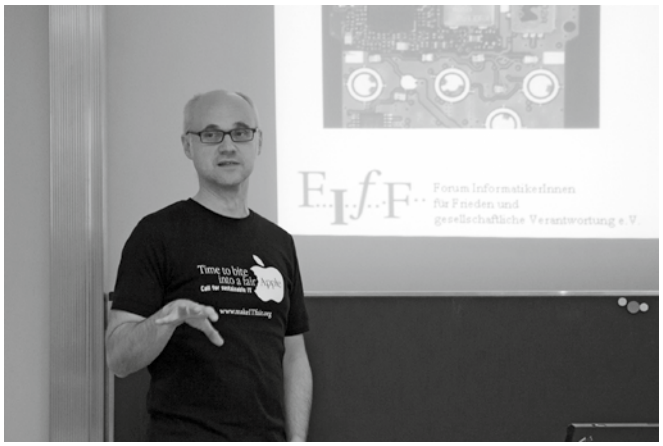
erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Berichte aus den Arbeitsgruppen der Jahrestagung 2012

Sebastian Jekutsch

Arbeitsgruppe: „Sind faire Computer möglich?“

Nach dem kleinen aber feinen Workshop im Vorjahr wurde auch in Fulda eine Arbeitsgruppe zu Fairer IT angeboten.



Im Laufe meiner Recherchen habe ich viele interessante Quellen entdeckt und einige davon in der AG vorgestellt. Die „Arbeit“ der Gruppe bestand auch dieses Jahr darin, sich aus der Vielzahl von Informationen eine Meinung zu bilden, wie man die unschöne Situation bei der Herstellung von Hardware verbessern kann.

Der Ablauf wurde etwas gestrafft, hinzu kam ein Augenmerk auf aktuelle Entwicklungen:

- „Ist IT-Produktion unfair?“ mit Beispielen aus dem Rohstoffabbau, der Fertigung und der Entsorgung von Altgeräten, auf Basis öffentlich zugänglicher Recherchen diverser zivilgesellschaftlicher Initiativen.
- „Sind faire Computer möglich?“ mit einer Aufzählung der Probleme im Vergleich etwa mit fairem Kaffee oder Kleidung: viele Rohstoffe, viele Akteure, viele Länder und Industrieabhängigkeit.
- „Was können wir tun?“ mit einer Reihe von Gegenstrategien, die trotz scheinbar aussichtsloser Lage Hoffnung aufkommen lassen, die IT-Produktion doch zumindest an einigen Stellen fairer gestalten zu können, etwa durch Bau teilfairer Geräte, Ranking von Firmen, Siegel, Gesetzesinitiativen, öffentlichen Protest, Bildungsarbeit und so weiter.

Zu Gunsten von Nachfragen und Diskussion haben wir das eine oder andere weggelassen. Immer wieder kommt man an einen Punkt wo eine Abwägung der Argumente und Ziele schwierig ist. Hier eine Meinung bilden zu können ist die Stärke einer Arbeitsgruppe gegenüber etwa einem Vortrag. Eine Bestätigung aus dieser Runde: Das FIfF sollte weiterhin und vor allem das Thema unter die Leute bringen.

Schade allerdings, dass es nur vier Teilnehmer gab, und da sind der Organisator und der Fuldaer Hiwi schon eingerechnet.

Die Folien schicke ich auf Anfrage gerne zu. Wer bei dem Thema auf dem Laufenden bleiben möchte, kann sich unserer Mailingliste anschließen: *http://lists.fiff.de/mailman/listinfo/fiff-fairit*

Sebastian Jekutsch ist FIfF-Mitglied aus Hamburg.
Kontakt: sj@fiff.de.

Faire Computer

Karin Kleinn, Britta Schinzel

Arbeitsgruppe: „Verantwortung in der Informatik“

(1) Brainstorming zu den Fragen

1. Welche durch Informatik (neu) geschaffenen Fakten sind gesellschaftlich ambivalent und problematisch und relevant für informatische Verantwortungsfragen? Was ist schädlich und wenn ja, warum?

2. Wie können InformatikerInnen diese Entwicklungen beeinflussen? Welche Aufgaben haben InformatikerInnen dabei? Wie können InformatikerInnen ihre Verantwortung wahrnehmen?

Beide Fragenkomplexe wurden bereits vermischt behandelt.

