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

Stefan Hügel

Betrifft: Cyberpeace

Bedrohungen

Diesmal funktioniert alles.
(Spliff, „Computer sind doof", 1982)

Wir leben heute unter vielfältigen Bedrohungen. Gerade haben uns die Anschläge in Brüssel wieder die Verwundbarkeit unserer hochintegrierten und -technisierten Zivilisation vor Augen geführt. Man kann den Terrorismus dieser Anschläge als Angriff auf Europa und unsere Gesellschaft begreifen. Man kann ihn aber auch als Reaktion auffassen – auf die Bedrohung, die unsere westlichen *Gesellschaften ihrerseits für die Gesellschaften des Nahen Ostens darstellen: Durch konventionelle militärische Angriffe und durch Cyberwarfare, wie Drohnenangriffe und Angriffe auf Industrieanlagen. Wir führen einen unerklärten,* neuen *Krieg in diesen Staaten – wer diesen Krieg* angefangen *hat, hängt wie so häufig vom Standpunkt ab.*

Allgegenwärtige Bedrohung – das war das Umfeld, in dem das FIfF 1984 gegründet wurde. Es ist heute kaum noch vorstellbar, ständig unter dem Damoklesschwert einer Auslöschung der Menschheit, mindestens aber der uns vertrauten Zivilisation, zu leben. Ständiger Fluglärm durch übende Tiefflieger führte uns die Bedrohung jeden Tag plastisch vor Augen und Ohren. Offenbar gab es mehrere Vorfälle, bei denen es nur der Besonnenheit einzelner Menschen im letzten Moment zu verdanken war, dass es damals nicht zum Äußersten kam.

Verstärkt wurde die Bedrohung durch das SDI-Programm, im Volksmund auch *Star Wars* genannt, des damaligen US-Präsidenten Ronald Reagan. Experten der Informatik, die sich kurze Zeit später im FIfF zusammenfinden sollten, wussten: Was uns hier als Mittel gegen die atomare Bedrohung verkauft werden sollte, verstärkte diese zusätzlich, indem man Maschinen – damals noch weniger zuverlässig als heute – mit der Entscheidung betrauen wollte, das atomare Feuer bei einem Angriff des *Gegners* auszulösen. Der *Unsicherheitsfaktor* Mensch, der zuvor noch das Schlimmste verhindert hatte, konnte *endlich* ausgeschaltet werden. Der Versuch, diesen automatisierten Atomtod, oder *Atomkrieg aus Versehen*, verfassungsrechtlich anzugreifen, scheiterte bekanntermaßen.

Die Gefahr der weltweiten atomaren Vernichtung scheint (vorläufig) gebannt. Die Bedrohungen durch Cyberwarfare sind heute real, erscheinen aber abstrakt und sind für viele unsichtbar – lediglich wenn Cyberkriminelle eine große Zahl von Computern mit Schadsoftware infizieren, wie es derzeit mit der Ransomware *Locky* geschieht, wird uns die Bedrohung bewusst. Auch hier wurden lebenswichtige Einrichtungen – Krankenhäuser – geschädigt. Wenn es sich hier auch um Kriminelle handelt und nicht um Militärbehörden: Die Methoden sind die gleichen und sie richten die gleiche Art von Schaden an.

Bedrohungen durch Cyberwarfare lassen sich unter vier Kategorien fassen: Bedrohung der Grundrechte und der Sicherheit unserer Infrastruktur durch Maßnahmen der Ausspähung und Überwachung, Bedrohung des Lebens Unschuldiger und rechtsstaatlich als unschuldig Geltender durch Drohnen – ferngesteuert oder autonom –, Bedrohung von technischen Anlagen – militärisch oder zivil – durch Schadsoftware und Bedrohung unserer Demokratie durch *Information Warfare*, die Täuschung und Manipulation der Öffentlichkeit – auch unbeabsichtigt – durch Medien und nachrichtendienstliche Mittel.

