H 7625

# FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

28. Jahrgang 2011 Einzelpreis: 7 EUR

**4/2011 – Dezember 2011**

# Killerroboter, Cyberwar & Co.


ISSN 0938-3476

**• #0zapftis • Urban Mining • EuroDIG • IT-Genossenschaft •**

FIfF Kommunikation

Titelbild: defwheezer (CC BY-NC-SA 2.0)
http://www.flickr.com/photos/defwheezer/999161292

*Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.*

# Inhalt

Ausgabe 4/2011

inhalt

## Schwerpunkt »Killerroboter, Cyberwar & Co.«

**26** Mahnen und Aufklären – Information Warfare und FIfF
*- Ute Bernhardt*

**27** Gehören Killerroboter vor ein Kriegsgericht?
*- Hans-Jörg Kreowski*

**30** Die Himmelsstürmer
*- Eric Töpfer*

**35** Wie eine renommierte Forschungsinstitution zum effizienteren Töten beiträgt
*- Otto Reger*

**38** Cyber-Krieg oder Cyber-Sicherheit – wächst aus Abhängigkeiten auch die Einsicht?
*- Ingo Ruhmann*

**43** Master of Peace Studies
*- Ute Bernhardt*

**44** Für eine zivilisierte Bildung und Wissenschaft
*- Ralf E. Streibl*

## FIfF e.V.

**04** Brief an das FIfF – „#0zapftis“
*- Stefan Hügel*

**05** Kurzbericht von der FIfF-Jahrestagung 2011 „Dialektik der Informationssicherheit“
*- Dagmar Boedicker, Stefan Hügel*

**06** Protokoll der Mitgliederversammlung 2011

**08** How To FIfF – Teil 2
*- Raffael Rittmeier*

**03** Editorial
*- Hans-Jörg Kreowski, Stefan Hügel*

## Aktuelles

**08** Staatlicher Hausfriedensbruch
*- Kommentar von Dagmar Boedicker*

**09** „It's not the business of the customer …" Höchst persönlicher Nachruf auf Steve Jobs
*- Dietrich Meyer-Ebrecht*

**10** Log 4/2011
*- Stefan Hügel*

**15** Urban Mining
*- David Koschnick*

**19** EuroDIG: Im Wechselbad von Zielkonflikten
*- Wolf Ludwig*

**22** Eine IT-Genossenschaft
*- Dagmar Boedicker*

**24** AC3 – der AKtiVCongreZ
*- Stefan Hügel*

**25** Zur Existenzberechtigung des Verfassungsschutzes
*- Erklärung des FIfF e.V.*

## Retrospektive

**51** Informatik und Militär: Zusammen in den Abgrund
*- Hans-Jörg Kreowski*

## Rubriken

**54** Lesen – Neues für den Bücherwurm

**59** Impressum/Aktuelle Ankündigungen

**60** SchlussFIfF

# Editorial

Von den Anfängen der Computertechnik und Informatik bis heute werden deren Errungenschaften militärisch genutzt. Ihre vielfältige und umfassende Verwendung in der Rüstungstechnik einerseits und bei der Planung und Organisation von Kriegen andererseits hat völlig neue Formen der Kriegsführung ermöglicht und die Bedrohung durch Kriege um einige perfide Komponenten erweitert. Ein Beispiel sind Killerroboter, die programmiert töten und dabei zusätzlich die Illusion nähren, die eigenen Soldaten könnten verschont bleiben. Ein anderes Beispiel ist das, was unter den schillernden Begriff des *Cyberwar* fällt: Propaganda, Spionage, Sabotage mit Mitteln der Informations- und Kommunikationstechnik, um militärische und vor allem auch zivile Infrastruktur des Gegners lahmzulegen. Der Schwerpunkt in diesem Heft ist dem Themenkomplex *Killerroboter, Cyberwar & Co.* gewidmet, und es sollen neue Tendenzen der Verflechtung von Informatik und Rüstung zusammengestellt und kritisch erörtert werden.

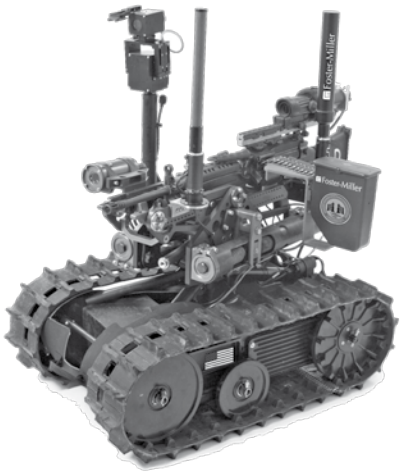
Den Anfang bildet der Beitrag von *Ute Bernhardt*: *Mahnen und Aufklären – Information Warfare und FIfF*, in dem sie einen kurzen Abriss liefert, wie sich das FIfF seit der Gründung mit der Verquickung von Militärwesen und Informatik auseinandersetzt.

Die nächsten drei Beiträge lassen sich dem Thema Killerroboter zuordnen. *Hans-Jörg Kreowski* stellt die Frage: *Gehören Killerroboter vor ein Kriegsgericht?* Er verneint aus fachlicher Sicht, dass autonome Killerroboter, wie sie zukünftig geplant sind, das Kriegsvölkerrecht beachten können, und fordert, dass sie deshalb geächtet werden sollten. *Eric Töpfers* Beitrag *Die Himmelsstürmer* geht mit vielen interessanten Einzelheiten auf die Frage ein, *wie die Drohnenlobby ihren Kriegsrobotern den zivilen Luftraum öffnet.* Schließlich stellt *Otto Reger* das *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung* vor, wobei er vor allem darauf eingeht, *wie eine renommierte Forschungsinstitution zum effizienteren Töten beiträgt.*

Der folgende Beitrag mit dem Titel *Cyber-Krieg oder Cyber-Sicherheit* stammt von *Ingo Ruhmann*. Er geht detailliert und differenziert auf das Phänomen *Cyberwar* ein und fragt sich: *Wächst aus Abhängigkeiten auch die Einsicht?*

Die letzten Beiträge des Schwerpunkts behandeln den Themenkomplex der friedensorientierten Bildung. *Ute Bernhardt* informiert kurz über den Studiengang *Master of Peace Studies*, der von 2001 bis 2010 an der FernUniversität Hagen lief. *Ralf E. Streibl* plädiert *Für eine zivilisierte Bildung und Wissenschaft*: „Um echten Frieden zu schaffen, ist Friedensfähigkeit notwendige Voraussetzung – hieran zu arbeiten ist eine große Herausforderung und zentrale Aufgabe für Bildung und Wissenschaft."

Darüber hinaus passt die Retrospektive zum Schwerpunkt. Hans-Jörg Kreowskis Beitrag *Informatik und Militär – Zusammen in den Abgrund* aus dem Tagungsband der 3. FIfF-Jahrestagung 1986 in Berlin zeigt, dass sich an der Verflechtung von Informatik und Rüstung gar nicht so viel geändert hat. Es klang vor 25 Jahren vielleicht dramatischer und bedrohlicher, weil es vielfach um Massenvernichtungswaffen ging und sich zwei Weltmächte feindlich gegenüberstanden.



Der aktuelle Teil beginnt mit einem der wohl größten innenpolitischen Skandale der letzten Zeit: dem vom Chaos Computer Club enttarnten Staatstrojaner, dessen Fähigkeiten offenbar weit über das verfassungsmäßig erlaubte hinausgingen. *Staatlichen Hausfriedensbruch* nennt das *Dagmar Boedicker*; sie nimmt engagiert dagegen Stellung. *It's not the business of the customer …* überschreibt *Dietrich Meyer-Ebrecht* seinen höchst persönlichen Nachruf auf Steve Jobs.

Den weiteren *Ereignissen, Störungen und Probleme der digitalen Gesellschaft* widmet sich *Stefan Hügel* wie immer im *Log 4/2011* – es kann wohl nicht mehr überraschen, dass wieder einiges zusammen gekommen ist.

In seinem Beitrag *Urban Mining* beschreibt *Thomas Koschnick* den nachhaltigen Umgang mit bereits verwendeten Ressourcen und gesammelten Abfällen aus unserer urbanisierten Gesellschaft, bei dem Städte nicht nur aus Verbrauchersicht betrachtet, sondern auch als Quelle wertvoller Ressourcen gesehen werden, die genutzt und wiederverwertet werden können. *Wolf Ludwig* beschreibt das *Wechselbad von Zielkonflikten*, das die Verständigung über Regeln im Netz begleitet und das im regelmäßig stattfindenden *EuroDIG* – European Dialogue on Internet Governance – aufgelöst werden soll.

*Kann ein genossenschaftlich organisiertes Unternehmen funktionieren?*, fragt *Dagmar Boedicker*, und beantwortet die Frage anhand der *7-it eG* aus München. Danach folgt ein Kurzbericht vom dritten *AKtiVCongreZ*, dem Treffen netzpolitisch Aktiver vom 7.-9. Oktober in Hamburg.

In der Rubrik *Lesen* haben wir uns dieses Mal zwei Veröffentlichungen angeschaut: Das erste ist – passend zum Schwerpunkt – das Buch *Cyberwar – das Internet als Kriegsschauplatz* von *Sandro Gaycken*. Dazu hat *Britta Schinzel* den Sammelband *Informatik und Gesellschaft – Verflechtungen und Perspektiven* von *Hans-Jörg Kreowski* unter die Lupe genommen.

Wir wünschen unseren Leserinnen und Lesern eine anregende und interessante Lektüre – und viele neue Erkenntnisse und Einsichten.

*Hans-Jörg Kreowski und Stefan Hügel*
*für die Redaktion*

**Brief an das FIfF**


# #0zapftis

*„Sie berufen sich hier pausenlos aufs Grundgesetz /*
*sagen Sie mal / sind Sie eigentlich Kommunist?"*
Franz Josef Degenhardt (1931-2011)

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

das Irritierende ist, dass es mich nicht mehr besonders überrascht …

Die Nachricht verbreitete sich schnell auf dem AKtiVCongreZ in Hamburg: Der Chaos Computer Club habe einen Staatstrojaner analysiert: „Der kann alles."

*Alles* heißt: Quellen-Telekommunikationsüberwachung (verfassungsgemäß). Beliebige Funktionalität nachladen (nicht verfassungsgemäß). Damit beliebige Daten auf dem infiltrierten Rechner lesen (nicht verfassungsgemäß) und schreiben (auch nicht verfassungsgemäß). Screenshots anfertigen und an die Behörden übermitteln (nicht verfassungsgemäß). Von der offenbar katastrophal mangelhaften Sicherheit der Software gar nicht zu reden.

Nach kurzem Rätselraten über den Ursprung des Trojaners waren es zunächst die bayerischen Behörden: das Landgericht Landshut hatte vor einiger Zeit über eine Quellen-TKÜ zu befinden (rechtmäßig), die mit 30-sekündlicher Übermittlung von Screenshots verknüpft wurde (nicht rechtmäßig). Aus dem bayerischen Innenministerium verlautete zu dem Urteil, man vertrete dort eben eine andere Rechtsauffassung.

Die bayerischen Behörden waren aber offenbar nicht die einzigen, die sich dieser oder vergleichbarer Software bedienten. Ein Bundesland nach dem anderen musste einräumen, dass es Online-Durchsuchungen durchgeführt habe. Auch einige Bundesbehörden waren nicht zimperlich.

Am 27. Februar 2008 urteilte das Bundesverfassungsgericht, dass es ein Grundrecht gebe auf die *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* – auch bekannt als *Computer-Grundrecht*. In den 70ern wurden einfache Postboten aus dem Staatsdienst entfernt, wenn sie nach Auffassung des Verfassungsschutzes nicht die Gewähr dafür boten, jederzeit für die freiheitlich-demokratische Grundordnung einzutreten. Wie viele verfassungswidrige Gesetze muss ein Parlament beschließen, wie viele verfassungswidrige Handlungen müssen die Verantwortlichen staatlicher Organe vornehmen, um sich dem Verdacht auszusetzen, die verfassungsmäßige Ordnung beseitigen zu wollen?

Und die zuständigen Behörden? „Was für verfassungsrechtliche Skelette tanzen denn noch in den Kellern der deutschen Sicherheitsbehörden, wenn ein so massiver Verstoß wie der Staatstrojaner eine Kleinigkeit sein soll?" fragte Pavel Meyer von der Piratenpartei in der *Frankfurter Allgemeinen Zeitung* zu den Verharmlosungsversuchen von Regierungen und Behörden. Der Bundesinnenminister hielt es dagegen nicht einmal für nötig, zur Bundestagsdebatte zu einem der größten innenpolitischen Skandale der letzten Zeit zu erscheinen. Zu Recht wurde er dafür in der Presse scharf kritisiert.

Zäh gestaltet sich offenbar die Arbeit in der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags. Nachdem man die Hälfte der ersten Sitzung nach der Sommerpause mit einer weitgehend formalistisch geführten Debatte verbrachte, ob Gutachten zu den Themen Urheberrecht und Netzneutralität beauftragt werden sollten oder nicht (sie wurden nicht in Auftrag gegeben), kam dann zumindest der Text zu Netzneutralität zur Abstimmung, der im Juli verschoben worden war. Dass der beschlossene Text mit Sondervoten gespickt ist, sollte nicht überraschen – zu weit auseinander liegen hier offensichtlich die Wertvorstellungen von Koalition und Opposition. Der CDU-Abgeordnete Peter Tauber wunderte sich während der Debatte darüber, dass die Opposition plötzlich staatliche Regulierung fordern würde, die sie sonst – bei Vorratsdatenspeicherung und Netzsperren – vehement ablehne. Die Frage ist wohl einfach, ob man *oben* reguliert – bei Behörden und Konzernen – oder *unten* – bei Bürgerinnen und Bürgern, wie es Konservative gerne fordern.

Gerade ist der Höhepunkt des FIfF-Jahres zu Ende gegangen: die diesjährige Jahrestagung in München. Neben einer spannenden Tagung, die sich vor allem um die Themen Sicherheit und Datenschutz drehte – einen Kurzbericht gibt es in diesem Heft, das Tagungsheft wird dann als Ausgabe 1/2012 Ende März 2012 erscheinen – wurde auch turnusgemäß der Vorstand neu gewählt. Für meine Wiederwahl als Vorsitzender und das mir damit entgegengebrachte Vertrauen bedanke ich mich herzlich. Stellvertretender Vorsitzender ist in den kommenden zwei Jahren Dietrich Meyer-Ebrecht, neu in den Vorstand gewählt wurde unsere Geschäftsführerin Ingrid Schlagheck – beiden zu ihrer Wahl herzlichen Glückwunsch. Nicht mehr zur Wahl standen Carsten Büttemeier und Julia Stoll, die damit aus dem Vorstand ausscheiden. Ich danke beiden herzlich für ihr Engangement und die geleistete Arbeit.

Ein letztes Wort: Stört es eigentlich jemanden, wie über die jüngste Finanzkrise debattiert wird? *Man müsse das Vertrauen der Finanzmärkte zurückgewinnen.* Frei nach Bertolt Brecht, „… daß das Volk das Vertrauen der Finanzmärkte verscherzt habe. Und es nur durch doppelte Arbeit zurückerobern könne. Wäre es da nicht doch einfacher, die Finanzmärkte lösten das Volk auf und wählten ein anderes?"

Gegen die Einrichtung des Sondergremiums, das stellvertretend für den Bundestag über die Vergabe von Zahlungen aus dem

Euro-*Rettungsschirm* entscheiden soll, wurde vom Bundesverfassungsgericht gerade eine einstweilige Verfügung erlassen. Erneut wird damit ein Bundestagsbeschluss – zumindest vorläufig – vom Verfassungsgericht verworfen. Das Irritierende ist, dass es mich nicht mehr besonders überrascht.

Ah, und noch etwas - schrieb ich gerade „größter innenpolitischer Skandal"? Gerade wurden zwei Männer tot aufgefunden, die dem Anschein nach – gemeinsam mit einer Komplizin – für eine Reihe rechtsextremer Morde in den letzten zehn Jahren verantwortlich sind. Das geschah anscheinend weitgehend unbehelligt von Polizeibehörden und Verfassungsschutz – während gleichzeitig jedes brennende Auto mit aller Härte des Gesetzes als „Linksterrorismus" verfolgt wird. Oder wie es Twitterer *haekelschwein* formuliert: „Um als Terrorist zu gelten, müssen Rechte 13 Jahre bomben und morden, Linke ein Auto demolieren und Muslime eine Casio-Uhr tragen."

Das Irritierende ist, dass es mich nicht mehr besonders überrascht.

Mit FIfFigen Grüßen

*Stefan Hügel*



**Dagmar Boedicker, Stefan Hügel**

# Dialektik der Informationssicherheit

## Jahrestagung des FIfF in Kooperation mit der Hochschule München

*Vom 11. bis 13. November 2011 fand die diesjährige Jahrestagung des FIfF in Kooperation mit der Hochschule München statt.*

Unter dem Motto *Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit* trafen sich Expertinnen und Experten aus Wissenschaft, Wirtschaft und Technik mit interessierten Bürgerinnen und Bürgern, um sich von Freitagabend bis Sonntagvormittag mit der Sicherheit von Information und Daten auseinanderzusetzen.

In allen Bereichen der Gesellschaft nimmt der Rechnereinsatz laufend zu; das Internet ist nicht nur für Industrie, Handel und Behörden, sondern auch für den Privatbereich zu einem zentralen Teil der Infrastruktur geworden. Damit ist die Sicherheit der Informationen wichtiger als je zuvor; aber sie ist durch mächtige Interessen bedroht. Auf allen Ebenen entstehen Konflikte.


Der Bayerische Landesbeauftragte für den Datenschutz, *Dr. Thomas Petri*, beleuchtete in seinem Einführungsvortrag die Vorratsdatenspeicherung aus EU-rechtlicher und verfassungsrechtlicher Perspektive. Er stellte dabei den Weg der Vorratsdatenspeicherung dar: von der mehrmaligen Ablehnung durch den Bundestag, zuletzt im Februar 2005, über die EU-Richtlinie 2006, deren Umsetzung in nationales Recht 2007 und die Ablehnung durch das Bundesverfassungsgericht 2010 bis hin zur heutigen Debatte um Wiedereinführung, Quick-Freeze und Quick-Freeze-Plus. Anschließend diskutierten *Constanze Kurz*, Sprecherin des *Chaos Computer Club*, *Enno Rey* von der IT-Sicherheitsfirma *ERNW*, *Michael George*, bayerischer Verfassungsschützer im Bereich Wirtschaftsspionage, *Thomas Petri* und *Rainer Gerling*, IT-Sicherheits- und Datenschutzbeauftragter der *Max-Planck-Gesellschaft*. Sie behandelten die Wechselwirkungen der Sicherheitsaspekte Anonymität, Integrität und Vertraulichkeit an konkreten Beispielen aus dem privaten Bereich der Bürger, aus der Wirtschaft und aus der Arbeit staatlicher Einrichtungen. Wie nicht anders zu erwarten, ergab sich eine lebhafte Diskussion, in der unterschiedliche Wertvorstellungen, unterschiedliche Ziele und unterschiedliche Vorstellungen politischen Handelns aufeinandertrafen.

