Internet - zum potentiellen Kriegsgebiet erklärt. Mit der Befähigung der Bundeswehr zum Cyberkrieg beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – und zwar weitgehend ohne Parlamentsbeteiligung, ohne demokratische Kontrolle, ohne rechtliche Grundlage.

Das klingt zwar ziemlich beunruhigend, bleibt aber eher abstrakt. Was hat all das mit uns zu tun? Was müssen wir befürchten? Wo sind die Betroffenen? Berechtigte Fragen, aber sie greifen zu kurz. Denn nicht alles, was wir hierzulande nicht unmittelbar spüren und erleiden, ist problem- oder harmlos. Schließlich gelten Grund- und Menschenrechte auch für Menschen in anderen Ländern, die sehr wohl betroffen sein können – ganz abgesehen vom Eskalationspotential dieser digitalen Aufrüstung, das auf uns zurückschlagen kann; und ganz abgesehen auch von ungelösten völkerrechtlichen Problemen.

Selbstverständlich ist es legitim, wenn die Bundeswehr geeignete Schutzmaßnahmen ergreift, um sich gegen Cyberattacken von außen zu wehren, die gegen ihre eigene Militär-IT gerichtet sind - angeblich sind das Zigtausende pro Tag (2016: über 47 Mio. IT-Angriffe auf die Bundeswehr).[1] Doch das Bundesverteidigungsministerium gibt sich damit nicht zufrieden. Im Gegenteil: Es erhebt den - unseres Erachtens nach rechtsstaatswidrigen - Anspruch auf kooperative Zuständigkeit der Bundeswehr für die – so wörtlich - *„gesamtstaatliche Sicherheitsvorsorge“* und Abwehr von Cyber-Angriffen. Also auch zum Schutz anderer staatlicher, kommunaler und ziviler Netzwerke im Innern des Landes, für den in Friedenszeiten jedoch ausschließlich Polizei, Geheimdienste und Justiz zuständig sind sowie speziell das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Nationale Cyber-Abwehrzentrum, in dem alle Sicherheitsorgane zusammenwirken. Bundeswehreinsätze im Innern zum Schutz nichtmilitärischer IT-Systeme vor Cyber-Attacken sind insoweit weder verfassungsgemäß noch erforderlich.

Doch es kommt noch härter: Denn die Bundeswehr soll mit ihrer verharmlosend "Cyber- und Informationsraum" genannten Cyber-Kampftruppe nicht nur abwehren können - Ihre dort beschäftigten Cyberkämpfer sollen darüber hinaus bereits im Vorfeld in fremde IT-Systeme eindringen und diese ausforschen können sowie zu eigenen Cyberangriffen auf andere Staaten und deren Infrastruktur befähigt werden. Im Klartext: also zum Führen von Cyberkriegen - im Übrigen auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen der Bundeswehr im Ausland, etwa in Afghanistan oder Mali. So sieht es die geheime *Strategische Leitlinie Cyber-Verteidigung* des Verteidigungsministeriums (2015) vor und auch das *„Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016“*. Das bedeutet: Die Bundeswehr soll eigene Cyberwaffen entwickeln, um getarnt in fremde IT-Systeme einbrechen, diese über Sicherheitslücken, Trojaner, Viren etc. ausspähen, manipulieren, fehlsteuern, lahmlegen, schädigen oder zerstören zu können.

Doch selbst wenn es sich dabei nicht um eigene völkerrechtswidrige kriegerische Angriffe handelt, sondern um Cybergewalt zur Selbstverteidigung gegen Militäratta-

---

[1] https://www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html

cken von außen, dann wäre das zwar völkerrechtlich prinzipiell zulässig, doch höchst riskant. Warum? Weil davon nicht allein militärische Ziele betroffen wären, sondern – zumindest als „Kollateralschäden“ - auch zivile Infrastrukturen. Denn auch Cyberangriffe, die nur auf militärische Ziele gerichtet sind, können rasch zum Flächenbrand führen, sobald sie sich auf kritische zivile Infrastrukturen ausbreiten, diese lahmlegen oder gar zerstören. Digitale Waffen sind in einer vernetzten Welt keineswegs Präzisionswaffen und die Streuwirkung kann immens sein. Und das mit gravierenden, ja lebensbedrohlichen Folgen für die Zivilbevölkerung, wenn die Gegenattacken etwa zu lang andauernden Ausfällen der Strom- und Wasserversorgung oder des Krankenhaus-, Gesundheits- oder Verkehrswesen führen. Dies wäre ein Verstoß gegen das Humanitäre Völkerrecht.