Überwachung

Cyberwarfare beginnt mit der Überwachung der Zivilgesellschaft – diese Ausspähung der Menschen verletzt ihre Privatsphäre und damit die Menschenwürde als ein elementares Menschenrecht. Doch der Schaden, den die Überwachungsmaßnahmen anrichten, ist größer: Voraussetzung für die Überwachung ist die Manipulation von IT-Systemen und die Geheimhaltung oder sogar der absichtsvolle Einbau von Schwachstellen. Die Folge sind unzuverlässige und unsichere Computer- und Kommunikationssysteme wie Internet oder Mobilfunknetze, von deren reibungslosem Funktionieren gleichzeitig weite Teile unserer Gesellschaft abhängig sind. Durch die Aufrüstung für die Cyberwarfare wird auch in Friedenszeiten die Sicherheit der zivilen IT-Infrastruktur ausgehöhlt und untergraben.

Drohnenangriffe

Ausspähung und Computermanipulationen bereiten konventionelle militärische Operationen vor, beispielsweise rechtswidrige Drohnenangriffe durch die Ortung von Zielpersonen, und sie sind damit die Grundlage aggressiver (kriegerischer) Operationen. „*We kill people based on Metadata*", diese Aussage des ehemaligen Direktors von CIA und NSA, General Michael Hayden, macht den Zusammenhang zwischen nachrichtendienstlicher Ausspähung und extralegaler Tötung klar. Drohnenangriffe for-

dern laufend zahlreiche Opfer unter Unbeteiligten. Angriffe, die auf unsicheren Eigenschaften der Ziele basieren (*Signature Strikes*) richten sich gegen Opfer, gegen die nicht einmal ein hinreichender Verdacht besteht. Computergestützte militärische Operationen erzeugen zusätzlich die Illusion eines *sauberen* Krieges und senken damit die Schwelle des Einsatzes. Weiter gesteigert wird das Bedrohungspotenzial durch Systeme, die autonom agieren, also automatisiert töten. Dass wir von einer funktionierenden Maschinenethik noch weit entfernt sind, zeigt vielleicht auch der Fall des Microsoft-Chatbots *Tay*, der sich binnen kurzer Zeit vom virtuellen Hipster-Mädchen zum Hitler-Bot entwickelte und nach kurzer *Umlernphase* autonom Hass-Kommentare twitterte.

Schadsoftware

Staatliche Cyberkrieger sind heute die ressourcenstärksten Hackerorganisationen weltweit. Ihre Cyberangriffe sind nicht zu kontrollieren und gefährden neben ihren eigentlichen Zielen auch zivile Systeme, wie etwa Systeme zur Sicherstellung lebenswichtiger Ressourcen (Wasser, Energie), Krankenhäuser oder Chemiewerke. Der gegen eine iranische Atomanlage gerichtete *Stuxnet*-Wurm breitete sich weltweit aus. Wir können wohl davon ausgehen, dass es weitere gefährliche Trojaner vom Stuxnet-Format als *APT – Advanced Persistent Threats* – von staatlicher Herkunft gibt.

> *Die Schadsoftware* Stuxnet*, entdeckt im Jahre 2010, wurde für einen Angriff auf die Urananreicherungsanlage des Iran in Natanz und das Kernkraftwerk Buschehr eingesetzt. Es handelt sich dabei um ein Schadprogramm zum Angriff auf ein System zur Überwachung und Steuerung der Firma Siemens (Simatic S7), das in die Steuerung von Frequenzumrichtern, z. B. zur Steuerung der Geschwindigkeit von Motoren, eingreift. Durch Manipulation der Drehzahl wurden die Zentrifugen zur Urananreicherung beschädigt. Die Schadsoftware wurde dafür über mobile Feldprogrammiergeräte (spezielle Notebooks) in die physisch isolierten Prozesssteueranlagen eingeschleust. Aufgrund seiner hohen Komplexität und seines Zieles, Steuerungssysteme von Industrieanlagen zu sabotieren, gilt Stuxnet bisher als einzigartig. Es wird angenommen, dass die Schadsoftware durch staatliche Akteure in den USA und in Israel gezielt zur Zerstörung Iranischer Atomanlagen entwickelt wurde; für staatliche Stellen spricht die hohe Komplexität und der damit verbundene Aufwand für die Erstellung der Software.*

Der Einsatz von Cyberwaffen durch Staaten ist eine Kriegshandlung mit erheblichem Eskalationspotenzial, die die internationale Sicherheit erheblich gefährdet.