Am Samstag wurden Einzelaspekte vor allem der Datensicherheit und des Datenschutzes in gut besuchten und informativen Arbeitsgruppen vertieft, wie:

- Mobile Datenträger: Wenn Daten das Unternehmen verlassen,
- Data-Mining im Internet,
- „Facebook & Co und meine Daten im WWW",
- kritische Infrastrukturen und kritische Informationsinfrastrukturen.

Außerdem gab es Arbeitsgruppen zu:

- EU-Sicherheitspolitik und -forschung,
- „Faire Computer? Gibts das?“,
- Rüstung und Informatik: „Killerroboter, Cyberwar & Co“ (hätte beinahe wegen Überfüllung geschlossen werden müssen),
- Perspektiven einer europäischen Zusammenarbeit netzpolitischer Gruppen.

Die Sicherheitsbeauftragte eines DAX-Konzerns, *Monika Hansmeier*, schilderte anschließend in ihrem Vortrag die Fragen der Sicherheit, die in einem Großkonzern zu berücksichtigen sind – von der *Security Awareness* über organisatorische Vorkehrungen bis hin zu technischen Maßnahmen.

Anschließend zeigte das FIfF in der Münchner Erstaufführung den Film *Behind the Screen – das Leben meines Computers*. In diesem vom FIfF unterstützten Film wird eindringlich dargestellt, welche Auswirkungen die IT-Industrie im globalen Süden hat: Umweltschäden, Gesundheitsgefährdung bei Menschen und Zerstörung wirtschaftlicher Infrastrukturen sind der Preis, den andere für unseren informationstechnischen Fortschritt bezahlen müssen.

Am nächsten Morgen zeigte der FIfF-Studienpreisträger 2010, *Phillip Brunst*, in seinem sehr anschaulichen Vortrag die Konflikte zwischen Anonymität, Integrität und Vertraulichkeit auf der einen und Strafverfolgung auf der anderen Seite. Er ging dabei detailliert auf die Überwachung von Bestands-, Verkehrs- und Inhaltsdaten ein. Sowohl über die technischen Rahmenbedingungen als auch über die einschlägigen gesetzlichen Regelungen gab er einen Überblick, der sich zu einem Rahmen der digitalen Überwachung verdichtete, in den man aktuelle Themen wie Vorratsdatenspeicherung und Online-Durchsuchung einordnen kann.

In einer Begleitausstellung mit Ständen, Videos und Poster-Sessions ging es um Themen wie *Security Awareness*, Organisationen, Produkte und Sponsoren der Tagung. Mitarbeiterinnen und Mitarbeiter der Humboldt-Universität zu Berlin wiesen auf das immer geringer werdende Lehrangebot im Bereich *Informatik und Gesellschaft* hin, und forderten die Tagungsteilnehmer auf, Lehrangebote und -wünsche für einen virtuellen Studiengang einzureichen.

Den Ausklang bildete wie gewohnt die Mitgliederversammlung des FIfF, bei der in diesem Jahr auch der neue Vorstand gewählt wurde (siehe das Protokoll im Anschluss).

In Summe war es wieder eine gelungene Tagung und ein wahrer Höhepunkt des FIfF-Jahres. Die Jahrestagung 2012 wird in Fulda vom 9. bis 11. November 2012 stattfinden – freuen wir uns darauf!

# Mitgliederversammlung des FIfF

# München, Hochschule München, 13.11.2011, 11:15-15:55 Uhr

## – Beschlussprotokoll –

Sitzungsleitung: Stefan Hügel als Vorsitzender des FIfF

1. **Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung**
   Zur Versammlung ist ordentlich eingeladen worden und diese ist dadurch beschlussfähig.
   Das Protokoll führt: Jens Rinne

2. **Beschlussfassung über Tages- und Geschäftsordnung**
   Tages- und Geschäftsordnung wird von den Anwesenden in bekannter Form genehmigt

3. **Bericht des Vorstands (einschl. Kassenbericht)**
   Stefan Hügel berichtet über die Vorstandsarbeit in 2011 und den Haushalt 2011.
   Dabei werden keine Beschlüsse gefasst.

4. **Bericht der Kassenprüfer**
   Für die am 27.06.2011 in Bremen durchgeführte Kassenprüfung berichtet Kurt Fussangel der MV. Aus dem Kassenprüfungsprotokoll: „Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen.“ (Derzeitige Kassenprüfer: Michael Ahlmann, Kurt Fussangel und Gernot Lucks)
   Dabei werden keine Beschlüsse gefasst.

*Mitgliederversammlung, Foto: Dagmar Boedicker*

**5. Diskussion der Berichte**
Es werden keine Beschlüsse gefasst. Die MV dankt der engagierten, sehr gut strukturierten Kassenprüfung.

**6. Entlastung des Vorstands**
Die Entlastung des Vorstands wurde aus der MV vorgeschlagen.
Der Vorstand wird einmütig bei 9 Enthaltungen entlastet.

**7. Festlegung der Wahlleitung**
Die MV bestimmt einmütig bei einer Enthaltung Friedrich Strauß als Wahlleitung. Friedrich Strauß übernimmt die Sitzungsleitung und stellt fest, das 31 stimmberechtigte Mitglieder anwesend sind.

**7.1 Wahl des neuen Vorstands**

**Wahl der/des Vorstandsvorsitzenden:**
Vorschlag: Stefan Hügel

gültige Stimmen: 24
davon: ja: 24
nein: 0
enthalten: 0

**Stefan Hügel** ist gewählt und nimmt die Wahl an.

**Wahl der/des stellvertretenden Vorstandsvorsitzenden:**
Vorschläge: Jens Rinne und Dietrich Meyer-Ebrecht

| | 1. Wahlgang | 2. Wahlgang |
|---|---|---|
| **abgegeben** | 24 | 24 |
| **Enthaltungen** | 3 | 2 |
| **Ungültig** | 1 | 0 |
| **Jens Rinne** | 10 ja | 9 ja |
| **Dietrich Meyer-Ebrecht** | 10 ja | 13 ja |

**Dietrich Meyer-Ebrecht** ist im 2. Wahlgang gewählt und nimmt die Wahl an.

**Wahl der Beisitzerinnen und Beisitzer:**

Stimmberechtigt: 27

| Vorschläge | ja | nein | enth. |
|---|---|---|---|
| **Jens Rinne** | 23 | 0 | 2 |
| **Sylvia Johnigk** | 22 | 0 | 3 |
| **Raffael Rittmeier** | 22 | 0 | 3 |
| **Kai Nothdurft** | 24 | 0 | 1 |
| **Britta Schinzel** | 20 | 1 | 4 |
| **Hans-Jörg Kreowski** | 24 | 0 | 1 |
| **Ingrid Schlagheck** | 18 | 3 | 4 |

Alle Kandidierenden sind gewählt und alle sind anwesend und nehmen die Wahl an.

**8. Neuwahl der Kassenprüfer**
Die MV wählt Kurt Fussangel (24 ja/0 nein/0 enth.), Michael Ahlmann (23/0/1), Gernot Lucks (19/3/2) und Klaus Lüttich (23/0/1 : zugestimmt) vorbehaltlich der Zustimmung der nicht anwesenden Kandidaten zu den neuen Kassenprüfern des FIfF.

*Nach der MV haben die gewählten Kassenprüfer die Wahl angenommen.*

Stefan Hügel übernimmt als Vorsitzender des FIfF die Sitzungsleitung.

**9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen**
Es werden keine Beschlüsse gefasst.

**10. Berichte aus den Regionalgruppen**
Es werden keine Beschlüsse gefasst.

**11. Anträge an die Mitgliederversammlung**
Der MV liegen keine Anträge vor.

**12. Verschiedenes**
Es werden keine Beschlüsse gefasst.
Die Anwesenden danken für die tolle Organisation dieser Jahrestagung.

**13. Genehmigung des Protokolls**
Das Protokoll wird einstimmig genehmigt.

München, den 13. November 2011
Protokoll: Jens Rinne

*Der neue Vorstand (ohne Ingrid Schlagheck)*
*Foto: Dagmar Boedicker*

**Raffael Rittmeier**

# How To FIfF

## Teil 2: Initiativen und Arbeitsgruppen, -kreise, -kringel, -punkte

In Teil 1 von *How To FIfF* habe ich die FIfF-Regionalgruppen beschrieben. Inhaltliche Themen haben aber in der Regel keine regionalen Grenzen. In Arbeitskreisen oder Arbeitsgruppen schließen sich deshalb Menschen überregional zusammen, die sich zu einem bestimmten Themengebiet austauschen und dazu arbeiten möchten. So soll sich die inhaltliche Arbeit des FIfF gestalten – im Idealfall. Gibt es keine Arbeitsgruppen, dann bleibt die Arbeit an Einzelnen hängen, nicht selten aus dem Vorstand. Da der Vorstand die vielfältigen Themen nicht allein bearbeiten kann (und soll), sei hiermit auf die Wichtigkeit der Arbeitskreise und -gruppen hingewiesen. Die Ziele und die Organisationsform eines AK oder einer AG können sehr unterschiedlich sein. Häufig gibt es auf den Jahrestagungen Impulse zur Gründung einer kontinuierlichen AG. Wichtig sind die Kommunikation und Öffentlichkeitsarbeit, schließlich sollen Andere sich anschließen oder später auf die erarbeiteten Ergebnisse aufbauen können. Die Ergebnisse können auf der Webseite *fiff.de* und in der FIfF Kommunikation veröffentlicht werden. Eventuell kommen so viele Informationen zusammen, dass eine eigene Broschüre veröffentlicht werden kann (wie zuletzt die zweite Broschüre zur elektronischen Gesundheitskarte: *fiff.de/egk*). Zur Unterstützung der Arbeit und Kommunikation können Mailinglisten eingerichtet und das Wiki genutzt werden *(wiki.fiff.de)*. Die Geschäftsstelle und der Vorstand stehen bereit Interessierte zu unterstützen. Dafür haben wir folgende Themengebiete zusammengefasst und verantwortliche Kontaktpersonen benannt:

- Arbeit
- Datenschutz, Überwachung, Kontrolle
- Frieden
- Bildung, Gesundheit, Soziales, Umwelt
- Gender
- Informationsgesellschaft, IT-Politik, IT-Recht
- IT-Sicherheit, Verletzlichkeit
- Verantwortung von InformatikerInnen, „Informatik und Gesellschaft“ in der Lehre

Den Kontakt kann unsere Geschäftsstelle herstellen: *fiff@fiff.de.*

**Der Kommentar**

# Staatlicher Hausfriedensbruch

*Es ist ungeheuerlich! Unser Grundgesetz, geschaffen nach den Erfahrungen einer Diktatur und mühevoll verteidigt vom Verfassungsgericht, kann uns Bürgerinnen und Bürger nicht mehr vor Eingriffen des Staates schützen. Nicht gegen einen bayrischen Innenminister mit der unerschütterlichen Gewissheit, dass nichts an diesem Trojaner grundrechtsverletzend sei. Nicht gegen Sicherheitsbehörden, die beschaffen, was Software-Buden produzieren, ohne sich einen Teufel darum zu scheren, wie und von wem ihre Produkte eingesetzt werden. Wissen sie alle nicht, was sie tun? Oder machen sie, was sie wollen?*

Wir danken Euch aus tiefstem Herzen, liebe HacktivistInnen vom Chaos Computer Club, die getan haben, was ein BSI hätte tun sollen, oder irgendeine andere staatliche Organisation! Was sind das nur für Institutionen, die entweder so inkompetent und dumm oder so zynisch sind, dass sie wie ein Elefant im Porzellanladen über Bürgerrechte hinweg trampeln und dann die verdutzte Unschuld markieren?

Compliance und ähnliche Symbolbegriffe, Gesetze und Verordnungen, all das soll uns einreden, ein fürsorglicher Staat kümmere sich um Sicherheit und Wohlergehen seiner Bürger. Die Realität sieht anders aus, wie der CCC feststellen musste: „Aufgrund von groben Design- und Implementierungsfehlern entstehen außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern, die auch Dritte ausnutzen können.“ Es wäre lächerlich, wenn es nicht so traurig wäre: Da öffnen unsere staatlichen Beschützer ausländischen Diensten oder dem organisierten Verbrechen mit einem Danaergeschenk an die nichtsahnenden Bundesbürger die Hintertüren auf deren Rechner. Und wir müssen hoffen, dass es *nur* deutsche Sicherheitsbehörden sind, die sich auf den infizierten PCs tummeln.

Wir fordern, dass unseren Verfassungsrichtern anderes übrig bleibt, als in ohnmächtigem Zorn ihre roten Roben zusammenzuknüllen und in die Ecke zu schmeißen ... Quellen-TKÜ, das ist Sicherheitsbehörden in außergewöhnlichen Fällen erlaubt: Ja, sie dürfen notfalls und gemäß den Vorgaben des Verfassungsgerichts die verschlüsselte Kommunikation gefährlicher Personen abhören.

Aber sie dürfen unter keinen Umständen die Rechner ihrer *Untertanen* durchschnüffeln und manipulieren! Egal, ob sie ihren eigenen Dilettantismus oder die Gefährdung der öffentlichen Sicherheit oder ähnliche Ausreden dafür ins Feld führen! Schon gar nicht dürfen sie Daten und Code-Zeilen in die USA umleiten und dort einem nochmals erhöhten Risiko aussetzen. Das ist verboten, die Gesetzesbrecher sind sie!

*Dagmar Boedicker*

**Dietrich Meyer-Ebrecht**

# „It's not the business of the customer …"

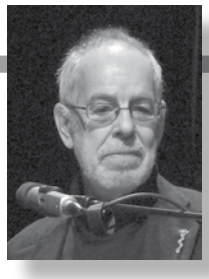
## Mein höchst persönlicher Nachruf auf Steve Jobs

„It's not the business of the customer to know what he wants" – zitierte die New York Times Steve Jobs in ihrem Nachruf. Heftiger Widerspruch regt sich, bin ich doch in meiner aktiven Berufszeit mit erhobenen Zeigefinger durch die Lande gezogen: Ihr IngenieurInnen, ihr InformatikerInnen, schaut hin, hört ihnen zu, den zukünftigen AnwenderInnen eurer technischen Kreationen, was brauchen sie, um sich durch neue Technik unterstützt zu fühlen, anstatt sich ihren Zwängen fügen zu müssen! Und dann, 1984, kam Steve Jobs mit seiner Crew und präsentierte den *Apple Macintosh* – den *Mac 128k* oder auch *Mac 1984*, das erste Modell dieses ungewöhnlichen Schreibtisch-Computers –, und dessen Konzept schien mit einem Schlag alle Unbequemlichkeiten, die wir bis dahin in der Benutzung der uns erst wenige Jahre zuvor bescherten ‚personal computers' in Kauf nahmen, aufzulösen: Maus und Icons, virtuelle Ordner statt Verzeichnisbäume, Doppelklicks statt Befehlscodes tippen, Intuition walten lassen statt Handbücher wälzen. 1984, vor die düstere Konnotation dieser Jahreszahl schob sich das bläuliche 9"-Displaybild eines virtuellen Schreibtisches.

1984, das Jahr, in dem ich – frisch an die RWTH berufen – befand, dass meine Sekretärin ein zeitgemäßes Schreibgerät haben musste. Digitale Textverarbeitung hielt gerade ihren Einzug in die Büros, das Angebot war schon vielfältig und umso unübersichtlicher. Nun, sie soll damit arbeiten, sie soll es sich aussuchen. Also hat sie sich nach Köln aufgemacht, um sich auf der OrgaTechnik, der großen Bürogerätefachmesse (heute die OrgaTec) kundig zu machen. Was sie mir am nächsten Tag berichtete, will ich aus dem Gedächtnis wiedergeben: Nach einem ermüdenden Rundgang und vielen fachchinesischen Erläuterungen der Verkäufer sei da noch ein kleiner, eher unauffälliger Stand gewesen mit einem vergleichsweise eigenwillig gestalteten Gerät. Auf ihre Frage nach einer Demonstration hätte der Standbetreuer sie eingeladen, sich doch einfach mal selbst daran zu setzen. Und dieses Gerät wolle sie haben! So kam, zunächst mit einem *Mac 512k*, dem etwas weiter ausgebauten Mac der ersten Stunde, Apple in mein Institut – und blieb. Trotz aller nachsichtigen bis herablassenden Kommentare der PC-Nerds – oder versteckte sich hinter der Abqualifikation ein wenig der Neid, dass uns Mac-UserInnen die Mühsal des Umgangs mit DOS und dem frühen Windows, mit dem MicroSoft knapp zwei Jahre später nachzog, erspart blieb? Meine Sekretärin jedenfalls konnte auf ihren Kolleginnentreffen damit punkten, dass sie als erste die Textverarbeitung beherrschte – und das ohne Schulung!

„It's not the business of the customer …" – wünschten wir uns denn Computer, deren Technik unter grauem Plastik kompakt und ansprechend verpackt war? Deren Funktion intuitiv erlebt werden konnte? Mit einer bislang ungewohnten Ästhetik der Displaygrafik? Wünschten wir uns Computer, die durch runde Formen bunten Plexiglases spielerisch den Blick auf Kabel und Platinen freigaben, später? Oder die, noch später, an die sachliche Strenge der Bauhaus-geprägten Designkonzepte des Dieter Rams anknüpften? Steve Jobs war nicht der Designer. Aber er hat nach seiner Rückkehr zu Apple 1997 verstanden, welchen Glücksgriff Apple 1992 mit ihrem Chefdesigner Jonathan Ive getan hatte und ihn in jeder Beziehung gefördert. Er hat damit einer gestalterischen Gegenbewegung stattgegeben. Waren die Achtziger Jahre durch die gesichtslose Gestaltung unserer technischen Umgebung gekennzeichnet, die nur noch einer Rationalisierung ihrer Herstellung Tribut zollte – PCs in uniformen Blechkästen, Autos wie kantige Schuhkartons, monotone Glasfassaden der Bürogebäude –, so lehrte uns Apple wieder, über eine funktionsbezogene Ästhetik eine emotionale Beziehung zu unseren alltäglich benutzten technischen Geräten aufzubauen. Haben Steve Jobs und seine Crew doch genauer danach geschaut, was wir ersehnten? Und haben sie tatsächlich Antworten erhalten, wenn sie gefragt haben? Ich glaube, eher war es eine glückliche Kombination aus Intuition und Sensibilität, eine Art Metakommunikation mit der Gemeinde der potentiellen BenutzerInnen.