(2) Ergebnisse des 3-jährigen DFG-Projekts *Weltbilder in der Informatik* mit Bezug auf Verantwortung und Geschlecht

Karin Kleinn berichtete über das oben genannte Forschungsprojekt, in dem verschiedene Kategorien von auf die Informatik bezogenen Weltbildern von Informatik-Studierenden untersucht wurden, etwa Technikbilder, Berufsbilder, Menschenbilder, Entwickelnde und Benutzende, Realitätskonstruktion etc. Unter anderem lieferte das Projekt Ergebnisse zur Verantwortungsnahme und zu Geschlechterbildern. Dabei zeigte sich ein Einfluss des Studiums insofern, als Studierende zu Beginn des Studiums noch aus der Sicht der Nutzenden argumentieren und daher durchaus Verantwortung der Profession für informatische Produkte sehen, während Studierende im Hauptstudium die Seite gewechselt haben, ihre Verantwortung fast nur in der Erfüllung professioneller Anforderungen gegenüber Vorgesetzten und Auftraggebenden sehen, weitergehende moralische Anforderungen aber öfter auf Auftraggebende und Benutzende schieben. Sie argumentieren viel mit *dual use* für die Nutzungsverantwortung. Wenn die Rede auf militärische Anwendungen kommt, so erscheint ihnen dies eine einmalige binäre Entscheidung dagegen oder dafür. Mikroethische Fragen innerhalb der Software-Entwicklung sind nicht im Bewusstsein der Studierenden, ebenso wenig wie der Einfluss von Arbeitsklima und Arbeitshaltungen. Die Notwendigkeit, Nutzende zu integrieren, wird nur am Ende der Benutzungsschnittstelle gesehen.

(3) Zusammenbringen von (1) und (2), Diskussion dieser Ergebnisse und mögliche Maßnahmen

Die meisten Vorschläge bezogen sich auf die Lehre, ethische Grundbildung an der Schule, und ethische Fragen und IuG im Informatik-Unterricht.

- Lehrerausbildung: Vermittlungskompetenz entwickeln, zur Wiederverwendung Unterrichtsmaterialien entwickeln und in Berufsverbänden verbreiten, auf einheitliche Plattformen bringen, aber auch dezentrale Entwicklungen.

- Defiziten in der universitären Ausbildung begegnen.

Weiter wurde die Wichtigkeit von Öffentlichkeitsarbeit betont, den Kulturwandel in die öffentliche Wahrnehmung zu bringen, so wie dies zur technischen Überwachung teilweise bereits geschehen ist, Defizite dabei durchaus skandalisieren, um Rechtfertigungsdruck zu erzeugen.

Constanze Kurz, Britta Schinzel

Arbeitsgruppe: „Fallbeispiele zu Ethik und Verantwortung in der Informatik“

Im Rahmen der GI-Fachgruppe *Informatik und Ethik* wurden eine Reihe von Fallbeispielen entwickelt, welche an mehreren Hochschulen in Seminaren erprobt wurden. Einige davon sind in [1] veröffentlicht.

Die GI-Arbeitsgruppe veröffentlicht weiterhin regelmäßig im *Informatik Spektrum* Fallbeispiele unter der Rubrik *Gewissensbits*. Drei solcher Fallbeispielen wurden in dieser AG in drei Arbeitsgruppen durchgespielt, anschließend im Plenum der AG vorgestellt. Sie wurden besprochen und den Aspekten:

- Wer sind die Akteure?
- Welche ethischen Konflikte können auftreten?
- Was geschieht auf der Metaebene?

Dabei wurde auch jeweils an der Tafel eine Grafik zur Visualisierung der Beteiligten und ihrer Beziehungen untereinander angefertigt.

Das erste Fallbeispiele hieß: *Spyware*, dabei geht es um ein gutes Angebot zur Mitarbeit in einer Firma, die unter anderem Online-Werbung und Spyware herstellt; das zweite Fallbeispiel hieß *Kollateralschaden*. Hierbei geht es um die Veröffentlichung eines Urlaubsfotos aus der Famile in Facebook, ohne dass die Abgebildeten vorher gefragt wurden. Das dritte, Fallbeispiel, das aus Zeitgründen nicht mehr vorgeführt werden konnte, hieß *Anonymisierer*, wobei es um die (Nicht-)Erlaubnis geht, an einer Universität, *Tor*-Software zu benutzen und zu lehren.

