Hans-Jörg Kreowski

Cyberpeace-Forum

Am Freitag, dem 11. November 2016, von 18 bis 20 Uhr und am darauffolgenden Samstag von 14 bis 16 Uhr fand das Cyberpeace-Forum im Haus der Wissenschaft in der Bremer Innenstadt statt. Es war konzipiert als ein Bremer Beitrag zur Cyberpeace-Kampagne des FIfF zur Diskussion aktueller Entwicklungen zum Thema Cyberkrieg. Die Veranstaltung begann am Freitagabend mit einer Podiumsdiskussion anlässlich der Kooperation der Hochschule Bremen mit der Bundeswehr. Am Samstagnachmittag wurden aktuelle Entwicklungen und Gegenentwürfe zum Thema Cyber- und Drohnenkrieg vorgestellt und diskutiert. Beide Veranstaltungsteile waren mit je rund 80 Teilnehmenden passabel besucht. Das Publikum war gut gemischt: Jung und Alt, Frauen und Männer, viele Friedensbewegte, erstaunlich wenige mit direktem Informatikbezug.

Zu der Freitagsveranstaltung unter dem Motto *Zapfenstreich für die Zivilklausel?* wurde mit folgendem Text eingeladen:

> *Die Hochschule Bremen richtet mit Beginn des Wintersemesters 2016/17 einen dualen Studiengang für Informatikerinnen ein. Kooperationspartner hierfür ist die Bundeswehr. Erst 2012 hatte die Hochschule in ihrer Zivilklausel beschlossen: „Studium, Lehre und Forschung an der Hochschule Bremen dienen ausschließlich friedlichen Zwecken. Der Akademische Senat lehnt die Beteiligung von Wissenschaft und Forschung an Projekten mit militärischer Nutzung bzw. Zielsetzung ab […]". Die Entscheidung für die Kooperation mit der Bundeswehr hat innerhalb und außerhalb der Hochschule Bremen intensive Reaktionen und auch Protest ausgelöst. Droht eine Militarisierung der Bildung oder ist die Bundeswehr ein Kooperationspartner wie jeder andere? Auch bundesweit wird diese Entwicklung beobachtet und diskutiert. In der Podiumsdiskussion zwischen Vertreterinnen und Vertretern von Hochschulen, Politik, Gewerkschaften und Friedensbewegung soll das Für und Wider beleuchtet werden.*

Auf dem Podium saßen Susanne Grobien (Vorsitzende des Wissenschaftsausschusses der Bremischen Bürgerschaft), Hans-Jörg Kreowski (Universität Bremen und FIfF), Cornelia Mannewitz (Gewerkschaft Erziehung und Wissenschaft) und Axel Viereck (Hochschule Bremen, Konrektor Studium und Lehre). Die Diskussion wurde moderiert von Ralf E. Streibl in Vertretung von Tim Voss (Deutscher Gewerkschaftsbund Bremen-Elbe-Weser).

Zu der Vortrags- und Diskussionsveranstaltung am Samstag unter dem Motto *Aufrüstung zum Cyberkrieg* hieß es im Einladungstext:

Fotos von der Veranstaltung Hartmut Drewes

> *Die Bundesministerin für Verteidigung Ursula von der Leyen hat im April angekündigt, in der Bundeswehr eine Organisationseinheit Cyber- und Informationsraum aufzubauen. Neben Land, Luft, Wasser und Weltraum wird damit ein fünftes Schlachtfeld offiziell eröffnet. Diese Maßnahme reiht sich ein in die weltweite Aufrüstung für den Cyberkrieg. Das bedroht vor allem auch zivile Infrastrukturen wie Strom- und Wasserversorgung, Verkehr, Gesundheitswesen und die Netzwerke von Staat und Wirtschaft in den Industriestaaten. Die nahezu täglichen Nachrichten über Cyber- und Drohnenangriffe zeigen, dass die Gefahr auch heute schon real ist. Aber auch die Kriegsgefahr allgemein wächst, weil Cyberwaffen vergleichsweise billig und einfach zu beschaffen und zu bedienen sind und weil die Schwelle, sie einzusetzen, eher niedrig ist. Es ist deshalb dringend erforderlich, sich der Gefahren des Cyberkriegs bewusst zu werden und ihnen friedliche Alternativen entgegenzusetzen.*

Es gab fünf kurze Impulsvorträge: *Cyberkrieg und Völkerrecht* von Rolf Gössner (Internationale Liga für Menschenrechte, Bremen), *Die Bundeswehr im Cyber- und Informationsraum* von Thomas Gruber (Informationsstelle Militarisierung, Tübingen), *Die Perversität autonomer Waffen* von Hans-Jörg Kreowski,