„It's not the business of the customer …" – sich Gedanken über Folgewirkungen zu machen. Unter Steve Jobs' zweiter Apple-Karriere hob Apple vom bodenständigen Computergeschäft ab und begab sich mit *iPod* und *iTunes*-Shop auf Höhenflug im Unterhaltungsgeschäft, mischte zuletzt mit *iPhone* und *iPad* den Markt der mobilen Kommunikation auf. ‚Informatik und Gesellschaft', bis dahin ein eher ideelles Konstrukt, erhielt eine alltäglich erfahrbare, eine anfassbare Relevanz: die digitalen ‚Allesköner' als ständige Begleiter, als integraler Teil unseres Lebens, permanent und ubiquitär. Das Paar am Nebentisch, sie checkt ihre Email, schaut was ihre ‚Freunde' gerade twittern – er, die weißen Stöpsel im Ohr, den Blick auf ferne abstrakte Orte fixiert, diskutiert gestikulierend mit dem imaginären Gegenüber: Lyfestyle! An welcher Kreuzung werde ich abbiegen, in welchem Restaurant werde ich relaxen, in welchem Hotel werde ich heute Abend landen – mein smarter digitaler Begleiter weiß es bereits: Lyfestyle! Wie hätte wohl Orwells sein „1984" beschrieben, vorhersehend wie bereitwillig wir rund um die Uhr die Schnitt-



**Dietrich Meyer-Ebrecht**

**Dietrich Meyer-Ebrecht** ist stellvertretender Vorsitzender des FIfF. Er war bis 2004 Inhaber des Lehrstuhls für Bildverarbeitung der RWTH Aachen.

stellen für eine umfassende Ausspähung unseres Treibens und Tuns, unserer Wege und Kontakte mit uns herumtragen. Sind *iPhone*, *iPads* und all die SmartPhones von Apple's Epigonen bereits die „äppäräti" aus Gary Shteyngart's dystopischer „Super Sad True Love Story"? Noch amüsiert es uns, wenn das kleine Mädchen auf *YouTube* befindet, dass die Zeitschrift wohl kaputt sei, weil sich das Bild beim darüber Wischen nicht bewegt …

„It's not the business of the customer …" – hinzuschauen, unter welchen menschenverachtenden Arbeitsbedingungen Apple's Lifestyle-Produkten produziert werden – oder doch? Vielleicht fällt dem ‚customer' doch allmählich auf, welch ein Widerspruch zwischen diesen „schönen" Produkten und den hässlichen Umstände ihres Entstehens klafft. Für Apple wäre es kaum mehr als ein unternehmerisches ‚add on' gewesen, in der Rentabilitätsrechnung kaum spürbar, mit der Schubkraft der Innovationen seiner Lifestyle-Produkte auch eine menschenwürdige Produktion und einen nachhaltigen Ressourcenumgang zum Lifestyle zu erklären. Der ‚customer' würde es vermutlich sogar honoriert haben! Ob auch Terry Gou, CEO von Foxconn, sind wir uns nicht so sicher – zwar betrauerte er den Verlust eines ‚großen Freundes' öffentlich, aber womöglich nur, weil in der Folge sein einträgliches Geschäft mit der Apple-Produktion leiden könnte. So jedenfalls schreibe ich auch diese Kolumne immer noch auf meinem sechs Jahre alten *PowerBook*, und jedes Mal, wenn es mich juckt, nun endlich auf ein aktuelles Produkt umzusteigen, sehe ich die Menschen an den Bändern bei Foxconn vor mir und denke dann, du kannst dein altes noch ganz gut weiter benutzen.


*Mac SE 1/20 (1987), Nachfolger des legendären Mac 128k, mit 1MB-Arbeitsspeicher und 20MB-Festplatte*

Steve Jobs, unter all den ingeniösen Gestaltern unserer technisierten Gesellschaft wärst du mir die Lichtgestalt – hättest du, gepriesener Visionär, dich auch eingesetzt für gesellschaftliche Utopien und wie man ihnen mit adäquaten Technologien den Weg bereiten könnte – hättest du deine Macht als CEO und Chef-Innovator eines der gewinnträchtigsten Unternehmen auch eingesetzt, um Apple zum Vorbild für menschwürdige Produktionsbedingungen aufzubauen, auf dass deine schönen Schöpfungen auch von den Menschen gerne in die Hand genommen werden, denen wir ihren Zusammenbau verdanken. So aber schrumpfst du für mich leider wieder (fast) auf Normalmaß. Dennoch, wenn ich in Nostalgie auf den *SE 1/20* im Kellerregal blicke – 1987 unser erster ‚home computer' (Bild) –, möchte ich deine genialen Schöpfungen in unserer ansonsten eher tristen Computerwelt nicht missen wollen.

**Stefan Hügel**

# Log 4/2011

## Ereignisse, Störungen und Probleme der digitalen Gesellschaft

*Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.*

### August 2011

**8. August 2011:** Google bestätigt, dass in der Vergangenheit mehrfach Nutzerdaten von US-Geheimdiensten angefordert worden seien. Dies betreffe auch Daten, die auf europäischen Servern gespeichert sind. Die Anforderungen würden aber immer genau geprüft. Google ist – wie alle US-Unternehmen – nach dem *Patriot Act* zur Herausgabe solcher Daten zur Auswertung beispielsweise durch die National Security Agency (NSA) verpflichtet (Quelle: Wirtschaftswoche, Heise).

**8. August 2011:** Im „neuen" elektronischen Personalausweis (nPA) wird eine weitere Sicherheitslücke entdeckt, durch die er missbräuchlich genutzt werden kann. Das Informatikzentrum der Sparkassenorganisation (SIZ) meldet am folgenden Tag, es habe die Sicherheitslücke behoben. Bereits im Januar war eine Schwachstelle entdeckt worden, durch die die PIN ohne Installation von Schadsoftware auf dem Rechner des Opfers ausgespäht werden konnte. Die damalige Version wurde darauf vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zurückgezogen (Quelle: Piratenpartei, Heise).

**8. August 2011:** Gegen eine Bestimmung im geplanten Rundfunkänderungsstaatsvertrag, durch die Wohnungseigentümer beim Auffinden nicht ermittelbarer Mieter helfen müssen, wenden sich Datenschütze und Vermieterverbände. Der Paragraph nötige Vermieter, ihre Mieter zu bespitzeln, erklärte der Direktor der Vereinigung Haus und Grund in Schlswig-Holstein. Dies

spreche Freiheitsrechten und Datenschutz Hohn. Auch Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein kritisiert die Bestimmung (Quelle: Heise).

**9. August 2011:** Die Kommunikation in sozialen Netzwerken in Indien soll stärker staatlich überwacht werden. Die Regierung übt Druck auf die Anbieter von Web-2.0-Diensten aus, ihre Angebote einfacher überwachbar zu machen. Dem Kommunikationsminister zufolge könnten Möglichkeiten dieser Dienste durch Terroristen zur Planung von Anschlägen genutzt werden. Die indische Regierung hatte bereits zuvor Telekommunikationsanbieter unter Druck gesetzt (Quelle: IDG News Service, Heise).

**11. August 2011:** Die Regierung in Großbritannien erwägt, Kommunikationsdienste und Internet-Seiten zu sperren, um die im Land stattfindenden Unruhen zu bekämpfen. Es bestehe der Eindruck, die Unruhen seien über soziale Medien organisiert worden, so Premierminister David Cameron. Auch in Ägypten, Tunesien und Libyen wurde zuvor das Internet eingeschränkt, um gegen die dort stattfindenden Aufstände vorzugehen (Quelle: Heise).

**15. August 2011:** Erfreut reagieren chinesische staatliche Medien auf die Forderungen des britischen Premierministers Cameron, Internet-Dienste zu kontrollieren. Als ehemaliger Verfechter absoluter Internetfreiheit habe die britische Regierung „eine Kehrtwende" vollzogen, so die Nachrichtenagentur Xinhua. Sie habe nun anerkannt, dass ein Gleichgewicht zwischen Freiheit und Überwachung gefunden werden müsse. Die chinesische Zeitung Global Times fordert dazu auf, die Grenzen von Demokratie und Meinungsfreiheit zu überdenken (Quelle: Global Times, Heise).

**15. August 2011:** Der seit 9. Juli 2011 unabhängige Südsudan wird das Landeskürzel „SS" und damit auch die Top-Level-Domain (ccTLD) „.ss" bekommen. Das war von der Regierung bei der zuständigen ISO 3166 Maintenance Agency so beantragt worden (Quelle: Heise).

**17. August 2011:** Die Bundesregierung will die Befugnisse aus dem Terrorismusbekämpfungsergänzungsgesetz (TBEG) um weitere vier Jahre verlängern und dabei noch ausweiten. Zusätzlich zu den bisherigen Auskünften bei Banken, Fluggesellschaften, Reisebüros, Postdienstleistern und Telekommunikationsanbietern soll es auch eine Abfrageerlaubnis bei zentralen Buchungssystemen und eine Möglichkeit zur Abfrage von Kontostammdaten geben. Der Bundedatenschutzbeauftragte Peter Schaar kritisierte, dass die nach dem 11. September 2001 in großer Eile erlassenen Gesetze bereits zum zweiten Mal ohne unabhängige Überprüfung verlängert werden sollen. Nicht einmal der gesetzlich geforderte Evaluationsbericht sei bisher vorgelegt worden. Der Vorsitzende der Gewerkschaft der Polizei (GdP), Bernhard Witthaut, begrüßte die Verlängerung und forderte die schnelle Wiedereinführung der Vorratsdatenspeicherung (Quelle: netzpolitik.org, Heise).

**19. August 2011:** In einer Mitteilung fordert das Unabhängige Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein die Betreiber von Web-Seiten auf, den Like-Button von Facebook bis Ende September zu entfernen, und droht mit Bußgeldern wegen Verstoß gegen geltendes Datenschutzrecht. Der Like-Button ermögliche User-Tracking ohne die Genehmigung der Nutzer, so das ULD in einer technischen Analyse. Außerdem genügten die Formulierungen in den Nutzungsbedingungen und Datenschutzrichtlinien nicht annähernd den gesetzlichen Anforderungen (Quelle: ULD, Heise).

**25. August 2011:** Berichten des Freitag zufolge ist eine Datei von Wikileaks mit dem Namen *cables.csv* im Internet verfügbar – möglicherweise der vollständige Cablegate-Datensatz. Die Datei ist mit einem Passwort geschützt; dieses wurde jedoch ebenfalls – in der Annahme, es sei „temporär" – weitergegeben (Quelle: Freitag, netzpolitik.org).

**26. August 2011:** BKA-Chef Ziercke findet, dass es beim Datenschutz eine unbegründete Hysterie gebe. Auch er wolle keinen Überwachungsstaat und erkenne an, dass sich Menschen Gedanken über den Datenschutz machten. Der Kampf gegen schwere Straftaten mache aber den mindestens sechsmonatigen Zugriff auf Verbindungsdaten erforderlich. Er fordert deswegen eine neue Regelung der Vorratsdatenspeicherung (Quelle: hr-info, Heise).

**26. August 2011:** Die CDU teilt betroffenen Mitgliedern mit, dass bereits im August 2009 bei einem Angriff auf das Mitgliedernetz Mitgliederdaten entwendet worden seien. Diese wurden am 12. August 2011 ins Netz gestellt. Es handele sich dabei um Nachnamen, interne Kennung und E-Mail-Adresse (Quelle: Heise).

**26. August 2011:** Das australische Repräsentantenhaus verabschiedet die *Cybercrime Legislation Amendment Bill 2011*, die unter anderem vorsieht, dass Telekommunikationsanbieter zur Speicherung von Verbindungs- und Inhaltsdaten verpflichtet werden können. Damit bleiben auf dem Rechner befindliche Informationen, E-Mails, SMS-Nachrichten und weitere Daten verfügbar; der Zugriff sei nur mit richterlicher Genehmigung erlaubt. Durch das Gesetz soll das australische Recht mit der umstrittenen europäischen Cybercrime-Convention in Einklang gebracht werden. Unternehmen, Bürgerrechtler, Datenschützer und Oppositionelle kritisieren den Entwurf. Er übernehme von der Cybercrime-Convention nur die Grundrechtseingriffe, nicht jedoch deren Schutzbestimmungen (Quelle: Heise).

**30. August 2011:** Offenbar wurde der libysche Geheimdienst bei der Internetüberwachung von einer Reihe ausländischer Unternehmen unterstützt. Belege dafür wurden von Reportern des Wall Street Journal in Tripolis gefunden. Darunter seien Tochterunternehmen des Computerherstellers Bull und des Boeing-Konzerns (Quelle: Wall Street Journal, Heise).

**30. August 2011:** Über die niederländische Firma Diginotar ist der Iran offenbar an ein SSL-Zertifikat gekommen, mit dessen Hilfe verschlüsselte Gmail-Verbindungen abgehört werden können (Quelle: netzpolitik.org).

**31. August 2011:** Netzpolitiker der SPD, die im Gesprächskreis „Netzpolitik und Digitale Gesellschaft" beim SPD-Parteivorstand organisiert sind, befürworten in einem Musterantrag die umstrittene Vorratsdatenspeicherung von IP-Adressen. Die Vorratsdatenspeicherung müsse „differenziert" betrachtet werden.

Bereits 2007 hatte das Berliner Amtsgericht geurteilt, dass durch die Speicherung der Adressen das Surfverhalten detailliert nachvollzogen werden könne und deswegen von einer Verletzung des Rechts auf infomationelle Selbstbestimmung auszugehen sei. Der Vorstoß der SPD wird in netzpolitischen Kreisen kontrovers diskutiert (Quelle: Heise).

**31. August 2011:** Das Bundesinnenministerium wird vorläufig keine Nacktscanner zur Sicherheitsüberprüfung an Flughäfen einsetzen. Die Technik sein noch nicht ausgereift, die Scanner zwar leistungsfähig, aber noch nicht flächendeckend einsetzbar. In einem Feldtest war festgestellt worden, dass die Scanner bei ca. 70 % der Fluggäste Alarm schlugen und Nachkontrollen erforderlich machten (Quelle: Bundesinnenministerium, Heise).

## September 2011

**1. September 2011:** Das amerikanische Unternehmen Cataphora hat eine Software erstellt, die „Charakterprofile" von Unternehmen und Mitarbeitern erstellt und damit dazu beitragen soll, die Produktivität zu erhöhen. Dazu werden digitale Dokumente wie E-Mails, Einträge in Terminplanern oder weitere Texte daraufhin analysiert, welche Schriftfarben die Mitarbeiter verwenden, wie sie Ausrufezeichen setzen und wie häufig sie „bitte" verwenden. Dies könne auf Frustration hindeuten; solche Mitarbeiter sollten besonders beobachtet werden. Es sollen auch beispielsweise entscheidungsschwache Mitarbeiter erkannt werden, um Informationen für die Beförderung in Führungsposition zu bekommen (Quelle: Technology Review, Heise).

**1. September 2011:** Der Verkehrsausschuss des Europäischen Parlaments hebt das Verbot der Anzeige realer Abbildungen in Nacktscannern anstatt von Verfremdungen wie Piktogrammen mit den Stimmen der konservativen und der sozialdemokratischen Fraktion auf. Das Verbot hatte der Ausschuss zuvor noch befürwortet. Begründet wurde die Entscheidung laut einer Mitteilung von Alexander Alvaro (FDP) damit, dass es nur einen Hersteller gebe, dessen Geräte mit Piktogrammen arbeiteten, und dieser damit eine Monopolstellung erlangen würde. Liberale und Grüne kritisieren die Entscheidung; die Befürworter entzögen sich ihrer Verantwortung zum Schutz der Privatsphäre (Quelle: Heise).

**2. September 2011:** Der Vorsitzende des Rechtsausschusses des Bundestags, Siegfried Kauder, fordert schärfere Strafvorschriften zur Geheimhaltung. Jede Veröffentlichung solle tabu sein, die Menschen in Gefahr bringen kann. In solchen Fällen müssten abschreckende Strafen möglich sein. Kauder setzt sich damit von einem Gesetzentwurf auf Initiative der FDP ab, der die Pressefreiheit im Strafrecht stärken will (Quelle: netzpolitik.org, Neue Osnabrücker Zeitung, Heise).

**8. September 2011:** Angesichts der Kritik am Datenschutz des sozialen Netzwerks Facebook setzt Bundesinnenminister Hans-Peter Friedrich auf Selbstkontrolle. Es solle einen Kodex geben, der auch Regelungen zur Datensicherheit enthalte. ULD-Leiter Thilo Weichert zeigte sich irritiert über die Erklärung, dass nach einem Gespräch mit Facebook „die Diskussion, inwieweit deutsches Datenschutz- und Telemedienrecht für Facebook gilt, deutlich entschärft" sei. „Er sollte als Bundesdatenschutzminister zumindest dafür eintreten, dass die geltenden Regelungen eingehalten werden", erklärte Weichert (Quelle: Heise).

**10. September 2011:** Bei der Demonstration „Freiheit statt Angst" in Berlin haben sich rund 5.000 Teilnehmer versammelt, um für die Privatsphäre und gegen Überwachungswahn zu protestieren (Quelle: netzpolitik.org).

**12. September 2011:** Der Landesdatenschutzbeauftragte Sachsens, Andreas Schurig, bezeichnet die Dresdner Massenabfrage von Handy-Daten im Zusammenhang mit einer Demonstration gegen Neonazis als unverhältnismäßig und rechtswidrig. Es sei nicht geprüft worden, ob die umfassende Abfrage angemessen gewesen war. Schurig sprach gegen die an der Aktion beteiligten Behörden eine formelle Beanstandung aus (Quelle: Heise).

**13. September 2011:** Ein Initiativbericht der liberalen Abgeordneten Sophie in't Veld zur Überprüfung der Antiterrorpolitik wurde im Europäischen Parlament an die Ausschüsse zurücküberwiesen. Die Einigung über eine Evaluierung scheiterte vor allem am Widerstand der konservativen Fraktion (Quelle: Heise).

**14. September 2011:** Die frühere Abgeordnete des europäischen Parlaments für die SPD, Erika Mann, ist als Lobbyistin in Brüssel für Facebook angeworben worden. Ihre ehemalige Mitarbeiterin Eva Maria Kirschsieper arbeitet bereits als Facebook-Lobbyistin in Berlin (Quelle: netzpolitik.org).

**14. September 2011:** Die Petiton beim Deutschen Bundestag gegen die Vorratsdatenspeicherung überschreitet die wichtige 50.000er-Marke. Damit wird im Petitionsausschuss eine öffentliche Anhörung durchgeführt (Quelle: netzpolitik.org).