Referenzen

[1] Debora Weber-Wulff, Christina Class, Wolfgang Coy, Constanze Kurz, David Zellhöfer: Gewissensbisse: Ethische Probleme der Informatik. [transcript]-Verlag 2009, Reihe Kultur und Medientheorie

Kai Nothdurft, Sylvia Johnigk

Arbeitsgruppe: „Cyberpeace“

In einem dreistündigen Workshop diskutierten insgesamt 15 Teilnehmende das Thema Cyberpeace. *Dabei wurden die bisher vom FIfF argumentierten Forderungen besprochen und auf dieser Basis das Thema* Cyberwarfare und friedenspolitische Antworten *weiter diskutiert und zusätzliche Forderungen entwickelt. Die Diksussion ist nicht abgeschlossen. Der momentane Stand wird im Folgenden wiedergegeben.*

Begriffsklärung

Zunächst wurde eine Abgrenzung der Begriffe *Cyberwar*, *Cyberwarfare*, *Cyberterror*, *Cybercrime*, *Cyber Espionage*, *Hacktivismus* vorgenommen. Einigkeit herrschte darüber, dass nicht alle Arten von Cyber-Angriffen als Kriegshandlungen eingestuft werden dürfen.

Unter *Cyberwarfare* wird von den Teilnehmenden des Arbeitskreises ein Angriff oder die Verteidigung gegen einen Angriff mittels IT auf ein IT-System verstanden, etwa in Form von Hacking-Attacken oder Malware. Um aber tatsächlich als *Cyberwar* zu gelten ist zusätzlich die Motivation und das Ausmaß des Schadens entscheidend. Man hat bisher nur von Krieg gesprochen, wenn es auch eine kinetische Wirkung einer Waffe gab. Für eine Kriegshandlung muss zudem mindestens eine der beteiligten Konfliktparteien ein Staat sein. Völkerrechtlich wird ein Konflikt erst bei einer vierstelligen Anzahl von Getöteten als Krieg eingestuft.

Medienhype?

Der Begriff *Cyberwar* erfuhr in den vergangenen Monaten in den Medien einen regelrechten Hype. Auf Sicherheitskonferenzen, Tagungen und in Regierungskreisen wird hektisch nach Lösungen gegen vermeintliche oder tatsächliche Bedrohungen gesucht. Das führt zu einer technischen und verbalen Aufrüstung, die eine gefährliche Rüstungsspirale in Gang gesetzt hat. Es wurde diskutiert, ob mit der Dauerpräsenz in den Medien bereits eine – möglicherweise sogar gewollte – Desensibilisierung der Öffentlichkeit und Gewöhnung an Cyberwarfare als legitime und normale Maßnahme staatlicher Sicherheitsstrategie einhergeht. Ein vergleichbarer Effekt ist bei der Informationsflut über Pannen in französischen Atomkraftwerken zu beobachten, wodurch kritische Störungen kaum noch auffallen.

Der AK diskutierte, inwieweit ein Cyberwar eine reale Bedrohung darstellt, ober ob es sich hier um Panikmache und Hysterie handelt. Es bestand der Eindruck, dass die Diskussion stark interessengetrieben von den Herstellern von IT-Sicherheitsprodukten und Sicherheitsbehörden geführt wird, und auf Seiten der Politik eine gewisse Ratlosigkeit über die richtige Strategie herrscht. Unabhängige Forschung zur Bedrohungslage, den militärischen Strategien oder dem Status von Cyberwaffen ist den Teilnehmenden weitgehend unbekannt oder technisch wenig fundiert. Eine Ausnahme bildet die Untersuchung des *Stuxnet*-Wurms. Da viele Informationen der militärischen Geheimhaltung unterliegen, ist die Recherche schwierig.

Der AK hält einen reinen Cyberwar für ein eher unrealistisches Szenario. Sehr viel wahrscheinlicher erscheint dagegen, dass Cyberwarfare vorbereitend oder als Unterstützungsmaßnahme

Eindrücke aus den Arbeitsgruppen, Fotos: FAI Fulda

begleitend zu einer allgemeinen kriegerischen Handlung eingesetzt wird.

Bemerkenswert ist, dass ausgerechnet die hoch entwickelten Industrieländer die verbale, strategische und technische Hochrüstung vorantreiben anstatt, zur Deeskalation beizutragen, obwohl gerade sie besonders anfällig für Cyberangriffe sind und dementsprechend besonders stark unter Cyberwarfare leiden würden.

Bestätigung und Erweiterung der FIfF Positionen

Der AK war sich einig, dass Deeskalation wichtig ist. Die bereits veröffentlichten Forderungen des FIfF[1] dazu erfuhren weitgehende Zustimmung.

