FIfF e.V.
Goetheplatz 4, 28203 28203
28203 Bremen
Fon 0421 33659255
Fax 0421 33659256
fiff@fiff.de
www.fiff.de

Presseerklärung **15.07.2015**

Presseerklärung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.:

FIfF fordert einen öffentlichen Diskurs über die neue Cyber-Sicherheitsstrategie der Bundeswehr

Die Pläne der Verteidigungsministerin Ursula von der Leyen, das Internet zu einem Kriegsschauplatz zu erklären und die Fähigkeit der Bundeswehr offensiv Einsätze im In- und Ausland durchzuführen auszubauen, ist eine Ankündigung Deutschlands, zukünftig wissentlich gegen die Genfer Konvention verstoßen zu wollen.

Deutschland ist aktuell nicht in der Lage, sein Parlament vor Angriffen zu schützen. Nach dem Bundestagshack steht die Regierungsfähigkeit unseres Landes auf dem Spiel. Aber statt kritische Infrastrukturen in Deutschland besser zu schützen und hierzu IT-Fachkräfte des Landes einzusetzen, handelt die Verteidigungsministerin nach dem Motto einer amerikanischen Filmkomödie „Angriff ist die beste Verteidigung“.

Laut einem „geheimen Dokument“, das Spiegel-Online vorliegt, heißt es: »[...] Bei Missionen im Ausland soll es zum Beispiel möglich sein, die Nutzung von Internet und Mobilfunk durch den Gegner "einzuschränken, gegebenenfalls sogar auszuschalten" [...] Möglicherweise könnten Reservesoldaten aus der IT-Wirtschaft" in hoheitlichem Auftrag" zur Unterstützung im Cybernotfall herangezogen werden.«

Um einen Gegner gezielt abzuwehren, müssen mindestens zwei Voraussetzungen erfüllt sein: Zum einen muss man den Angreifer in Echtzeit bzw. zeitnah zweifelsfrei identifizieren und lokalisieren können, gleichzeitig bräuchte man eine adäquate chirurgisch präzise Waffe, um diesen Angreifer virtuell schädigen zu können, aber ohne andere ('kollateral') zu schädigen.

Beim Bundestagshack weiß man Monate später nur wenig über Hergang und Verursacher des Angriffs – und das trotz intensiver Untersuchungen durch das BSI und externe IT-Dienstleister.

Für präzise Cyberoperationen wird ein Arsenal unterschiedlich wirkender Cyberwaffen und eine Vorratshaltung umfangreicher Kenntnisse über geheimgehaltene Schwachstellen für ihren Einsatz benötigt. Dabei ist jede geheimgehaltene Schwachstelle eine vertane Chance, sie zu schließen, um unsere IT-Systeme sicherer zu machen.

Der Plan offensive Angriffe auf zivile Infrastrukturen (Internet und Mobilfunk) im Ausland durchführen zu wollen, würde zu Kriegszeiten einen völkerrechtlichen Verstoß gegen die Genfer Konventionen darstellen. Ein solches Szenario zu Friedenszeiten zur erklärten Sicherheitsstrategie Deutschlands zu machen, bedeutet eine Ankündigung zukünftig gegen die Genfer Konvention verstoßen zu wollen. „Es wäre ein Skandal Deutsche IT Fachkräfte zu missbrauchen und zwangszuverpflichten, um eine Sicherheitsstrategie zu unterstützen, die gegen Völkerrecht verstößt“, urteilt Sylvia Johnigk, Sprecherin der Cyberpeacekampagne.

„Wir sehen erheblichen Beratungsbedarf insbesondere der Bundesverteidigungsministerin, aber auch der Bundesregierung und des Bundestages und fordern einen öffentlichen parlamentarischen Diskurs unter Einbeziehung unabhängiger Berater_innen, um über die Risiken und Gefahren, die von einer derartig offensive Sicherheitsstrategie in Cyberspace ausgeht, öffentlich zu diskutieren“, fordert Werner Hülsmann, Beiratsmitglied des FIfF e.V.

Bei Rückfragen wenden Sie sich bitte an:
Sylvia Johnigk, Sprecherin der Cyberpeace Kampagne, sylvia@fiff.de
Werner Hülsmann, Beiratsmitglied des FIfF e.V., werner@fiff.de