**15. September 2011:** Der CDU-Politiker Hans-Peter Uhl (*#iminternetgeboren*) erklärt zur Petition gegen die Vorratsdatenspeicherung in der Tagesschau: „Das sind Menschen, die ein falsch verstandenes Freiheitsbild haben. Sie glauben, Internet ist nur so gesichert, wenn grenzenlose Freiheit ohne jede staatliche Aktivität sicher gestellt ist" (Quelle: Tagesschau, netzpolitik.org).

**18. September 2011:** Bei den Wahlen zum Berliner Abgeordnetenhaus erreicht die Piratenpartei 8,9 % der Stimmen und erhält damit 15 Sitze. Verluste muss vor allem die FDP hinnehmen; sie stürzt auf 1,8 % ab. Stärkste Kraft bleibt die SPD (Quelle: Tagesschau, Zeit, Spiegel, netzpolitik.org, …).

**21. September 2011:** Die Bundesregierung beschließt, den umstrittenen elektronischen Entgeltnachweis (ELENA) endgültig zu stoppen. Das ELENA-Gesetz soll komplett aufgehoben und die alte Rechtslage wiederhergestellt werden. Hauptgrund für die Einstellung ist die ungenügende Verbreitung der qualifizierten elektronischen Signatur (Quelle: Heise).

**22. September 2011:** Der Europäische Ministerrat verabschiedet ein Abkommen zur Weitergabe von Fluggastdaten an australische Behörden. Die Passenger Name Records (PNR), die Namen und Anschrift, Kreditkarten- und Telefonnummern, IP-Adressen und besondere Essenswünsche umfassen, sollen fünfeinhalb Jahre in Australien gespeichert werden; der Personenbezug soll für Regelabfragen nach drei Jahren verschleiert werden. Die

Neufassung verstoße gegen das europäische Datenschutzrecht und grundlegende rechtsstaatliche Prinzipien in Europa, kritisierte Jan Philipp Albrecht, Innenexperte der Grünen (Quelle: Heise).

**22. September 2011:** Facebook-Chef Mark Zuckerberg stellt eine grundlegende Renovierung des sozialen Netzwerks Facebook vor. Dabei soll die bisherige Pinnwand durch die „Timeline" ersetzt werden, in der Inhalte ein- oder zweispaltig angezeigt werden. Aktivitäten und Webinhalte sollen mit Facebook-Profilen verknüpft und weitgehend automatisiert – ohne expliziten Klick auf Like- oder Share-Buttons – angezeigt werden; dadurch wird Facebook zum „Lebens-Log" (Quelle: netzpolitik.org, Heise).

**26. September 2011:** Der Vorsitzende des Rechtsausschusses des Bundestags und Präsident der Bundesvereinigung Deutscher Musikverbände, Siegfried Kauder, hat einen Gesetzentwurf gegen Urheberrechtsvertöße im Internet angekündigt. Er fordert Sanktionen bis zur Sperrung des Internetanschlusses. Kauders Vorstoß wird auch in der Koalition kritisiert; der parlamentarische Geschäftsführer der CDU/CSU-Fraktion, Peter Altmaier, twittert: „Kauder-Strikes geht gar nicht: Wer Bücher klaut, ist kriminell, aber man nimmt ihm nicht die Lesebrille weg" (Quelle: Frankfurter Allgemeine, netzpolitik.org, Heise).

## Oktober 2011

**6. Oktober 2011:** Auf Zugangsdaten von Shared-Hosting-Anwendern bei der Hetzner Online AG hat möglicherweise ein unbefugter Zugriff stattgefunden. Die Daten waren im Klartext zugänglich. Von den Passwörtern der Rootserver-Verwaltung lagen nur kryptographische Prüfsummen vor, aus denen aber bei entsprechender Rechenleistung die Passwörter errechnet werden können (Quelle: Heise).

**7. Oktober 2011:** Deutschland und Österreich liegen bei einer Vergleichsstudie zur Informationsfreiheit schlecht ab: Deutschland belegt den fünftletzten, Österreich den letzten Platz. Die Rangliste basiert auf 61 Indikatoren in verschiedenen Kategorien (Quelle: Centre for Law and Democracy, Access Info Europe, Heise).

**7. Oktober 2011:** Die französische Behörde Hadopi, die Urheberrechtsverletzungen bekämpfen soll, hat ca. 650.000 Internet-Nutzern einen ersten, ca. 44.000 Nutzern bereits den zweiten Warnhinweis geschickt. Ca. 60 Internetnutzer müssen nach dem „Third Strike" mit einer Sperrung des Internet-Zugangs rechnen (Quelle: Hadopi, Heise).

**7. Oktober 2011:** Der Widerspruch gegen den Panorama-Dienst von Microsoft ist deutlich geringer als der gegen Google-Street-View im Vorjahr. Nach Angaben von Microsoft gab es ca. 80.818 Widersprüche; gegen Google waren es rund dreimal so viel (Quelle: Heise).

**8. Oktober 2011:** Der Chaos Computer Club (CCC) enttarnt eine staatliche Spionagesoftware. Die Software, die zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) eingesetzt wird, ist offenbar zu wensentlich mehr in der Lage: So können praktisch beliebige Daten ausgeleitet und weitere Schadsoftware ferngesteuert installiert werden. Zudem weist die Software erhebliche Sicherheitslücken auf. Bereits zuvor hatte das Landgericht Landshut festgestellt, dass die bei einer Überwachungsmaßnahme angefertigten Screenshots nicht rechtens waren (Quelle: Frankfurter Allgemeine, Zeit, Heise).

**16. Oktober 2011:** Der Ministerpräsident von Baden-Württemberg, Winfried Kretschmann, fordert ein Gebührensystem für PKW mit satellitengestützter Ortung. Im Nachrichtenmagazin Focus schlug er dafür das Navigationssystem Galileo vor. Voraussetzung dafür sei aber, dass der Datenschutz gewährleistet ist. Er erwartet durch ein solches System einen großen Markt für neue Technologien. In den Niederlanden wurde kürzlich ein solches Projekt („Kilometerheffing") wegen Datenschutzbedenken gestoppt (Quelle: Focus, Heise).

**17. Oktober 2011:** Wegen des Einsatzes von Trojanersoftware bei polizeilichen Ermitttlungen stellt die Piratenpartei Strafanzeige gegen Bayerns Innenminister Joachim Herrmann (CSU) und gegen Beamte des bayerischen Landekriminalamts (Quelle: Heise).

**17. Oktober 2011:** Ein französisches Gericht lässt die Zugriffe auf die Website Copwatch (copwatch-idf.org) sperren. Der Entscheidung vorangegangen war ein Antrag des Innenministers Claude Guéant, der Seiten mit persönlichen Daten von Beamten sperren lassen wollte. Das Gericht ging mit seiner Entscheidung über den Antrag hinaus (Quelle: netzpolitik.org, Heise).

**22. Oktober 2011:** Der irische Datenschutzbeauftragte unterzieht die europäische Niederlassung von Facebook einer Prüfung. Dabei soll es auch um die die Beschwerden gehen, die der österreichische Jura-Student Max Schrems gegen Facebook eingereicht hat. Schrems hatte bei Facebook die über ihn gespeicherten Daten angefordert und dabei unter anderem Informationen gefunden, die er bereits gelöscht hatte (Quelle: Heise).

**24. Oktober 2011:** Die Datenbank des israelischen Einwohnermelderegisters mit dem Stand von 2006 wurde im Netz veröffentlicht. Die Datenbank enthält die Daten von ca. 9 Millionen israelischen Bürgern mit u.a. Name, Familienstand und persönlicher Identifikationsnummer. Offenbar wurden die Daten von einem früheren Mitarbeiter des Sozialhilfe-Ministeriums an ein Unternehmen verkauft (Quelle: Haaretz, netzpolitik.org).

**25. Oktober 2011:** Gegen den Regierungsentwurf für die geplante Visa-Warndatei haben Datenschützer verfassungsrechtliche Bedenken. Sie richten sich gegen die Bestimmung, auch die Daten von einladenden Personen zu speichern. Auch ein Abgleich mit der Anti-Terror-Datei wurde als problematisch bezeichnet (Quelle: Heise).

**25. Oktober 2011:** Die EU-Kommission veröffentlicht eine Mitteilung, nach der sie Einreisende elektronisch überwachen will. Vorbild ist das Ein-/Ausreisesystem der USA; es soll auch eine Vorzugsbehandlung für Vielreisende geben. Das System sei Teil des Gesamtkonzepts zur Überwachung des Schengen-Raums. Der innenpolitische Sprecher der Grünen im europäischen Parlament, Jan Philipp Albrecht, warnt vor einem Einstieg in die Kompletterfassung der Informationen bei Ein- und Ausreise (Quelle: Heise).

**26. Oktober 2011:** Bei den österreichischen Big Brother Awards wurde der Facebook-Kritiker Max Schrems mit dem Positivpreis „Defensor Libertatis“ ausgezeichnet. Er hatte 22 Anzeigen bei der irischen Datenschutzbehörde eingereicht. Den Sonderpreis „Lebenslanges Ärgernis“ erhielt dagegen Facebook-Chef Mark Zuckerberg. Weitere Auszeichnungen erhielten die östereichische Innenministerin Johanna Mikl-Leitner, Justizministerin Beatrix Karl, A1-Chef Hannes Ametsreiter, der Verleger Wolfgang Fellner und Renate Christ, Leiterin der Wiener Sozialabteilung. Bei der Volkswahl erhielt das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung die meisten Stimmen. Das Amt hatte unter anderem öffentlich gewählte Studuerendenvertreter auf eine Liste von Extremisten gesetzt (Quelle: bigbrotherawards.at, Heise).

**26. Oktober 2011:** Der Internetkonzern Google teilt mit, dass die Zahl der Fälle, in denen staatliche Behörden Nutzerdaten anfordern würden, weiter steige. Im ersten Halbjahr 2011 habe es eine 38 %ige Steigerung gegeben. Bei 67 % der Anfragen habe Google die Auskunft erteilt (Quelle: Google, Heise).

**27. Oktober 2011:** Gegen die Stimmen der Opposition verabschiedet der Deutsche Bundestag die umstrittende Reform des Telekommunikationsgesetzes (TKG). Der Gesetzentwurf war zuvor kurzfristig noch einmal korrigiert worden; dies wurde im Innenausschuss von der Opposition kritisiert. Die Kritik richtet sich vor allem gegen die unbegrenzte Speicherbefugnis für Daten, die für die Abrechnung von Diensten erforderlich seien, dies wird von den Kritikern als „Quasi-Vorratsdatenspeicherung“ bezeichnet (Quelle: netzpolitik.org, Heise).

**27. Oktober 2011:** Der europäische Parlament nickt das zuvor im Ministerrast beschlossene Fluggastdatenabkommen zur Übermittlung von Passenger-Name-Records (PNR) an australische Behörden ab. Die Datensätze werden dort fünfeinhalb Jahre gespeichert (Quelle: Heise).

**28. Oktober 2011:** Der Bundestag verlängert mit den Stimmen der Koalition die im Terrorismusbekämpfungsergänzungsgesetz (TBEG) vorgesehenen Anti-Terror-Befugnisse. Zum Teil werden die Befugnisse ausgedehnt; das betrifft Auskünfte von Banken, Fluggesellschaften, Reisebüros, Postdienstleistern und Telekommunikationsanbietern (Quelle: Heise).

**28. Oktober 2011:** Der Bundestag lehnt mit den Stimmen der Koalition und der SPD einen Antrag der Linken ab, die Befugnis des Bundeskriminalamts (BKA) zu Online-Durchsuchungen aufzuheben. Die Maßnahme sei „unnütz, unverhältnismäßig und unangemessen für einen Rechtsstaat“, so Jan Korte. Er nannte in dem Zusammenhang die Untersuchungen des Chaos Computer Club. Ein Sprecher der Koalition verwies auf die terroristische Bedrohungslage (Quelle: Deutscher Bundestag).

**28. Oktober 2011:** Nach der Klage zweier Bundestagsabgeordneter der SPD hat das Bundesverfassungsgericht das Sondergremium per einstweiliger Anordnung vorläufig gestoppt, das stellvertretend für den Bundestag über Maßnahmen aus dem Euro-Rettungsfonds EFSF entscheiden sollte. Das Gremium öffne möglicherweise eine Hintertür, die Beteiligung des Bundestages bei weitreichenden Entscheidungen in einen exklusiven Zirkel zu verlagern. Mit Entscheidungen verbundene Rechtsverletzungen seien dann nicht mehr rückgängig zu machen, da die Bundesrepublik Deutschland nach außen an die Entscheidungen gebunden sei (Quelle: Bundesverfassungsgericht, Spiegel).

**28. Oktober 2011:** Bei dem Spiel Battlefields3 des Unternehmens Electronic Arts installiert sich eine Schadsoftware, die den Rechner auf weitere Spiele von Electronic Arts überprüft und Daten darüber an das Unternehmen sendet. Der Nutzer muss vor Nutzung des Spiels dieser Ausspähung per Lizenzvertrag zustimmen; Juristen wie der Richter und Rechtsprofessor Thomas Hoeren aus Münster sehen in dem Lizenzvertrag einen Verstoß gegen deutsches Recht. Er bezeichnet die Bestimmungen als „null und nichtig“ und „Unverschämtheit“ (Quelle: netzpolitik.org, Spiegel).

**31. Oktober 2011:** Deutsche Schulbuchverlage planen offenbar einen „Schultrojaner“, mit dem durch technische Maßnahmen sichergestellt wird, dass digitalisierte Unterrichtsmaterialien nicht unerlaubt verbreitet werden. 1 % der Rechner sollen durch eine „Plagiatssoftware“ auf unerlaubte Kopien geprüft werden. Genaue Funktionalität und Einsatzbereiche werden im Vertrag nicht festgelegt (Quelle: netzpolitik.org, Heise).

## November 2011

**1. November 2011:** Nach der Ankündigung der schleswig-holsteinischen Landesregierung, ihre Facebook-Fanseite entgegen der Aufforderung des Leiters des unabhängigen Landeszentrums für Datenschutz, Thilo Weichert, nicht abzuschalten, will dieser der Staatskanzlei nun eine förmliche Beanstandung zukommen lassen. Nach Ansicht von Weichert verstoßen Fanseiten und „Like“-Button gegen deutsches Datenschutzrecht (Quelle: Heise).

**4. November 2011:** In Schleswig-Holstein waren Daten von rund 2500 psychisch schwer kranken Menschen monatelang frei im Internet abrufbar. Durch eine Sicherheitslücke bei einem Dienstleister in Rendsburg konnten Behörden- und Klinikbriefe, medizinische Befunde und psychologische Dokumentationen heruntergeladen werden (Quelle: Lübecker Nachrichten, Heise).

**Stefan Hügel**

**Stefan Hügel** ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main

**David Koschnick**

# Urban Mining

## Eine Herausforderung für die Ressourcensicherung im 21. Jahrhundert

*In diesem Jahr wurde der siebenmilliardste Mensch geboren, binnen der letzten hundert Jahre hat sich die Bevölkerungszahl mehr als vervierfacht. Dies hat zu einem immens wachsenden Ressourcenverbrauch geführt, welcher auch durch die rasante Entwicklung der modernen Informations- und Kommunikationstechnologie noch weiter verstärkt wird. Zwar kann der Ressourcenverbrauch in den Industrienationen durch immer modernere und effizientere Technologien verringert werden, der Gesamtressourcenverbrauch der Erde wird jedoch in den nächsten Jahrzehnten weiter ansteigen, da durch die wachsende Industrialisierung der Länder in Asien (z. B. China, Indien) und Südamerika (z. B. Brasilien) die Rohstoffsicherheit eingeschränkt bzw. nicht mehr gewährleistet ist. Der rasante Ressourcenverbrauch hat zur Folge, dass einige Rohstoffe, wie z. B. Kupfer, Silber, Indium, Titan bereits in diesem Jahrhundert erschöpft sein werden [vgl. Faulstich 2009, Weichbrodt 2011].*



In dem 2010 veröffentlichten Report der EU-Kommission *Critical raw materials for the EU – Report of the Ad-hoc Working Group on defining critical raw materials* wurden 41 verschiedene Rohstoffe anhand ihrer Bedeutung für die Wirtschaft und Verfügbarkeit bewertet. Dabei wurden 14 der 41 Rohstoffe als problematisch eingestuft.

**List of critical raw materials at EU level** (in alphabetical order):

| | |
|---|---|
| Antimony | Indium |
| Beryllium | Magnesium |
| Cobalt | Niobium |
| Fluorspar | PGMs (Platinum Group Metals)[1] |
| Gallium | Rare earths[2] |
| Germanium | Tantalum |
| Graphite | Tungsten |

1 *The Platinum Group Metals (PGMs) regroups platinum, palladium, iridium, rhodium, ruthenium and osmium*

2 *Rare earth include yttrium, scandium, and the so-called lanthanides (lanthanum, cerium, praseodymium, neodymium, promethium, samarium, europium, gadolinium, terbium, dysprosium, holmium, erbium, thulium, ytterbium and lutetium)*

**Abbildung 1:** *Liste der kritischen Rohstoffe in der EU (EU-Report: „Critical raw materials for the EU – Report of the Ad-hoc Working Group on defining critical raw materials")*

Viele dieser Rohstoffe werden in Zukunftstechnologien, wie der Nanotechnologie, der Elektro- und Hybrid-Fahrzeugtechnik sowie auch für die Informations- und Kommunikationstechnologien benötigt. Gerade in der deutschen Industrie existiert eine große Abhängigkeit von diesen Stoffen. Als Folge der möglichen Knappheit seltener Metalle kam es zu einem enormen Anstieg der Rohstoffpreise [vgl. EU-Report 2010]. Durch die wachsende Industrialisierung in China haben sich die politischen und ökonomischen Machtverhältnisse derart verändert, dass in den letzten Jahrzehnten die Volksrepublik China zu einer ernst zu nehmenden Wirtschaftsmacht aufgestiegen ist. Bei den Seltenen Erden deckt China über 95 % des Weltbedarfs ab und hat 2010 mit erhöhten Ausfuhrzöllen den Export dieser Stoffe massiv beschränkt. Außerdem hat China durch sein Monopol auf Seltene Erden die Möglichkeit, den Weltmarktpreis nahezu beliebig zu bestimmen. Da diese Stoffe für die Hightech-Industrie unersetzlich sind, müssen die Nachschubprobleme dringend gelöst werden. Aus diesem Grund haben sich Unternehmen der Großindustrie und die Ministerien, Wirtschaft, Außen und Entwicklung der Bundesrepublik Deutschland zu einer *Allianz zur Rohstoffsicherung* zusammengeschlossen, welche ihre Arbeit voraussichtlich ab dem 1. Januar 2012 aufnehmen wird [vgl. Jung et. Al. 2011].