Manipulation

Aufgrund ihrer mangelnden Transparenz sind militärische und geheimdienstliche Institutionen grundsätzlich schwer zu kontrollieren. Informationen zu Bedrohungen und Schwachstellen können manipuliert, verfälscht oder irreführend sein. Demokratische und parlamentarische Gremien werden falsch und unzureichend informiert oder schlicht belogen. Kontrollgremien sind ungenügend ausgestattet und können deswegen ihrer Aufgabe nicht umfassend nachkommen. Die unzureichende Information des NSA-Untersuchungsausschusses hat uns das Beispiel der NSA-Selektoren deutlich vor Augen geführt. Wie stichhaltig die Gründe für Geheimhaltung sind, kann die Öffentlichkeit nicht überprüfen – die Einstufung wird von den zu kontrollierenden Behörden selbst vorgenommen. Uns allen bekannt ist die Behauptung des damaligen Chefs des Bundeskanzleramts, Ronald Pofalla, als er die Debatte um die Snowden-Dokumente mit den Worten für beendet erklärte, die Vorwürfe seien nun „vom Tisch". Dieser Manipulationsversuch brachte Pofalla vor allem Häme ein. Doch Manipulation kann nicht immer so schnell aufgedeckt werden. Auch das zuverlässig einsetzende Medienstakkato nach Anschlägen – wenn auch nicht politisch, sondern wohl eher wirtschaftlich motiviert – trägt zur Verunsicherung der Bevölkerung bei und wird zu gern politisch ausgenutzt, um sofort Forderungen nach weiterer Aufrüstung bei Militär, Geheimdiensten und anderen Sicherheitsbehörden zu erheben.

… und Deutschland mittendrin

Nachrichtendienste kaufen beispielsweise *Zero-Day-Exploits* auf, um die damit verbundene Kenntnis von Schwachstellen in Softwaresystemen für Angriffe nutzen zu können. Auch wenn dem BND bisher offenbar weniger Geld bewilligt wurde als beantragt: Dies macht sehr deutlich, dass sich auch deutsche Behörden am Cyberkrieg beteiligen wollen. Nach den *Strategischen Leitlinien Cyber-Verteidigung* des Bundesministeriums der Verteidigung hätten offensive Cyber-Fähigkeiten das Potenzial, das Wirkspektrum der Bundeswehr signifikant zu erweitern. Möglich seien offensive Maßnahmen zur Beeinträchtigung von fremden Informations- und Kommunikationssystemen sowie der darin verarbeiteten Informationen. Das wäre nicht nur ein Verstoß gegen die Verpflichtung zur *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, die das Bundesverfassungsgericht 2010 festgestellt hat, sondern auch gegen die verfassungsrechtliche Unzulässigkeit von Angriffskriegen. Auch Drohnen sind ein Thema für die Bundeswehr: Nachdem die Nutzung der Drohne *EuroHawk* an fehlenden Genehmigungen für den Einsatz gescheitert ist, ist die Anschaffung auch von Kampfdrohnen offenbar geplant (möglicherweise Drohnen wie die israelische *Heron* oder die US-amerikanische *Reaper*, die acht *Hellfire*-Raketen tragen kann). Später soll es offenbar auch eine deutsche Beteiligung an der Entwicklung einer europäischen Drohne geben – Berichten zufolge sind hierfür 660 Millionen Euro eingeplant. Im Projekt *Eikonal* ist Deutschland auch an der Ausspähung des Frankfurter Knotens DE-CIX beteiligt.

Bedrohungen

Die Bedrohungen durch Cyberwarfare sind vielfältig. Auch wenn wir nicht mehr unter dem Damoklesschwert des millionenfachen Atomtods leben müssen: Cyberwaffen bedrohen uns und andere. Und sie haben auch indirekte Folgen: Kann ein potenzieller Selbstmordattentäter in einer europäischen Hauptstadt auch dadurch zum Terrorakt motiviert werden, dass er mitansehen muss, wie seine Familie im Feuer eines Drohnenangriffs ums Leben kommt?

Bedrohungen produzieren Angst und Angst produziert neue Bedrohungen: Die Rüstungsspirale nicht nur im Cyberspace muss ein Ende haben.