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

Erstens besteht die große Gefahr, dass es aufgrund von Fehlinterpretationen bei der Frage, ob es sich bei einem Cyberangriff um eine kriegerische oder um eine nichtmilitärische, etwa kriminelle Attacke handelt, zu vorschnellen militärischen Selbstverteidigungsschlägen kommt - und damit zu einer gefährlichen und folgenschweren Eskalation. Derzeit ist im Völkerrecht nicht klar und verbindlich definiert, wann ein Cyberangriff als kriegerische Angriffshandlung zu gelten hat. Nach derzeit noch vorherrschender Auffassung[2] unter Völkerrechtlern liegt ein solcher Angriff jedoch nur dann vor, wenn die zerstörerischen Auswirkungen mit denen konventioneller Waffengewalt vergleichbar sind – also wenn eine solche Online-Attacke etwa Züge entgleisen, Flugzeuge abstürzen, Kraftwerke explodieren lässt und Menschen verletzt werden oder umkommen. Doch NATO wie Bundeswehr behalten sich ausdrücklich vor, im Einzelfall zu entscheiden, ab wann es sich um einen solchen kriegerischen Angriff handelt und wie darauf reagiert wird – warum das so ist, verrät ein Oberstleutnant im Verteidigungsministerium:[3] *„weil wir hier auch ein Stück weit unberechenbar bleiben wollen und müssen“.* Diese Unberechenbarkeit hinsichtlich Anlass und Art eines Gegenschlags diene letztlich auch der Abschreckung, so die NATO-Philosophie.

Zweitens: Im Cyberkrieg gibt es keine Armeen, die sich gegenüberstehen und keine Soldaten in Uniform. Stattdessen kommen etwa Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz - also Software, die keine Uniform oder Staatsabzeichen trägt. Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben – um etwa unter falscher Flagge Konflikte zu schüren oder Kriegsgründe zu fingieren. So ist nicht nur schwer herauszufinden, ob es sich bei IT-Angriffen um zivil-kriminelle und wirtschaftliche oder um geheimdienstliche und militärische Operationen handelt. Der angegriffene Staat hat außerdem das Problem, die wahren Urheber zweifelsfrei zu identifizieren, um überhaupt rechtmäßig, angemessen und zielgenau reagieren zu können. Die Beweisführung ist in aller Regel äußerst schwierig. Der Internationale Gerichtshof verlangt jedoch eine klare Beweislage, denn es gibt kein Recht auf militärische Selbstverteidigung ins Blaue hinein oder aufgrund bloßer Indizien; ein Gegenschlag ohne klar identifizierbaren Aggressor ist jedenfalls völkerrechtswidrig.

---

[2] Quelle z.B. Robin Geiß, Völkerrecht im „Cyberwar", http://www.ipg-journal.de/schwerpunkt-des-monats/neue-high-tech-kriege/artikel/detail/voelkerrecht-im-cyberwar-859/

[3] Oberstleutnant Matthias Mielimonka, http://www.zebis.eu/veranstaltungen/archiv/podiumsdiskussion-cyberwar-die-digitale-front/

Und drittens: Diese Probleme werden noch verschärft durch eine gefährliche Rechtsauslegung im *„Tallinn Manual“* – einem NATO-Handbuch zur Anwendung des Völkerrechts auf die Cyberkriegsführung (2013). Zwanzig zumeist militärnahe Rechtsexperten aus NATO-Staaten, auch aus Deutschland, haben diesen Leitfaden erarbeitet. An den darin aufgelisteten 95 Regeln sollen sich alle NATO-Staaten im Fall eines Cyberkriegs orientieren - auch die Bundeswehr. Was aber ist daran so gefährlich? Drei Beispiele:

