Dietrich Meyer-Ebrecht – Rede bei der Demonstration

Freiheit statt Angst – Kundgebung 29. August 2015, Köln, Neumarkt

Freiheit statt Angst – dieses Motto muss jede Gesellschaft mit an die vorderste Stelle setzen! Ein großer Dank an die Organisatoren dieser Kundgebung und euch allen für euer Engagement, dass ihr nach einer langen Demo hier wieder zusammengekommen seid, um Solidarität zu zeigen, um der politischen Forderung Nachdruck zu geben.

Angst kann man nur durch Wissen begegnen. Hier ist es das Wissen über die Akteure und ihre Ziele. Dort, wo die Akteure nationale Behörden oder Unternehmen sind, ist noch mit Einschränkungen transparent, was ihre Ziele sind. Dunkel wird es, sobald die Geheimdienste ins Spiel kommen. Sie unterliegen keinerlei parlamentarischer Kontrolle, und die Politik tut alles, ihr Tun zu vernebeln. Noch undurchsichtiger wird es durch die internationale Zusammenarbeit der Geheimdienste – NSA, GCHQ, BND. Gemeinsam mauscheln sie sich an nationalen Richtlinien und Gesetzen vorbei. Von den Geheimdiensten geht jedoch die stärkste Triebkraft zur flächendeckenden Ausspähung aus. Über die Kriterien, mit denen sie die Netze durchkämmen, wissen wir nichts. Und wir erfahren nicht, wenn wir selber ins Fadenkreuz geraten – nicht wann, nicht wie, nicht warum. Regelmäßig werden Fälle bekannt, dass Unbescholtene ins Netz geraten – Kollateralschaden …

Hinter den Geheimdiensten stehen militärische Interessen. Für die Militärs ist der Cyberspace ein Spionageinstrument von einer bisher unerreichten Mächtigkeit. Aber dies ist erst die Grundstufe des Informationskrieges. Die Militärs wollen mehr. Sie nutzen das Internet, um in unsere Computer, in unsere Intranets, in unsere Infrastrukturen einzudringen und geheime Zugänge anzulegen. Einige sind entdeckt worden, z. B. bei der Telekom. Wir wissen nicht, wie viele und welche bis heute unentdeckt geblieben sind.

Über diese geheimen Zugänge zu den Netzen von Behörden, Institutionen und Unternehmen kann das volle Programm des Informationskrieges abgespielt werden: Durch Einspeisen von Missinformation und Desinformation kann eine nationale Zivilgesellschaft destabilisiert werden. Beispiele gab es in Osteuropa. Mit dem Einschleusen von Schadsoftware kann Sabotage bis zu physischen Zerstörungen bewirkt werden. Prominentes Beispiel ist die Zerstörung einer Reihe von Urananreicherungszentrifugen im Iran durch den Trojaner *Stuxnet*. Solche hochkomplexen Software-Entwicklungen sind Cyberwaffen. Kaspersky hat kürzlich über die Identifizierung und Analyse von allein 36 im Netz gefundener Schadprogramme dieser Art berichtet. Unvorstellbare Folgen kann die Übernahme der Kontrolle über kritische Infrastruktursysteme wie Energieversorgung, Verkehrssteuerung, Mobilfunknetze haben. Die Bundesregierung hat vor einigen Jahren eine Studie anfertigen lassen über die Folgewirkungen eines länger andauernden, großflächigen Stromausfalls. Die Ergebnisse lesen sich wie ein Albtraum. An dieser Flanke kann eine Nation niedergezwungen werden, ohne dass konventionelle Waffen zum Einsatz kommen müssen.

Cyberwarfare ist inzwischen fester Bestandteil der militärischen Szenarien. Darin ist der Cyberspace fünfter Operationsraum neben Land, Luft, See und Weltraum. Auch die Bundeswehr mischt jetzt mit. Ministerin von der Leyen arbeitet gerade daran, den Etat des BND und der Bundeswehr auf diesem Sektor um 750 Stellen aufzustocken. Unter anderem dient dieses Personalbudget zum Aufbau staatlicher Hackertrupps, die nach Sicherheitslücken fahnden und passende Exploits als digitale Einbruchswerkzeuge entwickeln. Kenntnisse und Exploits, auf einem prosperierenden Schwarzmarkt aufgekauft, ebenfalls mit unseren Steuergeldern. Natürlich werden diese Erkenntnisse und Entwicklungen geheim gehalten. Anderenfalls wären sie für Geheimdienste und Militärs wertlos. Absichtsvoll werden sie der Zivilgesellschaft vorenthalten: In zivilen Systemen bleiben diese Sicherheitslücken offen!

Es gibt weitere Risiken für die Zivilgesellschaft: Operationen mit Cyberwaffen sind unkontrollierbar, wie das Beispiel Stuxnet zeigt. Der Trojaner hat weltweit eine große Anzahl baugleicher Prozesssteuerungsanlagen befallen – Kollateralschaden. …

Cyberoperationen hinterlassen keine physischen Spuren. Der Urheber kann seine Identität verschleiern und die Spuren eines Angriffs verwischen. Ein Gegenschlag des Angegriffenen kann den Falschen treffen und zur Eskalation führen.

Dies sind nur einige der Risiken für die Zivilgesellschaft, die bereits heute sichtbar sind. Es wird höchste Zeit, dem militärischen Missbrauch unserer zivilen Netze entgegenzusteuern. Das will das FIfF mit seiner Kampagne *Cyberpeace* bewirken. Wir wollen über diese viel zu wenig beachtete Entwicklung aufklären. Wir wollen die Öffentlichkeit mobilisieren, Druck auf die Politik zu machen, um Maßnahmen für eine ausschließlich friedliche Nutzung der Informations- und Kommunikationsnetze einzufordern. Wir appellieren an unsere Regierung und an das Parlament:

- Frau von der Leyen, verzichten Sie auf Cyberwaffen für die Bundeswehr!
- Frau Merkel, Herr Steinmeier, setzen Sie sich für einen weltweiten Bann dieser Waffengattung ein!

Freiheit statt Angst – wer das will, muss auch diese Forderungen unterstützen!