Hans-Jörg Kreowski und Raffael Rittmeier

Bericht zur Cyberpeace-Kampagne in Bremen

In Bremen hat sich eine kleine Gruppe Interessierter zusammengefunden, die den Bremer Zweig der Cyberpeace-Kampagne bildet. Wir wollen kurz über den Stand der Arbeit berichten.

Ausgangspunkt war die *Weihnachtsvorlesung* des ersten Autors zum Thema *Cyberpeace – für eine friedensstiftende Informatik*, in deren Einladung es hieß:

> *Die Vorzeichen des größten Teils der Informatikforschung sind inzwischen zivil. Das war in der Anfangszeit des Faches anders, und auch heute noch kann nicht vernachlässigt werden, dass Informatik und Militär äußerst eng verflochten sind. Killerdrohnen und Cyberattacken sind nur die medial stark rezipierten Erscheinungen dieser unheilvollen Liaison. Was sich unter dem Begriff Cyberkrieg subsumieren lässt – und das heißt Krieg mit den Mitteln und dem Know-how der Informatik –, bedroht alle zivilen Infrastrukturen, Recht und Freiheit und letztlich sogar die menschliche Existenz. Der Gegenentwurf ist eine friedensstiftende Informatik.*

Es gibt auch eine Videoaufzeichnung der Weihnachtsvorlesung [1].

Seit Januar hat sich der Bremer Zweig der Cyberpeace-Kampagne alle drei bis vier Wochen getroffen und dabei begonnen, eine Reihe von Veranstaltungen zum Thema *Cyberpeace: Für eine friedliche Entwicklung der digital vernetzten Welt* zu planen. In einer Pressemitteilung ist die Idee so beschrieben:

> *Spätestens durch die Enthüllungen von Edward Snowden ist einer breiten Öffentlichkeit bewusst geworden, dass Geheimdienste weltweit und in horrendem Ausmaß die digitale Kommunikation ausspähen und überwachen und so Grund- und Menschenrechte wie den Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung außer Kraft setzen. Darüber hinaus zeigen die fast täglichen Meldungen von Hackerangriffen und Cyberattacken auf Konzerne, Banken, staatliche Einrichtungen und zivile Infrastrukturen, dass im Internet nicht nur Wirtschaftsspionage im großen Stil betrieben wird, sondern sogar die Funktionsfähigkeit von Wirtschaft, Staat und Gesellschaft bedroht ist. Die Versorgung unserer Lebensgrundlagen wie Trinkwasser und Energie ist abhängig von digitaler Steuerung. Sabotage und Hackerangriffe können lebensbedrohlich für jeden Einzelnen werden. Schließlich belegt nicht zuletzt der tausendfache tödliche Einsatz von Killerdrohnen in Afghanistan, Jemen und in Pakistan, dass schon jetzt die Anwendung von Informationstechnik zum „Kriegsalltag" in vielen Teilen der Welt gehört. Es findet zurzeit – teilweise ganz offen, teilweise verdeckt – eine gigantische Cyberaufrüstung statt. Die digitale Kriegsführung (Cyberwar) eröffnet den Konfliktparteien neue anonyme Möglichkeiten der Vernichtung. Unser Anliegen ist es, die Öffentlichkeit hierüber zu informieren und dafür zu gewinnen, eine Weichenstellung für den digitalen Frieden (Cyberpeace) zu unterstützen.*

Die erste Veranstaltung hat am 14. April 2015 im *Haus der Wissenschaft* in der Bremer Innenstadt unter dem Motto *Stoppt die digitale Ausspähung – Maßnahmen gegen Datensammelwut und Überwachungswahn* stattgefunden. Referenten waren der Rechtsanwalt Dieter Dette aus Bremen zum Thema *Deutsches Datenschutzrecht* und Prof. Dr. Klaus-Peter Löhr aus Berlin zum Thema *Selbstdatenschutz*. Dieter Dette ist zunächst auf die Entstehung des Datenschutzes in Deutschland eingegangen (u. a. Unzulässigkeit von Langzeit-/Querschnittprofilen). Er hat hervorgehoben, dass bisher der Gerichtsstand hinsichtlich der EU-Datenschutzrichtlinie ungeklärt ist. Zu der Möglichkeit der „Selbstzertifizierung" von US-Firmen durch das *Safe-Habour*-Abkommen wurde eine Studie von Galexia zitiert (siehe dazu z. B. [2] und [3]).

Ein Fazit dabei war, dass beim Datenschutz leider eine wirksame Kontrolle fehlt. Klaus-Peter Löhr hielt einen technischen Vortrag mit dem Anspruch, dass er auch für Laien verständlich sein sollte. Er propagierte im Wesentlichen S/MIME-Zertifikate für die vertrauliche E-Mail-Kommunikation und forderte die Bundesregierung auf, eine komfortable und eine kostenfreie Zertifizierungsstelle zu schaffen. Auf die Problematik mit zentralen Stellen, denen man dabei „blind" vertrauen muss, ging er nicht weiter ein und empfiehlt auch nicht PGP/GnuPG. Ansonsten erwähnte er, wie problematisch Werbeanzeigen und Cookies auf Webseiten z. B. im Gesundheitssektor sein können. Am Ende kam er zu dem Schluss, dass der Staat seinen Schutzpflichten nicht nachkomme und daher der Selbstdatenschutz (noch) notwendig sei.

Mitveranstalter waren das TZI (Technologie-Zentrum Informatik und Informationstechnik) der Universität Bremen und die FIfF-Regionalgruppe Bremen. Von beiden Vorträgen sind Videoaufzeichnungen verfügbar [4].

Ab Mai gibt es weitere Treffen, um die inhaltliche Auseinandersetzung mit dem Cyberpeace-Komplex voranzubringen, die erste öffentliche Veranstaltung auszuwerten und in die Planung von Folgeveranstaltungen einzutreten. Nach unserem Eindruck besteht ein großer Diskussionsbedarf, so dass wir unsere Bremer Initiative zur Nachahmung empfehlen, wobei natürlich immer die regionalen Gegebenheiten einbezogen werden müssen.

Referenzen

[1] http://mlecture.uni-bremen.de/ml/index.php?option=com_content&view=article&id=249

[2] http://www.galexia.com/public/research/articles/research_articles-pa08.html

[3] http://heise.de/-933700

[4] http://mlecture.uni-bremen.de/ml/index.php?option=com_content&view=article&id=263