- Danach gelten selbst solche Operationen als Cyberwar-Angriffe, die bloße wirtschaftlich-finanzielle Schäden eines betroffenen Staates verursachen, wenn diese gewisse Ausmaße annehmen, etwa einen Börsencrash. Dagegen wäre dann eine militärische, auch konventionelle Selbstverteidigung mit Kriegswaffen rechtens, so der Leitfaden, was zu einer unkontrollierbaren Eskalation der Auseinandersetzungen führen könnte.
- Laut Handbuch gelten zivile Hacker („Hacktivists“) als aktive Kriegsteilnehmer, wenn sie Cyber-Aktionen im Verlauf kriegerischer Konflikte ausführen. Solche Zivilisten können daher militärisch angegriffen und auch getötet werden. Selbst das Suchen und Offenlegen von Schwachstellen in Computersystemen des Gegners gilt demnach als kriegerische Handlung. Auf diese Weise wird die Kampfzone praktisch auf Privatpersonen und deren Laptops ausgeweitet.
- Das NATO-Tallinn-Manual sieht zudem vor, dass ein Staat sein Recht auf Selbstverteidigung auch präventiv ausüben darf – bevor überhaupt ein digitaler Angriff stattgefunden hat. Auch hier, wie bei konventionellen Militär-Erstschlägen, besteht hohe Missbrauchs- oder Missinterpretationsgefahr.

Mit der Rechtsauslegung in diesem NATO-Dokument werden die hohen völkerrechtlichen Eingriffsschwellen für bewaffnete Gewaltanwendungen zwischen Staaten unverantwortlich weit herabgesenkt sowie die restriktiven Kriterien des Selbstverteidigungsrechts aufgeweicht. Das gefährdet die Zivilbevölkerungen und die internationale Sicherheit in erheblichem Maße. Was einflussreiche, zumeist militärnahe Völkerrechtler da an Regeln für die NATO zusammengestellt haben, ist geeignet, die Grenzen zwischen innerer und äußerer Sicherheit, zwischen Zivilem und Militärischem, zwischen Krieg und Frieden, zwischen Angriff und Defensive zu verwischen - und eine schwere Datenattacke blitzartig in einen echten Krieg mit Raketen, Bomben und Granaten eskalieren zu lassen.

All dies bedeutet: Mit der Aufrüstung der Bundeswehr zum Cyberkrieg steigen Eskalationspotentiale, Kriegsbereitschaft und Kriegsgefahr – und davor schützt auch die obligatorische Zustimmung des Bundestags zu Militäreinsätzen im Einzelfall nur bedingt. Denn das Cyber-Konzept der Verteidigungsministerin für die Bundeswehr ist letztlich demokratisch kaum zu kontrollieren. Wobei die längst zur Interventionsarmee umgebaute Truppe ohnehin schwer kontrollierbar und skandalträchtig ist.

Wir vergeben unsere Negativpreise zwar für böse Pläne und Taten, aber wir geben unsere Preisträger_innen nicht verloren und verleihen den Preis gerne auch auf Bewährung. Voraussetzung dafür wäre, dass Sie, Frau Verteidigungsministerin, von der digitalen Aufrüstung abrücken, auf offensive Cyberwaffen für die Bundeswehr verzichten und eine ausschließlich defensive Cybersicherheitsstrategie verfolgen, um die Zivilbevölkerung effektiv zu schützen – flankiert von vertrauensbildenden Maßnahmen im Rahmen einer friedensorientierten Außenpolitik und Diplomatie (Stichwort: „Cyberpeace“). Wir fordern darüber hinaus eine weltweite Cyberabrüstung sowie eine völkerrechtliche Ächtung von Cyberspionage und Cyberwaffen. Und wir for-

dern die Schaffung einer unabhängigen Instanz der UN zur Untersuchung zwischenstaatlicher Cyberattacken und deren angemessener Abwehr.

Doch Sie, Frau von der Leyen, haben offenbar anderes zu tun. Sie suchen stattdessen, so wörtlich, „händeringend Nerds“: „Hacker, IT-Programmierer, IT-Sicherheitsfachleute, Penetrationstester, Systemadministratoren oder IT-Entwickler“. Der Bedarf der Bundeswehr liege bei rund 800 IT-Administratoren und 700 IT-Soldaten, also Cyberkämpferinnen und -kämpfern pro Jahr. Flächendeckend und großflächig wirbt die Bundeswehr auf Bahnhöfen, in Unis und Medien um Fachpersonal und Quereinsteiger für den Waffendienst am PC; auch zivile Experten aus Wirtschaft, Verbänden und NGOs werden für eine schlagkräftige „Cyber-Reserve“ geworben. In Anlehnung an den Kriegsslogan Ihres Vorvorgängers Peter Struck – *„Die Sicherheit der Bundesrepublik Deutschland wird auch am Hindukusch verteidigt“* – werben Sie nun mit dem Sinnspruch: *„Deutschlands Freiheit wird auch im Cyberraum verteidigt. Mach, was wirklich zählt…“*. Das klingt spannend und womöglich auch verlockend.