Ein effizientes Wirtschaften mit den vorhandenen Rohstoffen wird in Zukunft nötiger denn je werden. Die bisherige Kreislaufwirtschaft in Deutschland, aber auch in der EU, birgt noch großes Potenzial, um strategisch den Primärrohstoffverbrauch angesichts schwindender Rohstoffe und steigender Preise zu senken.

Um den Kriterien einer nachhaltigen Gesellschaft für die nächsten Generationen gerecht zu werden, bedarf es langfristiger Strategien und Konzepte. Braungart und McDonough zeigten in ihrem 2002 erschienenen Buch *Cradle to Cradle, Remaking the Way We Make Things* auf, wie eine Kreislaufwirtschaft aussehen könnte, in der Produkte nahezu vollständig wiederverwertbar bzw. biologisch abbaubar sind. Das Ziel ist nicht nur die Ökoeffizienz, sondern vor allem die Ökoeffektivität zu erhöhen [vgl. Braungart, McDonough 2002]. Cradle-to-Cradle-(C2C) Produkte werden schon während des Designs bzw. des Entwurfes so gestaltet, dass sie am Ende ihres Lebenszyklus optimal wiederverwertet werden können. Beispielsweise gibt es Kleidung und Kosmetikprodukte, welche durch Kompostierung biologisch vollständig abbaubar sind. Neben dem biologischen Kreislauf spielt der technische Kreislauf vor allem bei den Gebrauchsprodukten wie Mobiltelefonen, Computern, Fernsehern u.a. eine wichtige Rolle.

In den letzten Jahren wurde neben dem C2C-Ansatz ein weiteres Konzept *Urban Mining* entwickelt, welches den C2C-Ansatz unterstützt und ihn um die Wiedergewinnung bereits verwendeter Ressourcen erweitert.

Urban Mining bedeutet ein nachhaltiger Umgang mit bereits verwendeten Ressourcen und gesammelten Abfällen aus unserer urbanisierten Gesellschaft. Städte werden nicht nur aus Verbrauchersicht betrachtet, sondern auch als Quelle wertvoller Ressourcen gesehen, welche entsprechend genutzt und wiederverwertet werden können [vgl. Urban Mining e.V. 2011] (siehe Abbildung 3).

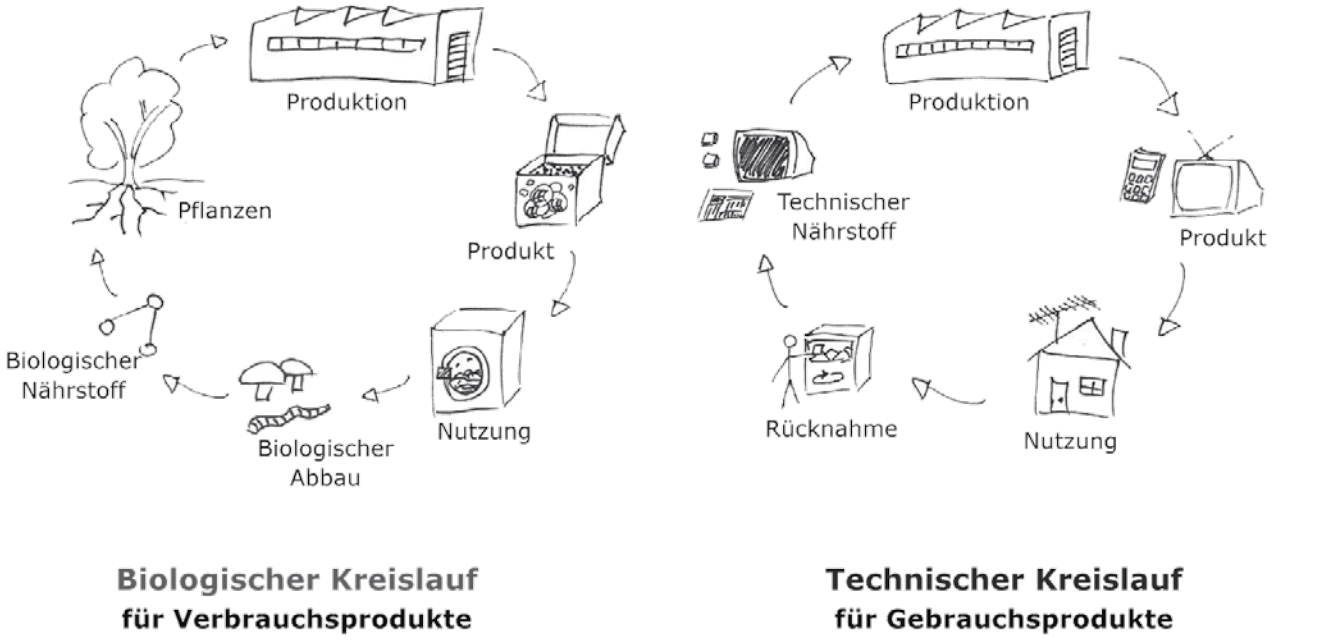



**Abbildung 2**: *Biologischer und Technischer Kreislauf [EPEA Hamburg GmbH 2009:* http://epea-hamburg.org/fileadmin/images/contentbilder/Bio_Tech_Cycle_deutsch.jpg]

Heutzutage existieren die technischen Verfahren, um bereits verwertete Rohstoffe wiederzugewinnen. In den letzten Jahrzehnten wurden immense Mengen an Ressourcen in Deponien abgelagert, welche heute durch gezielten Deponierückbau wieder zur Verfügung stehen könnten. Eine weitere Ressourcenquelle sind die Gebäude im Wohn- und Gewerbebereich. Bereits heute stehen durch den demografischen Wandel und den Zusammenbruch der DDR 1,1 Millionen Wohnungen und Industriegewerke in Deutschland leer [vgl. Gabriel 2007]. Durch den Bevölkerungsrückgang in Deutschland in den nächsten Jahrzehnten wird sich dieser Trend noch weiter fortsetzen. Die Wiedergewinnung der verwendeten Bauteile könnte ca. 35 % des Ressourcenverbrauchs für den Neubau von Gebäuden abdecken [vgl. BUND 2008, Dechantsreiter 2011]. Hier befindet sich ein noch kaum genutztes Potenzial zur Rohstoffwiedergewinnung. Problematisch jedoch sind häufig ungeklärte Eigentumsverhältnisse, welche die Ausschöpfung dieser urbanen Minen verhindern.

Urban Mining ist des Weiteren für die IT-Branche von Bedeutung, da in allen IT-Produkten (Handys, PC´s, Laptops) eine Vielzahl an Edel- und Sondermetallen verbaut sind, welche nach Ende des Lebenszyklus durch ein gezieltes Recycling zu einer Verringerung des Primärressourcenverbrauchs für IT-Produkte führen könnte. Besonders bei den Hightech-Produkten zeichnet sich ein Trend zu immer kürzer werdenden Produktlebenszyklen ab. Dies zeigt sich beispielsweise bei den Mobiltelefonen, welche heutzutage aus bis zu 60 chemischen Elementen bestehen [vgl. IFAT Entsorga]. Das Recyclingpotenzial betrug im Jahr 2009 weltweit 80.000t, wovon real gerade einmal ca. 2000t ordnungsgemäß recycelt wurden [vgl. Hagelüken 2011]. Die Ursachen für diese geringe Recyclingquote liegen zum einen darin, dass ein großer Teil der Geräte am Ende ihres Lebenszyklus nicht gesammelt bzw. erfasst wird, da sie bei den Konsumenten häufig in den Schubladen oder im Hausmüll landen. Zum anderen werden viele IT-Geräte als *Reuse* (Weiterverwendung) in Länder in Afrika oder Asien exportiert, zur Umgehung der Baseler Konventionen, welche ein Verbot für den Export von gefährlichen Abfällen beinhaltet. Durch den „halblegalen" (Reuse) und den illegalen Export gehen Ressourcen im Wert von ca. 4 Milliarden Euro pro Jahr weltweit verloren [vgl. Hagelüken 2008, Huismann et. Al. 2007]. Ein Großteil der exportierten Altgeräte wird in Afrika auf freien Flächen „gelagert" und verschmutzt dort die Umwelt. Nur ein Teil der Altgeräte wird unter primitivsten und für den Menschen gefährlichen Bedingungen recycelt [vgl. Kuper und Hojsik 2008]. Bei dem unsachgemäßen Recycling gehen über 75 % der Ressourcen unwiederbringlich verloren [vgl. Hagelüken 2008]. Hier ist besonders die Politik gefordert, Anreize zu schaffen, über effizientere Erfassungs- und bequeme Rückgabesysteme (z. B. Pfand, Rabatte) die Recyclingquote zu erhöhen. Derzeit werden nur ca. 30 % der gesamten IT-Produkte ordnungsgemäß recycelt, obwohl es bereits einige Unternehmen gibt, die sich auf das Recycling von IT-Produkten spezialisiert haben und hohe Recyclingquoten erzielen.

Grundsätzlich gibt es bei der Umsetzung von Urban Mining noch etliche Probleme zu lösen. Es beginnt bei den politischen Rahmenbedingungen, um für Unternehmen Investitionssicherheit zu gewähren. Dabei ist es wichtig, dass alle Akteure aus Wirtschaft, Kommunen, Forschung und Entwicklung zusammenarbeiten, um konkrete Handlungsbedingungen aufzustellen. Langfristig werden neue Kriterien für die Städteplanung

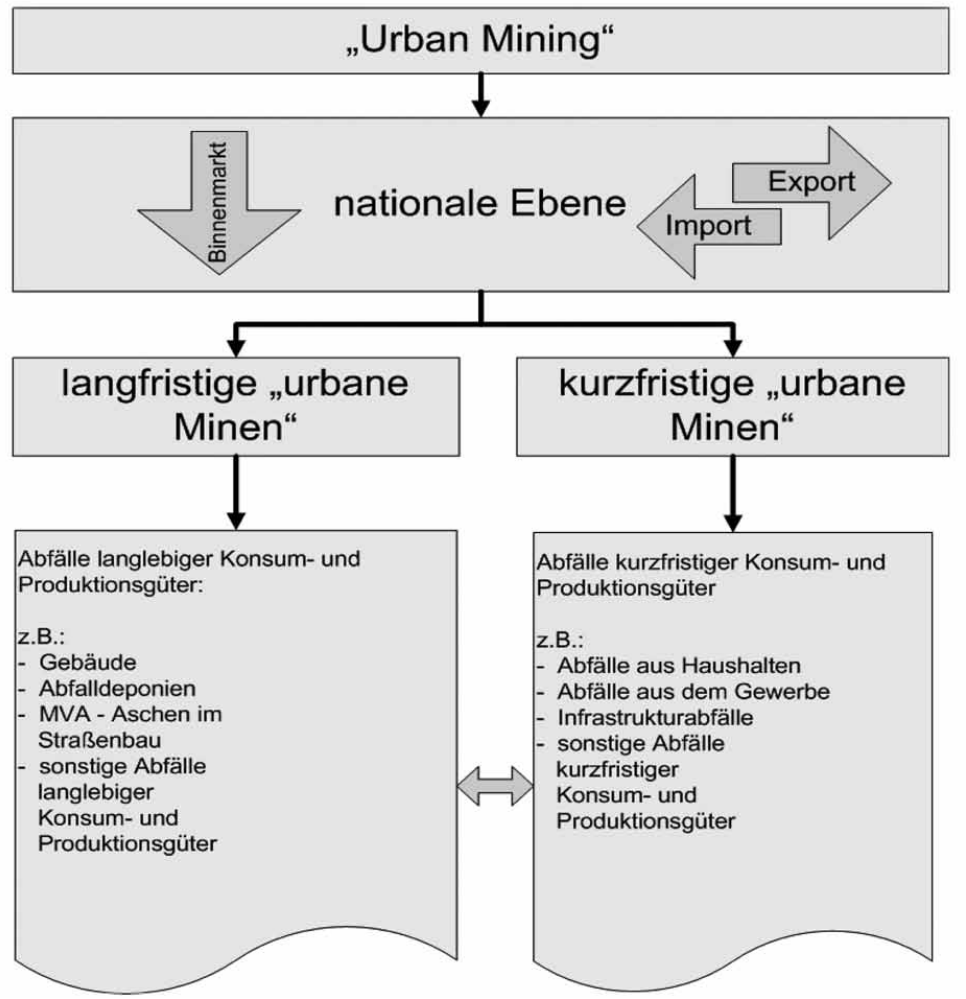



**Abbildung 3:** *Urban Mining Übersicht [Flamme, Krämer 2008]*

entstehen, um die Verfügbarkeit zukünftiger Rohstoffe zu sichern. Eine gute Erfassung und Dokumentation bestehender und zukünftiger Rohstoffquellen ist für eine erfolgreiche Umsetzung des Urban Mining von großer Bedeutung [vgl. Weichbrodt 2011]. Nicht zuletzt bedarf es der Aufklärung und Mitarbeit der Bevölkerung, welche die Grundlage für eine integrierte Kreislaufwirtschaft bildet.

Neben den gegenwärtigen Problemen bietet Urban Mining eine Vielzahl an Potenzialen und Chancen für die Gesellschaft (siehe Abbildung 4).

Eine Senkung des Ressourcenverbrauchs zieht langfristig auch eine Senkung der $CO_2$–Emissionen nach sich. Eine integrierte Kreislaufwirtschaft führt zu einer Verringerung des Abfallaufkommens und trägt damit auch zu einer Verringerung der Umweltverschmutzung bei. Durch eine Neuausrichtung der Kreislaufwirtschaft kommt es zu einem Innovations- und Wachstumsschub in dieser Branche, welche die Schaffung neuer Arbeitsplätze nach sich zieht. Gerade auch für KMUs besteht die Möglichkeit, neue Geschäftsfelder zu erschließen, indem sie sich beispielsweise gezielt auf das Recycling von einzelnen Produkten und Wertstoffen spezialisieren. Langfristiges Ziel von Urban Mining ist es, den Primärressourcenverbrauch zu senken und ein Großteil der Ressourcen durch Sekundärressourcen abzudecken. Urban Mining bedarf einer interdisziplinären Zusammenarbeit zur Entwicklung von Analyse und Bewertungsmethoden für urbane Minen aber auch zur Entwicklung neuer Technologien und Recyclingverfahren. Neben der Erhöhung der Ressourcensicherheit führt Urban Mining vor allem zur Förderung der Nachhaltigkeit und trägt zur Erhöhung der Lebensqualität der kommenden Generationen bei.

Professor Faulstich, der Vorsitzende des Sachverständigenrats für Umweltfragen der Bundesregierung ruft dazu auf, neue Wege in der Kreislaufwirtschaft zu beschreiten. Produkte sollten von ihrem Ende her konstruiert sein, so dass sie nach Ende ihres Gebrauchs wieder vollständig in die Kreislaufwirtschaft zurückgeführt werden könnten. „Wir brauchen eine integrierte Kreislaufwirtschaft, die weitgehend ohne Primärrohstoffe auskommt“ [siehe Faulstich et. Al. 2009]. Dabei sieht Faulstich die Reparaturfreundlichkeit und Langlebigkeit von Produkten als Gütezeichen, welches allerdings im Widerspruch zu den heutigen immer kürzer werdenden Lebenszyklen von Produkten steht. Hier ist ein Umdenken in Politik und Wirtschaft gefordert, um zu einer ökologischen Kreislaufwirtschaft zu gelangen. Diese Aufgabe stellt vor allem Anforderungen an die Logistik und die IT-Unterstützung, um ganzheitliche Erfassungs- und Dokumentationssysteme zu entwickeln und in der Praxis Transparenz der Altprodukt- und Materialströme zu gewährleisten. Urban Mining ist eine Möglichkeit zur effizienten Ressourcennutzung der knapper werdenden Rohstoffe.

**Potenziale und Chancen des Urban Mining für:**

| | |
|---|---|
| Natur | • Senkung des Ressourcenverbrauchs<br>• Senkung der $CO_2$-Emissionen<br>• Verringerung der Umweltverschmutzung<br>• Senkung des Abfallaufkommens |
| Individuum | • Schaffung neuer Arbeitsplätze in der Kreislaufwirtschaft<br>• Senkung des persönlichen ökologischen Fußabdrucks<br>• Monetäre Anreize |
| Unternehmen | • Spezialisierung von KMUs auf Recycling<br>• Innovations- und Wachstumsschub<br>• Imagegewinn<br>• Senkung des ökologischen Fußabdrucks<br>• Profitable Investitionen |
| Wissenschaft | • Entwicklung neuer Technologien<br>• Entwicklung von effizienteren Recyclingverfahren<br>• Interdisziplinäre Forschungsarbeit<br>• Entwicklung von Analyse und Bewertungsmethoden für Urbane Minen |
| Gesellschaft | • Förderung der Nachhaltigkeit und Lebensqualität für kommende Generationen<br>• Erhöhung der Verantwortlichkeit für Ökologie (Umweltschutz)<br>• Senkung des Primärressourcenverbrauchs<br>• Erhöhung der Ressourcensicherheit |

**Abbildung 4:** *Potenziale und Chancen des Urban Mining für die Gesellschaft*

## Literatur


Braungart, M., McDonough, W. (2002): Cradle to Cradle, Remaking the Way We Make Things. North Point Press

Braungart, M., (2011): Cradle to Cradle, Urban Mining Kongress 2011, Bremen

BUND (2008): Zukunftsfähiges Deutschland in einer globalisierten Welt: Ein Anstoss zur Gesellschaftlichen Debatte, Fischer

Dechantsreiter, U. (2011): Wiederverwendung gebrauchter Bauteile, Urban Mining Kongress 2011, Bremen

EU Report (2010) „Critical raw materials for the EU – Report of the Ad-hoc Working Group on defining critical raw materials"

Faulstich, M. (2009): Von der Abfallwirtschaft zur Ressourcenwirtschaft. Vortrag auf den 11. Münsteraner Abfallwirtschaftstagen, 10.02.2009

Faulstich, M., Brandt, E., Kreklau, C., v. Weizsäcker, E.U. (2009): Kreislaufwirtschaft als Antwort auf Rohstoffknappheit, In: BDE Perspektiven 2 Dezember 2009

Flamme, S, Krämer, P. (2008): „Urban Mining" – Schätze aus dem Hausmüll heben; Urban Mining Fachkonferenz, Düsseldorf

Gabriel, S. (2007): Die Bedeutung der Kommunalwirtschaft für eine hochwertige Entsorgung, Rede beim zweiten Bundeskongress VKS im VKU und Mitgliederversammlung am 13.09.2007

Hagelüken, C., C.E.M. Meskers (2008): Mining our computers – opportunities and challenges to recover scarce and valuable metals from end-of-life electronic devices. In: Reichel, H., Nissen, N.F. Müller, J., Deubzer, O., Electronics Goes Green 2008+, Fraunhofer IRB Verlag, Stuttgart

Hagelüken, C. (2011): Edelmetalle in der Stadt – Chancen und Herausforderungen des Recyclings, Urban Mining Kongress 2011, Bremen

Huismann, J., Magalini, F., Kuehr, R., et. Al. (2007): Review of Directive 2002/96 on Waste Electrical and Electronic Equipment (WEEE), Final Report 2007

Jung, A., Kurbjuweit, D., Neubacher, A., Schwägerl, C., Soibel, D. (2011): Jagd auf die Schatztruhe In: Der Spiegel Nr. 44 31.10.2011 S.74f.