Zur Rüstungskontrolle wurde vorgeschlagen, die Verbreitung von Exploits völkerrechtlich zu verbieten. Als wirksames Mittel wurde die Pflicht zur Offenlegung von Schwachstellen angesehen. Dadurch werden Cyberwaffen entschärft, die die Schwachstellen auszunutzen versuchen.

Das Attributierungsproblem

Im Konflikt um die georgische Provinz Südossetien wurde 2008 gezielt durch Cyberangriffe Kriegspropaganda und Irreführung betrieben, indem Kommunikationsstrukturen manipuliert und lahmgelegt wurden, u. a. durch Entstellung (*Defacement)* der Webseiten des Parlaments und des Außenministeriums von Georgien.

Nach einem Satz des Tragödiendichters Aischylos ist das erste Opfer des Krieges die Wahrheit. Dies gilt insbesondere für den Cyberwarfare. Da die Angriffe zunächst im virtuellen Raum stattfinden, sind ihre Wirkungen nur mittelbar wahrnehmbar. Dadurch sind Verdächtigungen und Behauptungen über angeb-

lich erfolgte Cyberangriffe nur schwer nachprüfbar. Von außen ist es schon schwierig festzustellen, ob überhaupt ein Angriff stattgefunden hat.

Das Problem verschärft sich dadurch, dass unter Umständen der Angreifer nicht eindeutig bestimmt werden kann. Selbst für die Angegriffenen, erst Recht aber für die Öffentlichkeit ist es schwierig nachzuvollziehen, wer den Angriff tatsächlich ausgeführt hat, also ihn einem konkreten Angreifer zuzuordnen. Aus der technischen Art eines Angriffs kann auch nicht immer auf die Motivation des Angreifers geschlossen werden, etwa ob es sich um eine Straftat oder einen kriegerischen Akt handelt. Dies erschwert eine angemessene politische Reaktion oder gar völkerrechtliche Sanktionierung.

Mit Forensik lassen sich zwar theoretisch Indizien und Spuren ermitteln, etwa durch Auswertung von Logdaten. Allerdings stehen viele durchaus vorhandene Daten kaum für eine Untersuchung zur Verfügung, wenn sie auf verschiedenen Systemen von verschiedenen Betreibern in unterschiedlichen Ländern gespeichert sind.

Um eine unabhängige, völkerrechtlich anerkannte Attributierung des Angriffs zum Aggressor vornehmen zu können, schlägt der AK vor, dass diese Daten über internationale Abkommen für transparente forensische Untersuchungen unter internationaler Aufsicht zugänglich gemacht werden, wenn behauptet wird, dass Cyberattacken stattgefunden haben und wenn der Angegriffene den Verdacht einer kriegerischen Motivation hegt und entsprechend politisch reagiert. Hier soll nicht einer weltumspannenden Vorratsdatenspeicherung das Wort geredet werden. Ein Aggressor wird ohnehin versuchen, soweit wie möglich seine Spuren zu verwischen und Daten zu löschen. Vielmehr sollen lediglich dann noch vorhandene Daten und Informationen ausschließlich für Vorfälle mit kriegsähnlichem Charakter völkerrechtlich legitimiert zusammengeführt und von unabhängigen Parteien idealerweise sogar öffentlich nachvollziehbar untersucht werden können.

Weiterführender Diskurs und Denkansätze im Arbeitskreis

Im Arbeitskreis wurden auch einige Aspekte diskutiert, zu denen die Teilnehmenden keine gemeinsame Sicht entwickeln konnten oder die nur angesprochen, aber nicht ausdiskutiert wurden, die aber eine wichtige Basis für die weitere Arbeit im FIfF bedeuten können:

1. Inwiefern sind durch Cyberwaffen zielgerichtete Angriffe (chirurgische Schläge) möglich, die damit in ihrer Wirkung eingrenzbar sind? Das Beispiel Stuxnet läßt an diesem Anspruch zweifeln. Der Stuxnet-Wurm wurde für ein sehr spezielles Ziel (die Urananreicherungsanlage in Natanz) entwickelt. Aufgrund eines Programmierfehlers ist er jedoch aus dem begrenzten Szenario ausgebrochen und wird inzwischen in modifizierter Form weiterverwendet.

2. Spielen beim Cyberwarfare nicht nur militärische Akteure mit? Cyberangriffe können nicht nur von militärischen Einheiten sondern auch von Cyberkriminellen, Wirtschaftsspionen, Terroristen, losen Hackergruppen, Scriptkiddies oder paramilitärischen Einheiten durchgeführt werden. Diese verschiedenen Kategorien von Angreifern verfügen über unterschiedliche Fertigkeiten und Schadpotenzial. Die Aktivitäten sind nicht unbedingt unter Cyberwarfare einzuordnen.

