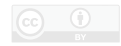


Impression von der Kundgebung (mit freundlicher Genehmigung von Hartmut Drewes)

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

Der Protest fand in den Medien ein beachtliches Echo. Da die Berichterstattung überwiegend positiv ausfiel, fühlte sich Joerg Helge Wagner, Ressortleiter Politik bei der *Bremer Tageszeitungen AG*, bemüht, eine harsche Kritik zu verfassen, die im *Bremer Tagblatt* als Kommentar auf Seite 2 erschienen. Es geht es aber auch darum, sich dort mit maritimer Kompetenz zu verhalten. „... kein Kuckucksheim ...“ Es ist ein Erd und Befürworter von Rüstung und Krieg, von denen es in Politik, Wirtschaft, Wissenschaft und in den Medien viele gibt, aus ihrer Deckung gelockt werden. Wir sollten diesen Damen und Herren viel öfter und kräftiger auf die Füße treten.



Ekkehard Lentz

Cyberpeace-Forum in Bremen Eine gelungene Zusammenarbeit

Bundesverteidigungsministerin Ursula von der Leyen nutzt die öffentliche Debatte zu Cyberattacken und Cyberwar, um das Thema an sich zu reißen. Bereits im Frühjahr 2016 kündigte sie an, in der Bundeswehr eine Organisationseinheit Cyber- und Informationsraum aufzubauen. Spätestens bei der Erstellung des neuen Weißbuchs hat das Bundesverteidigungsministerium die Entscheidung getroffen, dass die Bundeswehr auch Angriffe in fremde Netze verüben soll. Damit wurde ein Kurswechsel eingeleitet, der erhebliche Gefahren und ein großes Eskalationspotenzial birgt.

Das Cyberpeace-Forum am 11./12. November 2016 im Haus der Wissenschaft in Bremen passte somit in die Zeit. In der Einladung zu der zweitägigen Veranstaltung hieß es:

„Neben Land, Luft, Wasser und Weltraum wird ... ein fünftes Schlachtfeld offiziell eröffnet. Diese Maßnahme reiht sich ein in die weltweite Aufrüstung für den Cyberkrieg – und dabei geht es keineswegs nur um die Abwehr von Cyberattacken, sondern immer auch um die Fähigkeit zu eigenen Angriffen. Das bedroht nicht nur die militärischen Informations- und Kommunikationssysteme, sondern vor allem auch zivile Infrastrukturen wie Strom- und Wasserversorgung, Verkehr, Gesundheitswesen und die Netzwerke von Staat und Wirtschaft in den Industriestaaten, weil sie wegen ihrer immensen Abhängigkeit von Informations- und Kommunikationstechnik extrem angreifbar sind ...“

Die Zusammenarbeit des Veranstalterkreises habe ich in der Vorbereitung und Durchführung des Bremer Cyberpeace-Forums sehr positiv wahrgenommen: Cyberpeace-Team Bremen,

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Fiff) Regionalgruppe Bremen, Gewerkschaft Erziehung und Wissenschaft (GEW), Bremer Friedensforum und Bremische Stiftung für Rüstungskonversion und Friedensforschung.

Im Ansatz erinnerte die Anlage des Cyberpeace-Forums an erfolgreiche Zeiten in der deutschen Friedensbewegung. Von großer Bedeutung in der Auseinandersetzung um die Stationierung neuer atomarer Mittelstreckenraketen in der Bundesrepublik der 1980er-Jahre war das Auftreten führender Naturwissenschaftler, denen man zutraute, über die Wirkung moderner Massenvernichtungswaffen kompetent Auskunft geben zu können. In berufsbezogenen Friedensinitiativen bildeten sich vor 35 Jahren unterschiedliche Strukturen heraus, die sich teilweise bis heute stabil halten: Vereine mit einer festen Mitgliedschaft wie die Ärzte-Organisation IPPNW und die Naturwissenschaftler-Initiative gründeten sich, andere arbeiteten als lose Zusammenschlüsse. Neu war, dass sich hier Menschen zusammenfanden, die aus einer Berufsgruppe kamen und ihre Hauptaufgabe darin sahen, die Friedensthematik Kolleginnen und Kollegen nahe zu



Ekkehard Lentz

Ekkehard Lentz arbeitet als Erzieher und ist seit vielen Jahren in der Friedensbewegung aktiv. Momentan fungiert er ehrenamtlich als Sprecher des Bremer Friedensforums (www.bremerfriedensforum.de, www.facebook.com/bremerfriedensforum, <https://twitter.com/ekkehardlentz1>).

bringen und mit ihrer speziellen fachlichen Kompetenz Beiträge für die Friedensbewegung zu liefern.