Kuper, J., Hojsik, M. (2008): Poisoning the poor: Electronic waste in Ghana. Technical report, Greenpeace, Amsterdam, Aug. 2008

Urban Mining e.V. (2010): Url: http://www.urban-mining.com/ index.php?id=164

Weichbrodt, R. (2011): Technologietreiber Rohstoffknappheit - Cleantech 2020 – Ausblick für Urban Mining, Urban Mining Kongress 2011, Bremen



**David Koschnick**

**David Koschnick** beschäftigt sich zurzeit mit seiner Masterarbeit im Studiengang Umweltinformatik an der HTW Berlin. Er ist seit 2010 am Fritz-Haber-Institut der Max-Planck-Gesellschaft beschäftigt, wo er im Sommer des selben Jahres seine Bachelorarbeit verfasst hat. Zum FIfF kam er durch seinen Mentor Herrn Prof. Dr. habil. Klaus Fuchs-Kittowski.

**Wolf Ludwig**

# EuroDIG: Im Wechselbad von Zielkonflikten

## Eine Erfolgsgeschichte europäischer Verständigung über Regeln fürs Netz

*Es geschah am späteren Abend am Rande der ICANN-Konferenz Ende Juni 2008 in Paris. Schauplatz war die Terrasse eines Restaurants am Boulevard du Montparnasse. Um den Tisch sassen ein knappes Dutzend Leute aus dem Regierungslager (GAC), Europarat, dem Business-Sektor und Zivilgesellschaft (ALAC). Kaum waren die Reste der Nachspeisen abgeräumt, wurden die ersten Entwürfe und Skizzen auf die Papiertischdecke gekritzelt. Die Stimmung war enthusiastisch, die Debatte angeregt, der Plan reichlich ehrgeizig. Immerhin wollte man versuchen, bis Herbst des Jahres einen europäischen Ableger des globalen Internet Governance Forums (IGF) auf die Beine zu stellen. Und ab kommenden Monat war erstmal Urlaubspause angesagt.*



Spiritus Rektor der Runde war – wie schon so oft – der Kommunikationswissenschaftler und IGF-Mitgestalter Wolfgang Kleinwächter, der den European Dialogue on Internet Governance (EuroDIG) quasi als Blaupause des grossen Bruders aufziehen wollte. Tragende Säulen sollten auch hier die Multi-Stakeholder „in ihren jeweiligen Rollen" und gemeinsam mit europäischen Institutionen werden. Ein breit abgestütztes Forum, in dem alle gleichberechtigt und gleichermassen das Sagen haben, sollte die Debatte um die europäische Internet-Regulierung mitgestalten. „To dig in the future of European Internet Governance", war Losung und Auftrag der abendlichen Runde von Paris.

Erste Anläufe, die komplexen Fragen um die Verwaltung des Internets auch auf nationaler Ebene zu behandeln, gibt es bereits seit 2008 mit dem Vorläufer eines eigenen IGF in Grossbritannien. Seitdem spriessen nationale Ableger in zahlreichen europäischen Ländern wie Pilze aus dem Boden: 14 solcher Foren tagen einmal jährlich inzwischen allein in Europa. Europäische Internet-Bewegte überlegten daher schon seit dem IGF-Auftakt 2006 in Athen, ein solches Forum im europäischen Rahmen zu lancieren und damit eigene Akzente in der Debatte ums Netz zu setzen. Die Abendrunde von Paris wollte dies nun zügig umsetzen und stellte binnen weniger Monate – und überwiegend nebenamtlich – ein Organisationskonzept, eine Programmstruktur sowie ein Ablaufformat zusammen. Schon im Oktober 2008 ging in Strasbourg, unter der Schirmherrschaft des Europarats, der erste Pilotversuch über die Bühne (vgl. *http://www.eurodig.org/*). Dieser sollte nach Vorstellung der Vorbereitungsgruppe explizit nicht von Regierungsseite einberufen, sondern nach Vorbild des grossen IGF-Bruders eine „bottom-up"-Veranstaltung mit gleichberechtigter Beteiligung werden. Mit annähernd 150 Teilnehmenden, überwiegend aus Westeuropa, war der Zulauf zum ersten Euro-Dialog unerwartet hoch und verlangte förmlich nach Fortsetzung.

### Europäische Akzente

Auch die Kernthemen des EuroDIG-Programms orientierten sich am jährlichen IGF (im Dezember 2008 im indischen Hyderabad): Sicherheit, Datenschutz, Offenheit und Zugang. Der europäische Dialog sollte, so die Absicht der Organisatoren, „die europäischen Anliegen hervorheben und die Zusammenhänge zwischen den Bereichen Sicherheit, Datenschutz, Offenheit aufzeigen". Zur Eröffnung warnte die damalige EU-Medienkommissarin Viviane Reding in einer Grussbotschaft davor, „die Freiheit im Netz immer weiter gehenden Regelungen zur Sicherheit zu opfern". Eine vorausschauende und durch jüngere Entwicklungen nachhaltig begründete Furcht. Mit Hinweis auf verbreitete Datenvorratsspeicherungen bei Fluggesellschaften oder dem hartnäckigen Festhalten des deutschen Innenministers an der Online-Durchsuchung forderte der italienische Datenschutzexperte Stefano Rodota einen entschiedenen Einsatz für die Grundrechte der EU-Bürger (vgl. heise-Online 2008). Auch weitere Teilnehmer warnten vor den Gefahren eines „Überwachungsstaats", dem verbreiteten juvenilen Exhibitionismus wie der Leichtfertigkeit unbedarfter Netznutzer bei der Preisgabe persönlichster Infos nach der schlichten „Ich-hab-ja-nichts-zu-verbergen"-Attitüde. Die schwierige Balance zwischen Sicherheit, neuen Überwachungsmöglichkeiten und Verhältnismässigkeit war auch Thema für den Kölner Strafrechtsexperten Marko Gerke: „Früher war es so, dass manches, was offline verboten war, online gemacht werden konnte. Inzwischen sind wir soweit, dass viele Dinge, die offline nicht verfolgt werden, online strafbar sind." (vgl. Heise Online, 2008)

Datenschutz, das Recht auf Privatsphäre sowie deren Unvereinbarkeiten mit dem Sicherheitswahn mancher Innenminister waren Kernanliegen vieler am Euro-Dialog teilnehmenden Organisationen (vgl Heise Online 2007). Vorsicht ist dabei nicht nur gegenüber der ohnehin verdächtigen Staatsmacht geboten, sondern ebenso bei schnöden Wirtschaftsinteressen. Denn der serienmässige Datenhandel bei der deutschen Telekom sowie immer neue Missbrauchsfälle haben das Vertrauen selbst gutgläubiger Kunden nachhaltig erschüttert. Auch andere ungehemmte Sammeleien, wie die systematische Auswertungen von Kundendaten zu reinen Marketingzwecken, sind umstritten. Ebenso die Frage, ob die gesammelten Informationen bei Suchmaschinen wie Google oder auch bei Facebook zu Nutzerprofilen zusammengeführt werden können. Denn im Vergleich zu dem, was Google über uns weiss, erscheine mancher Geheimdienst „wie ein Kinderschutzbund", zitierte der SPIEGEL einen deutschen Fachhochschul-Professor (Speck 2008). Während die einen daher und immer lauter wirksame Schutzmassnahmen gegen Kinderpornographie und -missbrauch, schäbiges Denunziantentum wie bei *rotten neighbour* und anderen Schund im Netz fordern, sehen andere durch Überreaktionen bald auch Grundrechte wie Meinungsfreiheit bedroht. Die Meinungen zur Unterbindung von Missbräuchen im Netz sind daher nicht nur unter Interessengruppen und Fachleuten gespalten. Und mit immer neuen gesetzlichen Regelungen bis Verboten allein sei der zunehmenden Cyber-Kriminalität nach Einschätzung von Fachleuten ohnehin nicht beizukommen.

## Menschenrechte als Grundlage

Braucht es daher neue Grundrechte wie einen *Anspruch auf Anonymität*, fragte ein österreichischer Regierungsvertreter? Auch Annette Mühlberg, Referatsleiterin bei der deutschen Dienstleistungsgewerkschaft ver.di forderte einen wirksamen Schutz von Beschäftigten im Informationszeitalter: Denn „die zunehmende Online-Überwachung am Arbeitsplatz macht betrieblichen Datenschutz und dessen rechtliche Absicherung in einem Arbeitnehmerdatenschutzgesetz immer notwendiger". Die ver.di-Gewerkschaft hat dazu 2008 ein „Berliner Manifest: Öffentliche Dienste 2.0 – Die Daseinsvorsorge in der Informationsgesellschaft stärken!" verabschiedet (ver.di 2008). Auf einige Gemeinsamkeiten und Grundlagen konnte sich der erste Europäische Dialog zur Internet Governance (EuroDIG) bereits verständigen. Demnach müsse „die Regulierung des Internets auf der Grundlage der Menschenrechte erfolgen" (human rights-based), wie der französische Experte Bertrand de la Chapelle forderte. Im Zielkonflikt zwischen den Kernanliegen gilt die Formel: So viel Zugang und Offenheit wie möglich, so viel Sicherheit wie nötig. Auch dürften verbriefte Rechte und öffentliche Dienste „nicht zu profitablen Services verkommen". Die grössere Gefahr fürs Netz sehen Internet-Koryphäen wie Kleinwächter allerdings weniger bei regulierungswütigen Regierungen und durchsichtigen Wirtschaftsinteressen, sondern eher „bei unbedarften und naiven Usern" – und dagegen könnte nur Aufklärung und Befähigung helfen.

Neben der Vorübung auf das IGF 2008 in Hyderabad und der Verständigung über europäische Befindlichkeiten bei der Regelung des Netzes machte der erste Dialog noch eine Schwachstelle deutlich. Denn beim ersten EuroDIG vertreten waren vorwiegend Habende aus jenen Teilen Europas, die bereits über gute Infrastrukturen, passable Zugangsmöglichkeiten, Rechtsgrundlagen und dergleichen mehr verfügen. Jene Länder und südosteuropäischen Regionen, deren Bürger noch nicht über elementare Breitbandanschlüsse und andere Zugangsvoraussetzungen verfügen, blieben noch aussen vor. Der digitale Graben klafft auch weiterhin im vergleichsweise wohlhabenden Europa. Auch dieser Herausforderung wollten sich die Organisatoren beim geplanten Euro-Dialog 2009 stellen.

## Belgrad 2011: ein neuer Höhepunkt

Bei den auf Strasbourg folgenden jährlichen EuroDIG-Anlässen in Genf (2009), Madrid (2010) und Belgrad (2011) sind Interesse, Erwartungen und Beteiligung aus allen Stakeholder-Gruppen jeweils sprunghaft gestiegen. Am Rande gab es auch einige Befürchtungen, wonach mit dem Erfolg auch das Risiko oder etwaige Begehrlichkeiten auf Vereinnahmung wachsen könnten. Solche Ahnungen haben sich bislang jedoch nicht bestätigt, weil in den Gastgeberländern (*host countries*) jeweils andere Stakeholder die Federführung übernahmen und damit auch die nötige Ausgewogenheit gewährleistet werden konnte.

Ein vorläufiger Höhepunkt des Erfolgs war der letzte EuroDIG Ende Mai 2011 in Belgrad. Mit der Wahl des Konferenzorts sollte auch ein Zeichen hinsichtlich einer stärkeren Einbeziehung von europäischen Randregionen gesetzt werden. Denn eine digitale Spaltung gibt es durchaus auch in Europa. Während der zweitägigen Konferenz in der serbischen Hauptstadt waren über 500 Internetbewegte – etwa 100 davon über Fernteilnahme (*remote participation*) von zwölf regionalen Hubs – aus allen Teilen Europas beteiligt. Auch die Beteiligung von Jugendlichen stieg seit Strasbourg kontinuierlich und erreichte in Belgrad eine neue Qualität. Das Programm bot erstmals 20 Sessions (8 Plenaries, 8 Workshops sowie 4 Side events).

Mit dem Erfolg ging auch ein kontinuierlicher Reifungsprozess einher. Spätestens seit Belgrad lässt sich behaupten, dass EuroDIG inzwischen ein gesamteuropäisches Projekt ist und auch in Südost- und Osteuropäischen Ländern immer mehr wahrgenommen wird.


*Messages from Belgrade*
*http://www.coe.int/t/informationsociety/*

Neben der Bandbreite der behandelten Themen hat sich mit den Jahren auch die Diskurskultur deutlich verbessert. Prägten anfangs – zumindest in den Hauptteilen – noch überwiegend frontal verabreichte Experten-Beiträge die verschiedenen Pro-

**Wolf Ludwig**

**Wolf Ludwig** ist freier Medienjournalist in Neuchâtel/Schweiz, Vorsitzender von EURALO und ist seit Beginn am EuroDIG beteiligt.

### Exkurs: Internet Governance Forum (IGF)

Was vor Jahren noch als ziemlich verwegen schien, ein Diskurs auf Augenhöhe zwischen Regierungen, Wirtschaftsvertretern und jenen aus der Zivilgesellschaft über solch komplexe Fragen wie Internet Governance, ist seit Gründung des Internet Governance Forums (IGF) schon fast regulär geworden. Allen Skeptikern zum Trotz, schrieb der Weltgipfel zur Informationsgesellschaft (WSIS), von Genf 2003 bis Tunis 2005, mit der Gründung eines neuen Verhandlungsforums Geschichte. Seine schwierige Bewährungsprobe hat das Internet Governance Forum (IGF) nach den Premieren in Athen (November 2006) und Rio de Janeiro (November 2007) allemal bestanden. Das Interesse der Teilnehmenden, neudeutsch *Stakeholder*, war so unerwartet gross wie die Vielfalt der beim IGF jeweils behandelten Themen. Auch bei den nachfolgenden drei Anlässen hielten Zuspruch wie Zustrom unvermindert an.

An Zuständigkeit und Mandat dieses Internet-Weltforums wird zwar im UN-Gefüge weiterhin gefeilt. Einig ist man sich jedoch über dessen rein diskursiven Charakter, wobei Abstimmung und Zusammenarbeit unter den Interessengruppen (*Multi-Stakeholder*) wie auch anderen inter-governmentalen Organisationen (ITU, UNESCO nebst anderen) befördert werden soll (*enhanced cooperation*) – vgl. *http://www.intgovforum.org/*. Beobachter und Experten wie der Kommunikationswissenschaftler Wolfgang Kleinwächter wittern dabei auch Gefahr, dass derartige Foren zur reinen Routine verkommen, wenn irgendwann nur noch die ewig gleichen Verdächtigen zum IGF pilgern. Schon heute bemängeln VertreterInnen der Zivilgesellschaft die ungleichen Ressourcen und enormen Kosten für eine Beteiligung an den jährlichen Gipfeltreffen. Auch Regierungsvertreter wie Thomas Schneider, beim Schweizer Bundesamt für Kommunikation (BAKOM) für Internationales zuständig, sind sich dieser Probleme bewusst. Und vielen Regierungen, die beim Regulieren lieber unter sich bleiben und die Beteiligung anderer Gruppen als Einmischung in ihre Angelegenheiten betrachten, ist das IGF-Projekt ohnehin ein Dorn im Auge.

Das globale IGF wurde mit einer fünfjährigen Laufzeit als UN-Versuch auf Zeit konzipiert. Die Evaluation von 2010 hat nach fünf Anlässen überwiegend Lob und Empfehlung auf Fortsetzung ergeben. Ende September 2011 soll ein weiteres IGF in Nairobi stattfinden, doch die darauffolgende Zukunft ist aufgrund von UN-internen Widerständen (überwiegend aus dem totalitären Regierungslager) und mangels nachhaltiger Finanzierung weiterhin ungewiss.

grammteile (mit Powerpoint-Präsentationen und dergleichen), die oft zu wenig Raum für Diskussionen ließen, steht inzwischen der diskursive Dialog unter den Teilnehmenden im Vordergrund. Auch in diesem Bereich hat Belgrad neue Maßstäbe gesetzt. Bezeichnend dafür waren die Beiträge vorwiegend von jugendlichen Teilnehmenden, die in verschiedenen Debatten immer wieder Prinzipien des offenen und freien Zugangs einforderten. Andere warnten hingegen vor vereinfachten Erwartungsmustern, denn „Freibier oder Mahlzeiten gibt es nur, wenn andere (wie Sponsoren) dafür zahlen". Die unterschiedlichen Vorstellungen übers digitale Zeitalter zwischen den Eingeborenen (*digital natives*) und Immigranten (*migrants*) spiegelten sich auch in Belgrad deutlich wieder.

### Diskurs statt Bevormundung

Kurz vor dem letzten EuroDIG in Belgrad fand in Paris als Vorspiel auf den G8-Gipfel ein *E-G8-Forum* statt, zu dem Frankreichs Regierungschef Sarkozy eine handverlesene Schar von Regierungsvertretern und Wirtschaftsbossen geladen hatte. Die spärliche Beteiligung von Zivilgesellschaft war auf eine reine Alibiübung beschränkt. Kritiker sahen in der Veranstaltung ohnehin nur eine der üblichen Selbstinszenierungen des eitlen Staatspräsidenten mit magerem Resultat. Das *E-G8-Forum* setzte einen markanten Kontrapunkt zum EuroDIG-Konzept: herkömmliche Gipfelinszenierung, elitäres Top-down-Gehabe, abgehobenes Agendasetting – oder den Versuch, mit den Regeln und Verfahren von gestern die digitale Zukunft bewältigen zu wollen (Heise Online 2011). EuroDIG hingegen ist kein Schaulauf der Etablierten und Mächtigen, sondern bietet ein offenes Programm und gleichberechtigte Teilhabe aller an Netzfragen Interessierten. Bottom-up-Dialog statt Bevormundung durch Regierungsgewalt und machtvolle Wirtschaftsinteressen.