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet von Aaron Lye (Universität Bremen und FIfF) und *Wenn Big Data tödlich ist – Globale Überwachung und Drohnenkrieg* von Norbert Schepers (Rosa-Luxemburg-Stiftung, Bremen). Die Moderation hatten Eva Böller (Bremische Stiftung für Rüstungskonversion und Friedensforschung) und Barbara Heller (Bremer Friedensforum). Das Cyberpeace-Forum wurde organisiert vom Bremer Friedensforum, von der Bremischen Stiftung für Rüstungskonversion und Friedensforschung, vom Cyberpeace-Team Bremen, von der Bremer Regionalgruppe des FIfF und von der GEW Bremen. Die Podiumsdiskussion am Freitag wurde außerdem mitorganisiert vom DGB Bremen-Elbe-Weser. Die Veranstaltung wurde dankenswerterweise unterstützt von der Universität Bremen, der Hochschule Bremerhaven, dem AStA der Hochschule Bremen, dem Arbeitskreis Hochschulpolitik sowie vom Forum Friedenspsychologie.

Ich habe das Cyberpeace-Forum als Anregung zur Nachahmung relativ ausführlich beschrieben. Eine derartige Veranstaltung kann ein Publikum weit jenseits der an Informatik und Gesellschaft im engeren Sinne Interessierten erreichen und bietet die Chance zu Kooperationen mit Hochschuleinrichtungen, mit Gewerkschaften und mit Organisationen der Friedensbewegung. Im Falle des Cyberpeace-Teams Bremen wird die Kooperation auch fortgesetzt durch einzelne Veranstaltungen von April bis Juni 2017 mit dem Aufgreifen und Vertiefen der Vorträge von Norbert Schepers am 27. April und von Aaron Lye am 29. Juni sowie am 30. Mai mit einer Protestveranstaltung gegen die Konferenz und Messe *Undersea Defense Technology* in den Bremer Messehallen. Und im Herbst gibt es vielleicht das zweite Cyberpeace-Forum. Weitere Informationen lassen sich auf der Webseite *https://cyberpeace.fiff.de/Kampagne/CyberpeaceForum* finden. Insbesondere kann man dort auch Flyer und Plakat anschauen und das ziemlich beachtliche Medienecho nachvollziehen.

Von den fünf Vorträgen liegen drei in schriftlicher Fassung vor, die nachfolgend abgedruckt sind. Meinen eigenen Vortrag habe ich nicht verschriftlicht, weil ich auf der FIfFKon 2016 einen ganz ähnlichen Vortrag gehalten habe, der in der FIfF-Kommunikation 1/2017 nachzulesen ist.

Rolf Gössner

Cyberkrieg und Völkerrecht

Anlässlich der digitalen Aufrüstung der Bundeswehr im „Cyber- und Informationsraum"

Gegenwärtig wird die Bundeswehr mit einem neuen Kommando Cyber- und Informationsraum *aufgerüstet, das Anfang April 2017 in Dienst gestellt wurde – ergänzt von einem Forschungszentrum an der Bundeswehr-Universität in München.[1] Mit dieser digitalen Kampftruppe mit (geplant) fast 14.000 Dienstposten wird der „Cyber-Raum" zum potentiellen Kriegsgebiet erklärt, beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – bislang übrigens ohne Parlamentsbeteiligung, ohne demokratische Kontrolle und ohne gesetzliche Grundlagen.*

Diese Militarisierung des Interne[illegible]*klärung*, in der neuen Organisati-
raums dient nach Plänen des Bu[illegible]zentralisiert. Darüber hinaus wer-
sowohl der Verteidigung gegen[illegible]nen neue IT-Fachleute angewor-
auch eigener Cyberangriffe auf
Systeme (laut *Geheimer Strategi[illegible]*
gung des Bundesverteidigungsministeriums von 2015).[2] Erstmals spielt im *Weißbuch zur Sicherheitspolitik 2016* der Krieg im Cyberraum eine gewichtige Rolle – inklusive Cyberkämpfer.innen.[3] Das bedeutet: Auch die Bundeswehr entwickelt Cyberwaffen, um in fremde IT-Systeme einbrechen und dort Manipulationen vornehmen oder diese zerstören zu können.

Schon jetzt existiert übrigens eine kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn (*Computer Netzwerk Operationen*) mit 70/80 Soldaten, die für operative Maßnahmen zuständig ist. Diese Einheit wird nun erweitert und zusammen mit den bereits existierenden IT-Einheiten der Bundeswehr, etwa dem

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

I. „Deutschlands Freiheit wird auch im Cyberraum verteidigt" *(Bundeswehr-Werbung)*

Wir haben es bei dieser digitalen Aufrüstung mit einer operativen Befähigung der Bundeswehr zu tun. Im Klartext: mit der Befähigung auch zur verdeckten Cyberkriegsführung im In- und Ausland – auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen der Bundeswehr im Ausland. Nicht allein militärische Ziele lassen sich damit treffen, sondern – zumindest als „Kollateralschäden" – auch zivile Infrastrukturen. Dies kann zu lang andauernden Ausfällen etwa der Strom- und Wasserversor-