Heute geht es darum, sich auf internationaler Ebene für konkrete Vereinbarungen zu einem friedlichen Miteinander im Cyberraum einzusetzen, statt die militärische Logik ins Netz zu tragen. Die Zusammenarbeit von Wissenschaftlern und Friedensgruppen sollte fortgesetzt und intensiviert werden. Die Cyberpeace-

Kampagne des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. bietet eine gute Grundlage für weitere politische Aktivitäten.

Das Bremer Friedensforum hat die Kampagne auf seiner Website verlinkt: <http://www.bremerfriedensforum.de/743/aktuelles/Die-Cyberpeace-Kampagne-geht-weiter/>



FIfF e.V. – Pressemitteilung

WannaCry, ein Kollateralschaden des Cyberwar

18. Mai 2017 – Die Schadsoftware WannaCry wütet in der Welt. Vier Tage zuvor feierte der Kurzfilm „Cyberpeace statt Cyberwar“ Premiere auf der re:publica 2017. Der Film erklärt, warum das Geheimhalten von Schwachstellen zum Zweck eines Cyberwars eine Gefahr für die Bevölkerung ist. Die WannaCry-Pandemie traf auch Betreiber kritischer Infrastrukturen wie die Deutsche Bahn und britische Krankenhäuser und zeigt, wie verwundbar diese für Malware-Angriffe sind. Dies ist ein weiterer Aspekt, auf den der Film eingeht.

WannaCry veranschaulicht, dass Betreiber von kritischen Infrastrukturen nicht in der Lage sind, sich selbst und uns vor Angriffen aus dem Internet zu schützen. Und WannaCry hat eine Geschichte. Die Schadsoftware nutzt eine Schwachstelle, die von der NSA seit fünf Jahren geheim gehalten wurde. Vor einigen Monaten ist dieses Wissen von der NSA zu nichtstaatlichen Kriminellen gelangt. Dies veranschaulicht exemplarisch, was passieren kann, wenn staatliche Stellen wie Geheimdienste, Strafverfolgung und Militär Schwachstellen geheim halten, um sie zur Spionage, für Überwachung oder in Cyberwaffen zu verwenden.



Ausschnitte aus dem Film: Cyberpeace statt Cyberwar

Sylvia Johnigk, Vorstandsmitglied des FIfF, stellt fest: „Durch die Geheimniskrämerei bei Schwachstellen werden auch eigene Infrastrukturen und die von Verbündeten gefährdet.“ Über kurz oder lang scheitert die Geheimhaltung ohnehin. Schwachstellen können auch von anderen entdeckt werden. Sie besitzen einen enormen Wert, der sich sowohl bei Behörden als auch im Darknet zu Geld machen lässt.

Kai Nothdurft, ebenfalls im Vorstand, ergänzt: „Mit der Geheimhaltung einer Schwachstelle ist es vorbei, wenn jemand durch Hacking an die Information gelangt.“

Das FIfF fordert, dass gerade staatliche Stellen alle gefundenen Schwachstellen unverzüglich an die Hersteller melden und dann

in einem verantwortlichen Zeitrahmen veröffentlichen. Insbesondere öffentliche Stellen müssen die Integrität und Sicherheit von Informationssystemen bewahren. Sie sind an die Wahrung der Verfassung gebunden, die das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschließt.

Der Film ist unter <https://vimeo.com/216584485> abrufbar.



Schwachstellen werden auch von Kriminellen, wie Betrügern und Terroristen, gefunden und gegen uns eingesetzt.



cyberpeace.fiff.de, gefördert durch die Stiftung Bridge