Nach der Erfolgsgeschichte von vier EuroDIG-Ausgaben steigen auch die Erwartungshaltungen an künftige Anlässe – so im Juni 2012 in Stockholm. Waren die Konferenzen bislang von einer kleinen Vorbereitungsgruppe weitgehend „nebenbei" und mit Minimalbudget organisiert, braucht es künftig ein kleines Sekretariat, um die wachsenden Anforderungen an einen offenen Organisationsprozess und einen professionellen Tagungsablauf zu bewältigen. Auch die jährlichen Finanzierungen des Euro-Dialogs, bislang überwiegend von privaten Sponsoren, müssen breiter abgestützt und besser abgesichert werden. Zur Stärkung der Organisationsstruktur soll Ende September 2011 – im Rahmen des nächsten IGF in Nairobi – auch ein Trägerverein für EuroDIG gegründet werden, in dem alle Stakeholdergruppen vertreten sind. Bei der weiterhin ungewissen Zukunft des globalen IGF nach Nairobi (siehe Kasten links) werden die regionalen Standbeine und Foren zur Verständigung über Regeln fürs Netz absehbar umso wichtiger.

## Quellen


Berliner Manifest: Öffentliche Dienste 2.0 – Die Daseinsvorsorge in der Informationsgesellschaft stärken!, ver.di-Fachbereich Gemeinden, Berlin, September 2008, http://governet.de/9

sowie Berliner Manifest zur Grundversorgung in der Netzgesellschaft, Heise Online, 5.09.2008, http://www.heise.de/newsticker/Berliner-Manifest-zur-Grundversorgung-in-der-Netzgesellschaft--/meldung/115541

EU-Dialog zu globalen Regeln im Netz, Heise Online, 20.10.2008, http://www.heise.de/newsticker/Europaeischer-Dialog-zu-globalen-Regeln-fuers-Netz--/meldung/117653

Gerke, Marko, zitiert nach „Weitere Konsultationen zur Netzzukunft geplant", Heise Online, 22.10.2008, http://www.heise.de/newsticker/Weitere-Konsultationen-zur-Netzzukunft-geplant--/meldung/117816

Speck, Hendrik, Internet, Operation Datenschatz, zitiert nach DER SPIEGEL 44/2008,

Von Datenschutz und Schäuble-Katalog: Terrorbekämpfung, TK-Überwachung, Online-Durchsuchung, Heise Online, 06.09.2007, http://www.heise.de/ct/hintergrund/meldung/95584
Frankreich will auf G8-Gipfel für Internetsperren werben, Heise- Online vom 18.05.2011, http://www.heise.de/newsticker/meldung/Frankreich-will-auf-G8-Gipfel-fuer-Internetsperren-werben-1244926.html

## Weitere Literatur

Kleinwächter, Wolfgang, Zu gross gedacht? Der WSIS kämpft mit seinen Ambitionen, Medeinheft.ch-Dossier, 28. November 2003, http://www.medienheft.ch/dossier/bibliothek/d20_KleinwaechterWolfgang.html
Kleinwächter, Wolfgang, Internet Governance – die Kontroverse des WSIS, Eine globale Ressource im Spannungsfeld nationaler Interessen , Medienheft.ch-Dossier 24, 14. November 2005, http://www.medienheft.ch/dossier/bibliothek/d24_KleinwaechterWolfgang.pdf
Ludwig, Wolf, Regulierer und Stellwärter der Netze, Die ICANN und das Internet Governance Forum, Medienheft.ch-Politik, 30. November 2007, http://www.medienheft.ch/politik/bibliothek/p07_LudwigWolf_06.pdf
Meier, Werner A., Die Informationsgesellschaft – eine Chimäre, Die Zivilgesellschaft auf der Suche nach mehr Demokratie, Medienheft.ch-Dossier 20, 28. November 2003, http://www.medienheft.ch/dossier/bibliothek/d20_MeierWernerA.pdf
Müller, Matthias, Vom Engagement zur Strategie, Kirchliche Hilfswerke am WSIS, Medienheft.ch-Dossier 20, 28. November 2003, http://www.medienheft.ch/dossier/bibliothek/d20_MuellerMatthias.pdf
Riehl, Frédéric, Der WSIS als Modellbeispiel für internationale Zusammenarbeit, Regierungen, Wirtschaft und Zivilgesellschaft im Dialog, Medienheft.ch-Politik, 21. Januar 2004, http://www.medienheft.ch/politik/bibliothek/p21_RiehlFrederic.pdf
Organised Crime in Europe: the threat of cybercrime, Council of Europe, Octopus Programme, Situation report 2004, Strasbourg, March 2005



**Dagmar Boedicker**

# Eine IT-Genossenschaft

## Funktioniert das?

*Leicht verklärter Blick zurück: Vor gut 20 Jahren war unsere Branche ein weitgehend sorgenfreies Arbeitsparadies – mit Raum für Selbstverwirklichung in Startups und mit sicheren Arbeitsplätzen in großen Unternehmen. Personalabbau unter den ITlern, gewerkschaftliche Organisation, Sozialpläne oder Betriebsräte gab es kaum, Burnout war ein Fremdwort und Near- oder Off-Shoring wäre an fehlender Infrastruktur und kulturellen Grenzen gescheitert. Wer damals selbstständig war, durfte mit guten Honoraren und weit gehend selbst gewählten Arbeitsbedingungen rechnen. Das ist heute anders, und nicht alle digitalen Nomaden oder Soloselbstständigen fühlen sich wohl im ausgesuchten Leben. Höchste Zeit, nach neuen Organisationsformen zu suchen.*

Eine Genossenschaft (oder Kooperative) ist ein Zusammenschluss von Personen, die gleiche oder ähnliche wirtschaftliche, soziale oder kulturelle Interessen gemeinsam verfolgen. Im Firmenportrait schreibt 7-it von Prinzipien wie Mitgliederförderung, Selbsthilfe, Selbstverantwortung und Selbstverwaltung und Identitätsprinzip (Identität von Entscheidungsträgern, Geschäftspartnern und Kapitalgebern). Irgendwie klingt das anstrengend. Aber gut klingt:

> *Genossenschaften sind auch Wertegemeinschaften. Im Mittelpunkt stehen die Mitglieder, nicht irgendwelche „Shareholder" mit dem Wunsch nach kurzfristiger Profit-Maximierung.* http://www.7-it.de/

Im Portrait der 7-it habe ich gelesen:

> *„In unserem geschäftlichen Verhalten orientieren wir uns an den Prinzipien des ‚Ehrbaren Kaufmanns' – siehe unter* http://www.veek-hamburg.de/zielsetzungen.php*"*

Ist das nicht ein bisschen aus der Mode? Ich verbinde es eher mit den Buddenbrooks als mit Apple oder Microsoft. Und frage Härtel, ob es beispielsweise Kunden gäbe, für die die eG nicht arbeiten würde. Klare Antwort: Nicht für Betrüger oder Ausbeuter.


*Mensch kann mitmachen*
*Foto: Dagmar Boedicker*

## Die 7-it eG in München

Die 7-it wurde vor neun Jahren von sieben ITlern gegründet und arbeitet vorwiegend für kleine und mittlere Unternehmen (KMU). Nur auf einem ihrer acht Geschäftsfelder, den Schulungen, hat sie auch große Unternehmen als Kunden. Horst Härtel (Gründer und Vorstand) und Rainer Friedl (Justiziar) geben Auskunft zu ihrer Genossenschaft. Friedl hat ein Zertifikat als DSB-TÜV und wird sich demnächst als Rechtsanwalt niederlassen, er erzählt, wie und warum er Mitglied wurde. Es war ein Prozess, der auch bei anderen Mitgliedern ähnlich verlief: Zunächst in Anstellungen, unter anderem beim Staat, machte Friedl sich selbstständig. Als Selbstständiger war er Einzelkämpfer, an Hierarchien weder gewöhnt noch von davon begeistert. Wie viele Selbstständige suchte er Partner für ein loses Netzwerk, das ihm seinen Freiraum erhalten und seine Konkurrenzfähigkeit steigern sollte. Noch einen Vorteil hat ein solches Netzwerk: Anders als bei einem Einzelkämpfer hängen Kunden nicht nur von einer Person und deren Verfügbarkeit ab, was die Auftragsvergabe aus Sicht der Kunden bedenklich macht. Unter den Teilnehmer/-innen des Netzes können Aufträge ausgetauscht und so eine Querauslastung erreicht werden.

Ab 20 Mitgliedern braucht eine eG einen Aufsichtsrat. 7-it hat 23 Mitglieder, der Aufsichtsrat tagt vier Mal pro Jahr und prüft die Finanzen und die Organisation. Außerdem muss sich der Vorstand in einer jährlichen Generalversammlung rechtfertigen und entlastet werden. Dabei hat jedes Mitglied eine Stimme, unabhängig von der Anzahl der Genossenschafts-Anteile. Apropos Anteil: jede Mitglied hat nur einen, der mit 2500 Euro relativ hoch ist. Vielleicht deswegen hat 7-it Fremdkapital weder gewollt noch gebraucht und trotzdem keine Probleme mit der Finanzierung oder Liquidität. Das liegt aber natürlich auch daran, dass jedes Mitglied seine eigene Ausstattung, Geschäftsräume oder Betriebsmittel selbst finanziert – mit Ausnahme einiger gemeinsam genutzter Hard- und Software.

## Und wer macht da mit?

Nach neun Jahren „unermüdlicher Werbung“ (Härtel) sind auch zwei Frauen zur 7-it gekommen. Zwar sind Frauen in der Informatik unterrepräsentiert, aber das ist wenig. Liegt es vielleicht daran, dass die Rechtsform der eG in der IT wenig bekannt ist? Härtel erzählt, dass er etwa eine Anfrage im Monat zur Gründung einer eG erhält und die Anfragenden dann auch berät. Er kennt alle nicht mal 20 aktiven Genossenschaften bundesweit und die eG kooperiert mit einigen, beispielsweise wenn spezielles Knowhow oder zusätzliche Kapazität gefragt ist oder sie ihren Standort weit von München entfernt haben.

Die meisten Mitglieder der 7-it waren vorher Angestellte oder Selbstständige, zwei sind direkt nach dem Studium gekommen. Meist ist es ein längerer Prozess, in dem über persönliche Kontakte eine Anfrage zu einem Auftrag kommt und die folgende Kooperation sich als angenehm und fruchtbar erweist. Als ich Härtel frage, was er von gewerkschaftlicher Organisation hält, findet er sie sehr sinnvoll – wohl nicht überraschend für einen Genossenschaftsgründer. Er selbst ist nicht organisiert, weil er sich als Selbstständiger nicht repräsentiert fühlte. Leider hab ich zu fragen vergessen, wie es bei den anderen Mitgliedern aussieht.

## Die Vorteile einer eG

2009 hat 7-it ihre Mitglieder befragt, welchen Nutzen sie aus ihrer Mitgliedschaft ziehen. Sie sehen Vorteile bei der Werbung, Marketing und Vertrieb. Dabei helfen ein gemeinsamer, professioneller Web-Auftritt und monatliche Kontakte zu Kunden und anderen ITlern über das *Forum 7-it, g*egenseitige Unterstützung bei der Akquisition oder wenn sie die Dienstleistung der Partner vermarkten. Nicht allein akquirieren zu müssen, führt dazu, dass die Mitglieder Aufträge erhalten, an die sie als Einzel-Unternehmer nicht gekommen wären. Überhaupt die Akquisition. In den neun Jahren ihres Bestehens hat 7-it vieles probiert: Kaltakquise hat nicht funktioniert, Netzwerken dagegen funktioniert gut. Ein Instrument dafür ist mit etwa 1000 Kontakten das Forum 7-it. Darin lernen die Mitglieder selbst dazu, und sie kommunizieren ihr Knowhow, knüpfen Kontakte zu Kunden und neuen Mitgliedern.

Nicht zu verachten sind die Provisionen, die anfallen, wenn ein Mitglied Aufträge vermittelt. Und es hilft, auf ein breites Spektrum an fachlichem und Branchen-Knowhow bei den Mitgliedern zugreifen zu können, das führt zu internem Wissens-Transfer und gegenseitiger kostenloser Unterstützung bei technischen Fragen oder Problemen. Auch die Qualitätssicherung wird einfacher durch die eG. Für Mitglieder und Kunden ist es beruhigend, wenn bei Abwesenheit (bei Urlaub oder im Krankheitsfall) ein Stellvertreter da ist. Überhaupt sind die Kontakte ein großer Vorteil, sei es zu diversen Berufs- und Interessen-Verbänden oder einem großen Netzwerk von IT-Fachleuten außerhalb der 7-it oder zu Gesprächspartnern, wenn einem im Home Office die Decke auf den Kopf fällt.

Klassische Genossenschaftsvorteile sind günstigere Konditionen bei der Beschaffung und Nutzung von Hard- und Software, der

**Dagmar Boedicker**

**Dagmar Boedicker** ist Journalistin und technische Redakteurin.
Sie hat Politikwissenschaft studiert.

Betriebs-Haftpflicht oder wenn man die Dienstleistung eines anderen Mitglieds benötigt.

### Aber?

Ist eine eG nicht anstrengender als eine andere Organisationsform? In der 7-it praktizieren 23 *Häuptlinge* Selbstverantwortung und Selbstverwaltung – geht das: IT ohne Hierarchie? Härtel verneint beides, es geht nicht ohne Führung, aber die ist auch nicht anstrengender, nur anders. Weisungsbefugt im Sinne einer disziplinarischen Ordnung ist eigentlich niemand, auch nicht der Vorstand. Er kann zwar die Regeln der Zusammenarbeit festlegen und weiterentwickeln, aber bei der täglichen Arbeit organisieren die Mitglieder sich selbst und tragen die Verantwortung. Als Selbstständige sind sie das ja gewöhnt. Projektleiter und Team können zwar vom Vorstand festgelegt werden, normalerweise macht das aber die Person, die den Auftrag akquiriert hat, und das Team findet sich fast von allein. Wenns brennt, ist allerdings ein Eingreifen möglich. Die Rolle des Vorstands ist trotzdem entscheidend, er entscheidet beispielsweise bei Investitionen, Marketing, Vertrieb, Organisation und Abwicklung von Projekten und bei der Aufnahme neuer Mitglieder.

Gibt es keinen Streit über Aufträge oder Anfragen und ihre Verteilung? Härtel sagt: „Nie". Vielleicht liegt das daran, dass nicht jede/r in eine Genossenschaft passt. Krasse Egoisten, beispielsweise, die nicht teilen können, Menschen mit Ellbogenmentalität. Solche Probleme regeln sich aber von allein, weil die anderen nicht mehr mit diesem Menschen arbeiten wollen. Unter den sechs ehemaligen Mitgliedern der 7-it, die sie seit der Gründung auch wieder verlassen haben, waren auch welche, die nicht passten. Genossenschafts-Mitglieder müssen teamfähig sein und bereit, sich auch mal ohne Bezahlung zu engagieren.



**Stefan Hügel**

## AC3 – der AKtiVCongreZ

*Bereits zum dritten Mal fand vom 7.-9. Oktober 2011 der vom FoeBuD organisierte AKtiVCongreZ statt – leider wohl zum letzten Mal im DGB-Bildungswerk Hamburg-Sasel, das aufgrund von Sparmaßnahmen des DGB geschlossen wird. Rund 50 netzpolitisch Aktive aus unterschiedlichen Organisationen trafen sich, um netzpolitische Themen zu diskutieren und die Aktivitäten der nächsten Zeit zu planen.*

Nach einem Rückblick auf die netzpolitischen Aktivitäten und Ereignisse seit dem letzten CongreZ wurde in mehreren Arbeitsgruppen einzelne Themen bearbeitet:

- Strategische Neubewertung der Gesamtlage: Einem gestiegenen Bewusstsein für netzpolitische Themen in der Öffentlichkeit stehen unklare Visionen und „Feindbilder" gegenüber. Die Bewegung zerfasert ein wenig, verschiedene Positionen zu einzelnen Themen – Beispiel Vorratsdatenspeicherung – werden erkennbar. Dagegen sollten gemeinsame Grundforderungen, stärker strategisch ausgerichtetes Denken, niederschwellige Angebote für Neueinsteiger und gemeinsame Symbole zur Identifikation gesetzt werden.

- Aktionsformen: Hier wird unterschieden zwischen Online- und Offline-Aktionsformen und Einzel- und Massenaktionen. Online- und Offline-Aktivitäten sollen dabei kombiniert werden.

- Auswertung der Demonstrationen „Freiheit statt Angst" in Berlin und Brüssel.

- Elektronische Verwaltung: Dazu sollen Kriterien für gutes E-Government zusammengestellt und verbreitet werden. Wesentliche Aspekte sind dabei Freiwilligkeit, Dezentralität, Datensparsamkeit und Zweckbindung nach BDSG, Transparenz, institutionalisierte Bürgerbeteiligung.

- Elektronische Gesundheitskarte: Der FoeBuD plant eine Kampagne zu dem Thema; das FIfF hat bekanntlich letztes Jahr eine Broschüre herausgegeben, die in dem Rahmen verwendet werden kann. Ein Infopaket für Ärzte soll zusammengestellt werden.

- Vorratsdatenspeicherung: Leider beginnt die Front gegen die Vorratsdatenspeicherung zu bröckeln, wie beispielsweise der jüngste Vorstoß der SPD zeigt. Die Vorratsdatenspeicherung muss weiterhin auf nationaler Ebene verhindert werden; auf europäischer Ebene müssen wir auf die Aufhebung der Richtlinie hinwirken.

- Social Swarm – soziale Netze, die die informationelle Selbstbestimmung fördern. Ausgehend von der öffentlichen Debatte über die Datenschutzproblematik bei Facebook sollen datenschutzfreundliche Angebote gefördert werden; dabei will man auf bestehende Plattformen zurückgreifen.

Zusätzlichen Diskussionsstoff bot vor allem die Nachricht von der Analyse des Staatstrojaners durch den Chaos Computer Club, die sich am Samstag abend schnell bei den Teilnehmern verbreitete.

Der nächste AKtiVCongreZ wird voraussichtlich im April/Mai 2012 im DGB-Bildungswerk in Hattingen stattfinden.

**Erklärung des FIfF e.V.**

# Zur Existenzberechtigung des Verfassungsschutzes

Wir haben das Vertrauen verloren in einen Verfassungsschutz, der seit Jahren rechten Terror verharmlost und linken Bürgerrechtlern misstraut und sie bespitzelt. Seit Jahren berichten die Medien über national befreite Zonen, von Rechten Zusammengeschlagene an Autobahn-Raststätten, über Hetzparolen bei rechten Auftritten, über Ausländer und Deutsche, die sich nicht in den Osten Deutschlands wagen. Wir haben Mölln, Solingen und Hoyerswerda nicht vergessen.

Um die Bundesjustizministerin zu zitieren: „Gibt es ein fester gefügtes rechtsextremistisches Netzwerk in Deutschland, als bisher angenommen wurde und auch festgestellt wurde?"