3. Entgrenzung: Ist ein Cyberkrieg unwahrscheinlich, weil der Angreifer sich auch selbst mit Cyberwaffen schädigt? Aufgrund der Globalisierung bestehen zwischen potenziellen Gegnern gegenseitige wirtschaftliche Abhängigkeiten.

4. Welche Kriegsszenarien mit welchen Gegnern sind möglich und wahrscheinlich? Im AK wurden verschiedenene Szenarien mit ihren Eintrittswahrscheinlichkeiten betrachtet: Wer greift wen an, beispielsweise die USA China, China die USA, Groß gegen Klein (wahrscheinlich?), Klein gegen Groß?

5. Die technische Machbarkeit von Angriffen und die Wahrscheinlichkeit der effektiven Ausnutzung wurden diskutiert am Beispiel eines Angriffs auf die Stromversorgung. Die grundsätzliche Anfälligkeit zeigte sich aktuell an den Auswirkungen des Wirbelsturms *Sandy*.

6. Besitzen die westlichen Industrienationen einen technologischen Vorteil, verfügt beispielsweise China über vergleichbare Fähigkeiten, einen Cyberwarfare zu führen, oder hat China den Westen bereits überholt?

7. Nordkorea verfügt laut eigenem Bekenntnis über eine Cyberwar-Einheit. Das Land ist de facto vom Internet abgeschnitten. Die wenigen offiziellen Seiten des Landes werden im Ausland gehostet. Lediglich die Nomenklatura hat wahrscheinlich Zugang zum Internet. Offizielle Stellen und wenige Personen verfügen über E-Mail-Adressen (in China), die laut Wikipedia streng reglementiert sind. Dennoch kam es angeblich bereits zu Angriffen des nordkoreanischen Geheimdienstes auf Südkorea, das Land mit nahezu der höchsten informationstechnischen Vernetzung weltweit. Nordkorea kann dort einen höheren Schaden anrichten, als Südkorea im umgekehrten Fall.[2]

8. Gibt es im Cyberwar Internet-Verbot für die Zivilbevölkerung? Wird das *Stay-Put*-Konzept der NATO, wonach die Zivilbevölkerung „in einer Krise und im Verteidigungsfall grundsätzlich zu Hause bleiben“ soll, damit die Kriegsführung „nicht durch umher vagabundierende, orientierungslos oder obdachlos gewordene Menschen behindert“[3] wird, auf den Cyberwar ausgeweitet? Denkbar wäre eine Einschränkung der Nutzung von Kommunikationsmitteln, wie das Internet für unabhängige Informationsbeschaffung, oder die Reservierung von Bandbreite für militärische Zwecke bei *Denial-of-Service*-Attacken auf Netzinfrastrukturen.

Ergebnisse des Arbeitskreises

Die bisherigen Forderungen des FIfF zu Cyberpeace wurden vom AK im Wesentlichen bestätigt. Als Ergebnis kamen aber zwei neue Forderungen hinzu, die das FIfF offiziell übernehmen soll. Der AK fordert:

- unabhängige Forschung zu Cyberwarfare zu intensivieren: Wichtige Aspekte sind dabei Empirie zum Status Quo der Cyberwarfare und die Erforschung politischer Wirkungen. Wir fordern eine Forschung, die unabhängig und frei ist von kommerziellen Interessen der Sicherheitsindustrie und des Militärs. Es muss eine kritische Auseinandersetzung mit der gesellschaftlichen und politischen Wirkung von Cyberwarfare stattfinden.

- die unabhängige und öffentliche Untersuchung von Cyberangriffen, um durch Transparenz dem Attributierungsproblem entgegenzuwirken. Damit soll vermieden werden, dass unter dem Vorwand eines Angriffs im Cyberspace ein konventioneller Krieg gegen beliebige Gegner politisch legitimiert werden kann, ohne das ein tragfähiger Nachweis erbracht wurde. Eine solche Behauptung in den Raum zu stellen, ist noch einfacher als die Behauptung, ein Gegner würde bereits über ein umfangreiches Waffenarsenal verfügen, das unschädlich gemacht werden muss. Die Behauptung ist jakaum widerlegbar ist.