Ob Sie, Frau Ministerin und ihre Werberkolonnen schon mal beim *ChaosComputerClub* oder bei *Digitalcourage* vorbeigeschaut haben? Auch heute hier im Saal sitzen wohl reihenweise technikaffine und -kundige Menschen, die genau in Ihr Beuteschema passen. Darum hoffen wir sehr, dass diese Laudatio und unsere Preisvergabe solche Menschen dazu ermutigen, ihre Fähigkeiten für Frieden und Verständigung im Internet einzusetzen, statt für digitale Angriffe und Cyberkrieg auf dem „Schlachtfeld der Zukunft“!

Herzlichen Glückwunsch zum Negativpreis BigBrotherAward 2017, Frau Bundesverteidigungsministerin und Oberbefehlshaberin der Bundeswehr.

Laudatio: https://bigbrotherawards.de/2017/behoerden-bundeswehr-bundesministerin-fuer-verteidigung-dr-ursula-von-leyen

Dr. Rolf Gössner ist Rechtsanwalt, Publizist und Vorstandsmitglied der Internationalen Liga für Menschenrechte (Berlin; www.ilmr.de). Seit 2000 Mitglied der Jury zur Verleihung des Negativpreises *BigBrotherAward* (www.bigbrotheraward.de). Mitherausgeber der Zweiwochenschrift für Politik/Kultur/Wirtschaft *„Ossietzky“* und des jährlich erscheinenden *"Grundrechte-Reports";* als solcher ausgezeichnet mit der Theodor-Heuss-Medaille 2008; außerdem mit dem Kölner Karlspreis für engagierte Literatur und Publizistik und dem Bremer Kultur- und Friedenspreis. Sachverständiger in Gesetzgebungsverfahren von Bundestag und Landtagen. Internet: www.rolf-goessner.de Autor zahlreicher Bücher zum Themenbereich Demokratie, Innere Sicherheit und Bürgerrechte, u.a.:

- ***Menschenrechte in Zeiten des Terrors.*** *Kollateralschäden an der „Heimatfront“,* Hamburg 2007.
- ***Geheime Informanten.*** *V-Leute des Verfassungsschutzes: Neonazis im Dienst des Staates*, München 2003; Akt. Neuauflage als e-book 2012 bei Knaur-Verlag, München. Download-Direktlink: www.droemer-knaur.de/ebooks/7781709/geheime-informanten
- ***Mutige Aufklärer im digitalen Zeitalter****. Carl-von-Ossietzky-Medaillen an Edward Snowden, Laura Poitras und Glenn Greenwald*, Ossietzky Verlag GmbH, Dähre 2015
- Gössner/Schuhler: ***Terror – wo er herrührt, wozu er missbraucht wird, wie er zu überwinden ist***, isw-spezial 29, München, Dez. 2016 (www.isw-muenchen.de).
- ***Mutige Lebensretter und Aufklärer in Zeiten von Flucht und Abschottung.*** *Carl-von-Ossietzky-Medaillen an SOS Méditerranée und Kai Wiedenhöfer,* Ossietzky Verlag GmbH, Dähre 2017 (Juni).

Kontakt: rolf-goessner@ilmr.de

Quellen / Links (kleine Auswahl)

https://www.bmvg.de
https://www.bundeswehrkarriere.de/arbeitgeber-bundeswehr/der-cyber-und-informationsraum
https://www.bmvg.de/portal/a/bmvg/start/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8zinSx8QnyMLI2MQrw9LQw8zcw9gt0cnQ09flz0wwkpiAJKG-AAjgb6XvpR6Tn5SRCrHPOSjC3S9aOKUtNSi1KL9EqLgMIZJSUFxVaqBqoG5eXleun5-ek5qXopqaoG2HRk5BeX6EegKNQvyI2o8kkNdwQACvQD0g!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/
http://www.spiegel.de/politik/deutschland/bundesregierung-stellt-weissbuch-zur-sicherheitspolitik-vor-a-1102759.html
https://netzpolitik.org/2016/weissbuch-zur-sicherheitspolitik-bundeswehr-geht-in-die-cyberoffensive/
https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/
https://www.heise.de/newsticker/meldung/Bundeswehr-Weissbuch-Planspiele-fuer-den-Krieg-im-Cyberraum-3270870.html