Der AK schlägt folgende Gegenmaßnahmen zur Deeskalation und Abrüstung vor:

- Risikosenkung durch Dezentralisierung und Segregierung von IT-Systemen:
  Der Trend, immer mehr Systeme miteinander zu vernetzen und an das Internet anzubinden, erhöht deren Verletzlichkeit und damit das Gesamtrisiko von Cyberangriffen. Die Informationsgesellschaft wird somit als potenzielles Ziel immer attraktiver. Der Risikoeinsatz in diesem Poker gleicht einem *All-in.* Dezentralisierung und Segregierung können zur Deeskalation und Abrüstung beitragen.

- *Graceful Degradation* (Fehlertoleranz):
  IT-Systeme müssen robuster als bisher konzipiert und implementiert werden. Dadurch wird der potenzielle Schaden bei einer Cyberattacke gesenkt.

- Investition in defensive Technik und Maßnahmen:
  Wie können Frühwarnsysteme aussehen, wie kann man Angriffe erkennen, abwehren? Welchen Nutzen haben IPS, Netzwerkscanner, Analyse, SIEM-Systeme, und wie können diese Techniken allgemein zur Verfügung gestellt werden, etwa in Form von Open-Source-Produkten?

- Demystifizierung von Hacking:
  In der öffentlichen Wahrnehmung erscheint das Durchführen von Angriffen auf IT-Systeme als schwieriger als es tatsächlich ist. Die Sicherheit von Systemen wird überschätzt. Risiken werden nicht realistisch eingeschätzt und vielfach wird entsprechend unvorsichtig agiert. Bei IT-Projekten und der privaten Vorsorge wird der Sicherheit zu wenig Gewicht beigemessen. Durch Aufklärung kann ein besseres Risikobewusstsein erzielt werden, wodurch Vorsichtsmaßnahmen vermehrt umgesetzt und die Verletzlichkeit insgesamt gesenkt werden. Hacking zur Aufdeckung von Schwachstellen dient der Sicherheit.

- Dem Hype um Cyberwarfare entgegenwirken:
  Die Einschätzung der Bedrohungslage erfolgt fast immer mit einem *Worst-Case*-Szenario. Dies verschärft den Rüstungswettlauf und ebnet einer restriktiven und Demokratie-feindlichen Sicherheitsdoktrin den Weg, die die Bevölkerung als Sicherheitsrisiko betrachtet.

- Exportkontrolle für Überwachungstechnologie:
  Überwachungstechnologie lehnen wir generell ab. Zu einem Verbrechenswerkzeug wird sie, wenn sie in repressiven Gesellschaften zum Einsatz kommt. Deep-Packet Inspection Tools ermöglichen Zensur. Dadurch wird Propaganda ermöglicht und freie Kommunikation verhindert. Die Bevölkerung kann leichter manipuliert und aufgehetzt werden. Das folgende Beispiel zeigt, dass eine restriktive Durchsetzung eines Exportverbots notwendig ist: Oppositionelle in Bahrain wurden Opfer staatlicher Gewalt, da sie mittels deutscher Überwachungstechnologien ausgespäht werden. Der eigentliche Skandal ist, dass das Unternehmen *Gamma* behauptet, ihm sei die Technik auf einer Messe entwendet worden.[4] Das BKA erwägt das *Gamma*-Produkt *Finfisher* als Ersatz für den Bayerntrojaner zu kaufen.

Der Arbeitskreis hat gezeigt, dass die Diskussion noch längst nicht abgeschlossen ist. Das Thema wird das FIfF weiter beschäftigen: Es wurde eine Mailingliste eingerichtet[5], die zusammen mit dem Wiki[6] dafür genutzt werden kann. Interessierte sind herzlich eingeladen sich zu beteiligen.

Anmerkungen

1 *http://fiff.de/publikationen/fiff-kommunikation/fk-2012/fk-1-2012/fk-1-2012-cyberwarfare/view*
2 *http://www.zeit.de/digital/datenschutz/2011-08/cyberwar-korea*
3 *Zu Stay put siehe u. a.: http://www.spiegel.de/spiegel/print/d-13520723.html http://www.bildergalerie-diepholz.de/anlage_liebenau/html/das_szenario.html http://www.fritzstavenhagen.de/tl_files/pdf_word/alles_unter_kontrolle.pdf*
4 *http://www.heise.de/security/meldung/Trojaner-made-in-Germany-spioniert-in-Bahrain-1652460.html*
5 *CyberPeace@lists.fiff.de*
6 *http://wiki.fiff.de/Cyberwarfare*