Am 18. November 2011 haben sich die Innenminister über Maßnahmen in der Folge der Morde durch drei Rechtsterroristen geeinigt – ja, auf was eigentlich? Sie wollen die Zusammenarbeit zwischen Polizei und Nachrichtendiensten verbessern und dazu eine Zentraldatei einrichten.

## Das rechtliche Instrumentarium für Prävention und Strafverfolgung reicht aus

Die Sicherheitsbehörden müssen es nur nutzen wollen, aber an diesem Wollen müssen wir zweifeln. Es fehlt nicht an Information, es fehlt an Einsicht, dass rechtsextreme Gewalttaten unser Gemeinwesen einschneidender gefährden als islamistischer Terror, und dass linke Kritik niemanden tötet. 38 Jahre lang hat der Verfassungsschutz den Rechtsanwalt, Publizisten und Bürgerrechtler Dr. Rolf Gössner beobachtet und dabei eine 2000 Seiten starke Akte über ihn angelegt. Hat er befürchtet, Gössner würde Bomben ins Verfassungsgericht werfen? Nach § 129a Abs. 5 StGB – Unterstützung von und/oder Werbung für eine terroristische Vereinigung – sind 13 Ermittlungsverfahren gegen Rechte geführt worden, an die 700 waren es gegen linke und muslimische Verdächtige. Das BKA-Gesetz räumt bedenklich weit gehende Befugnisse ein.

Das Bundes-Datenschutzgesetz (BDSG) §19 (3) lässt nur eingeschränkte Auskunftsrechte für die von Überwachung Betroffenen zu. Geheimdienste arbeiten mit nachrichtendienstlichen Methoden, die wir Bürger gar nicht und das Parlament und die Datenschutz-Beauftragten nur eingeschränkt und nur so kontrollieren können, dass die Kontrollergebnisse nicht öffentlich werden. Soll die Polizei nun mit diesen Ermittlungsresultaten umstrittener Methoden auf Verbrecherjagd gehen? Soll sie sie im Auftrag einer Staatsanwaltschaft bei Gericht vorlegen, um zu wiederholten Malen feststellen zu müssen, dass sie einer rechtsstaatlichen Überprüfung nicht standhalten und vom Gericht möglicherweise nicht als Beweismittel zugelassen werden? Zwar lassen die Gerichte schon auch mal Beweismittel zu, die auf obskuren, teils illegalen Wegen gewonnen wurden – das schadet aber den Gerichten, der Polizei und dem Rechtsstaat in den Augen einer kritischen Öffentlichkeit.

Wir teilen die Auffassung der Humanistischen Union: „Wer angesichts der eklatanten Fehleinschätzungen des thüringischen Verfassungsschutzes eine engere Zusammenarbeit des Geheimdienstes mit der Polizei fordert, überträgt dessen zweifelhafte Methoden auf die polizeiliche Arbeit und gefährdet damit zentrale rechtsstaatliche Sicherheiten." Das Trennungsgebot darf nicht angetastet werden.

## Mitgefühl und Solidarität

Wir fühlen mit der Gemeinschaft der Bürgerinnen und Bürger, die sich nach den Hinrichtungen durch die drei Terroristen aus Thüringen selbst Verdächtigungen ausgesetzt sahen, obwohl die Umstände der Taten auf rechtsextreme Motive hinwiesen.

Menschen, die sich mit großem persönlichen Risiko gegen Rechts engagieren, lässt die Politik allein. Zivilcourage wird nicht ermutigt. Es scheint einfacher zu sein, der Pawlowschen Datensammelwut freien Lauf zu lassen, als sich mit den Ursachen des Rechtsextremismus auseinanderzusetzen.

Wir fordern mehr Aufklärung statt mehr Daten, vor allem aber die lang- statt kurzfristige Förderung von Projekten wie „Schule ohne Rassismus" und von Initiativen gegen den braunen Sumpf. Der Verfassungsschutz hat die 182 Todesopfer rechten Terrors, die Nichtregierungsorganisationen zählen, nicht verhindert. Er hat sich nicht als hilfreich erwiesen und schadet dem Rechtsstaat mehr als er nützt.

**Ute Bernhardt**

schwerpunkt

# Mahnen und Aufklären – Information Warfare und FIfF

*Was kann und wird passieren, wenn Computer zum Instrument der Kriegsführung werden? Welchen Einfluss haben Militärs auf die Informatik genommen? Was ist aus Informatik-Sicht von der Idee zu halten, Computer könnten einen Krieg besser führbar machen? Angenommen, man hielte das Führen von Kriegen für eine gute Idee: kann es jemals Computer geben, die dafür jemals zuverlässig und sicher genug sind?*

Diese und einige andere Fragen waren der Ausgangspunkt für die Gründung des FIfF zu einem Zeitpunkt, als die militärische Seite der Informatik wissenschaftlich, in den Berufsorganisationen und erst recht in der Öffentlichkeit unbekannt oder unbeachtet blieb.

Ziel des FIfF war, diese Unkenntnis der Verquickungen transparent zu machen und zur Diskussion zu stellen. Dazu erschienen 1983[1] und 1984[2] in kurzer Folge zwei Publikationen, und darin eine erste wissenschaftliche Aufarbeitung der Historie „Von der Feuertafel zum Kampfroboter" im deutschsprachigen Raum von Reinhard Keil. Die Folgen für die Informatik-Fachgebiete Software Engineering, Integrierte Schaltkreise, für die Informatik-Forschung und die Wissenschaft, sowie für sicherheitspolitische Fragestellungen und die damit verbundenen ethischen Fragen behandelten Joachim Bickenbach, Eike Best, Manfred Domke, Christiane Floyd, Helga Genrich, Klaus Haefner, Friedrich Holl, Rudolf Hollenbach, Reinhold Kimm, Hans-Jörg Kreowski, Werner Langenheder, Michael Löwe, Frieder Nake, Fanny-Michaela Reisin, Ingo Ruhmann, Jörg Siekmann und Rudolf Wilhelm.

Dennoch blieb es innerhalb der Informatik eine Nestbeschmutzung, auch nur die aufklärerische Frage zu stellen, in welcher Weise die Informatik durch militärische Interessen beeinflusst sei. Dies endete mit dem ersten Golfkrieg 1990/91 und dem über alle TV-Kanäle flimmernden Einsatz von „intelligenter" Präzisionsmunition. Die vorher abgestrittene Bedeutung, die Computer für die Kriegsführung haben, wurde danach nicht mehr verneint, sondern untersucht[3]. Die kritische Auseinandersetzung mit Informatik und Militär ist mittlerweile Bestandteil von Lehrbüchern[4].

Im FIfF wurde das Thema Cyberkrieg als Teil der militärischen Nutzung der IT intensiver aufgearbeitet und hinterfragt. Auch der Deutsche Bundestag beschäftigte sich mit den aus dem IT-Einsatz folgenden Konsequenzen für die Sicherheitspolitik und für die Rüstungskontrolle. Das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) beauftragte das FIfF 1994/95 mit einer systematischen Studie zum IT-Einsatz in der Kriegsführung und den Konsequenzen für Rüstung und Rüstungskontrolle[5] – dies war erneut die erste Analyse im deutschsprachigen Raum und zudem die über 10 Jahre einzige dieser Art im zivilen Bereich.

Die Konsequenzen von militärischen Hackerangriffen auf die zivile Nutzung der IT waren dabei von Beginn an unmißverständlich klar: „Militärische Sicherheitskonzepte und Bedrohungen sind die dominanten Einflußgrößen unseres informationellen Selbstbestimmungsrechtes"[6]. Leider haben sich die Warnungen vor den Folgen von Cyber-Kriegsführung nur allzu genau bewahrheitet: „Der Computer hat die Kriegsführung so grundlegend verändert, daß der Krieg als politische Option wieder führbar, da gewinnbar ist. [...] Mit dieser Kriegsoption für die hochentwickelten Staaten hat sich die weltpolitische Lage ebenso grundlegend verändert wie durch den Abbau der Spannungen zwischen Ost und West. Militärs halten die Entwicklungen in der Informations- und Kommunikationstechnik für wichtiger als die Entwicklung der Atombombe"[7].

Das FIfF hat bei seiner Gründung davor gewarnt, militärische Aktionen durch prinzipiell unsichere Computersysteme überwachen und ausführen zu lassen. In den vergangenen 25 Jahren sind Computer nicht zuverlässiger geworden. Die in dieser Zeit geführten Kriege und die gewachsene Bedeutung von Computern für Militärs haben aber gezeigt, dass es um Pseudorationalität von Technologie geht: In Zukunft soll der Unterschied von Simulation und Realität, so weit dies technisch möglich ist, verwischt werden. Aus der Simulation wird das „synthetische Environment". Der reale Krieg wird komplementiert durch sein virtuelles Abbild, das auf dem Internet und dem globalen militärischen Kommando- und Kontrollsystem abläuft.

Gerade die Kriege im Irak und in Afghanistan haben mit vielen Opfern gezeigt, dass Simulation und Realität weit auseinander klaffen. Die auf dem digitalen Feldherrenhügel zusammenlaufende Datenflut ermöglicht nicht allein eine Planung von Militärhandlungen, sondern bereinigt die chaotische Realität des Krieges zu steuerbaren Abläufen.

Es ist dieses computergestützten militärischen Systemen innewohnende Ziel der Machtprojektion, das den Sinn der im globalen Kommando- und Kontrollsystem bestehenden innigen Ver-

**Ute Bernhardt**

**Ute Bernhardt**, Informatikerin, wissenschaftliche Referentin und Lehrbeauftragte, Gründungsmitglied und ehemalige stv. Vorsitzende des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Arbeiten zu Datenschutz, Bürgerrechten sowie Informatik und Militär.

bindung von Computern und Militär erklärt: Computergestützte militärische Systeme dienen dazu, die Projektion militärischer Macht besser steuerbar und kontrollierbar zu machen.

Diese Form der Realitätssimulation und deren Steuerung in „War Rooms“ ist nicht auf Krisen und Kriege beschränkt. Ziel einer permanenten Simulation ist die Steigerung der Einsatzfähigkeit. Militärische Eingreiftruppen, die auf mögliche Einsätze umfassend vorbereitet sind, sollen dadurch jederzeit auf Abruf zur Verfügung stehen. Nicht zuletzt deswegen bezeichnet die US Army ihre als Force XXI bezeichnete Konzeption zukünftiger Landstreitkräfte als „strategische Armee", als Kampfeinheit, die zur Erreichung strategischer Ziele gedacht ist[8]. Voraussetzung dafür ist jedoch die andauernde Aufklärung all dessen, was möglicherweise militärisch bedeutsam werden könnte.

Der Computer hat heute für Militärs die Funktion eines allumfassenden Steuerungswerkzeugs[9]. Dies ist kaum ein Mittel zur friedlicheren Konfliktlösung, sondern hat nur einen Wert, wenn es darum geht, politische Interessen mit der Drohung militärischer Gewaltanwendung durchzusetzen. Die technologische Vormachtstellung in der Informationstechnik ist damit zum notwendigen Mittel für die Erhaltung militärischer Überlegenheit geworden.

Das FIfF und die Arbeit zum Thema „Informatik und Militär“ ist deshalb leider auch im Jahre 2011 weiterhin nötig.

## Anmerkungen

1 *Bickenbach, Genrich, Keil, Langenheder, Reisin: Informatiker für Frieden, Informatik für Krieg, Berlin 1983*

2 *Bickenbach, Keil, Löwe, Wilhelm: Militarisierte Informatik, Marburg, 1984*

3 *Ute Bernhardt; Ingo Ruhmann (Hrsg.): Ein sauberer Tod. Informatik und Krieg. Marburg, 1991*

4 *Ute Bernhardt; Ingo Ruhmann: Informatik und Militär. In: Jürgen Friedrich; Thomas Herrmann; Max Peschek; Arno Rolf (Hrsg.): Informatik und Gesellschaft, Heidelberg, 1995, S. 98-104*
*vgl. auch: Jürgen Altmann, Ute Bernhardt; Kathryn Nixdorf, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung. Lehrbuch. Wiesbaden, 2007*

5 *Ralf Klischewski, Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie; Gutachten für das Büro für Technikfolgenabschätzung des Deutschen Bundestages, Bonn, März 1995*

6 *Ute Bernhardt, Ingo Ruhmann: Netze des Todes; In: dies.: Ein sauberer Tod. Informatik und Krieg, Marburg, 1991, S. 1-6, S. 2*

7 *Ute Bernhardt, Ingo Ruhmann: Netze des Todes; In: dies.: Ein sauberer Tod. Informatik und Krieg, Marburg, 1991, S. 1-6, S. 2*

8 *Tradoc 525-5, S. 12; http://earthops.org/tradoc525/525-5toc.html*

9 *vgl. Ute Bernhardt; Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle. In: Wissenschaft und Frieden, Heft 1/97, Dossier Nr. 24, S. 1-16*



**Hans-Jörg Kreowski**

# Gehören Killerroboter vor ein Kriegsgericht?

*Seit einigen Jahren kann man in vielen Printmedien hin und wieder von Drohnen lesen, die im Grenzgebiet von Afghanistan und Pakistan eingesetzt worden sind, um führende Mitglieder von Al Kaida und den Taliban aufzuspüren und mit Raketen anzugreifen. Dabei sind inzwischen Hunderte Menschen getötet worden, darunter viele Frauen und Kinder. Vorläufig werden die Einsatzbefehle noch aus der US-Kommandozentrale in der Wüste von Nevada gegeben. Aber es wird durchaus daran gedacht, solche Drohnen zukünftig autonom über den Waffeneinsatz und damit über die Tötung aller Personen im Zielbereich entscheiden zu lassen. Da dabei sicherlich nicht nur kämpfende Soldaten den Tod finden werden, nach dem geltenden Kriegsrecht aber Zivilpersonen von Kriegshandlungen verschont werden sollen, könnte man fragen, ob dann Killerroboter vor ein Kriegsgericht gehören.*

### Killerroboter

Nach der *Unmanned Systems Roadmap* 2007-2032 und der *Unmanned Systems Integrated Roadmap* 2011-2036 plant das Department of Defense der USA in den nächsten Jahrzehnten einen erheblichen Teil der Waffensysteme in der Luft, auf dem Land und zu Wasser auf unbemannte Vehikel umzustellen. Diese Geräte sollen ihre Aufgaben zu einem großen Teil autonom erfüllen. Und da sie keineswegs nur der Erkundung, Bewachung und Aufklärung dienen, sondern viele davon auch bewaffnet sind, handelt es sich um ein Programm für die Entwicklung und Verwendung von Killerrobotern. Aber solche Waffensysteme sind keine reine Zukunftsmusik, sondern seit einigen Jahren mit wachsender Tendenz bereits im Einsatz im Irak, Afghanistan, im Grenzgebiet von Pakistan und jüngst auch in Libyen. Zu den bekanntesten unbemannten Fluggeräten (Drohnen) gehören der Predator und der Reaper. Der Predator war ursprünglich für die Aufklärung gedacht, ist inzwischen aber mit zwei Hellfire-Raketen ausgestattet. Der Reaper war von Anfang an mit acht Hellfire-Raketen bewaffnet. Das bekannteste bewaffnete unbemannte Landfahrzeug ist das Talon Sword, ein kleines Kettenfahrzeug, das mit verschiedenen Waffen wie Maschinengewehr oder Granatwerfer bestückt werden kann. Auf dem Wasser schwimmt beispielsweise der Protector, unter Wasser der Swordfish. Aber nicht nur die USA, sondern auch viele andere Länder der Welt haben, kaufen, entwickeln und bauen inzwischen unbemannte Militärsysteme. Dazu gehört auch Deutschland beispielsweise mit den unbemannten Fluggeräten Aladin, Luna, Mikado und KZO.

### Kriegsvölkerrecht

Das Kriegsvölkerrecht hat zwei Seiten. Die eine betrifft alle rechtlichen Aspekte im Zusammenhang mit der Frage, welche Rolle Krieg und Frieden beim Zusammenleben der Völker spielen

sollen (*ius ad bellum*). Hierzu gehört zum Beispiel die Aussage in der Präambel der UN-Charta, mit der sich die Mitgliedsstaaten verpflichten, die zukünftigen Generationen von der Geißel des Krieges zu befreien, oder wie es im Artikel 2 heißt:

> *„ ... Alle Mitglieder legen ihre internationalen Streitigkeiten durch friedliche Mittel so bei, dass der Weltfriede, die internationale Sicherheit und die Gerechtigkeit nicht gefährdet werden. Alle Mitglieder unterlassen in ihren internationalen Beziehungen jede gegen die territoriale Unversehrheit oder die politische Unabhängigkeit eines Staates gerichtete oder sonst mit den Zielen der Vereinten Nationen unvereinbare Androhung oder Anwendung von Gewalt."*

Die zweite Seite tangiert alle rechtlichen Regeln, die im Krieg gelten sollen (*ius in bello*). Die Haager Landkriegsordnung und die Genfer Konventionen sind bekannte Beispiele für völkerrechtlich verbindliche Vereinbarungen in diesem Zusammenhang. Zu den Regeln gehört, Opfer von Kriegen, Wehrlose und Unbeteiligte zu schützen, wobei insbesondere der Angriff auf Zivilpersonen verboten ist. Außerdem sollen kulturelle Güter geschont werden. Wer diese Regeln missachtet, kann als Kriegsverbrecher vor nationalen oder internationalen Gerichten angeklagt und verurteilt werden. Solche Prozesse hat es seit den Nürnberger Prozessen vereinzelt immer wieder gegeben. Gleichzeitig muss konstatiert werden, dass in allen Kriegen der letzten Jahrzehnte viele Kriegsverbrechen begangen worden sind, ohne dass sie einen Richter gefunden hätten. Als typische Beispiele, die hundertfach in den letzten Jahren passiert sind, kann man hier die Drohneneinsätze im Krieg gegen Al Kaida und die Taliban nennen, bei denen weit mehr Zivilpersonen, insbesondere Frauen und Kinder, getötet worden sind als feindliche Kämpfer. Typische Nachrichten, die in den letzten Jahren um die Welt gingen, belegen die Bedeutung und Problematik der fliegenden Killerroboter:

- Chef der pakistanischen Taliban von Drohne getötet.
- CIA lässt Todes-Drohnen nicht mehr von Blackwater bestücken.
- 30 Menschen von amerikanischen Drohnen getötet.
- Einsatz von Drohnen statt neuer Truppen.
- US-Drohne zerstört Haus mit sechs Taliban – 28 Tote insgesamt.

Und diese Liste der Meldungen ließe sich beliebig verlängern. Die meisten dieser Drohneneinsätze sind, soweit ich das sehe und verstehe, vom Kriegsvölkerrecht nicht gedeckt.

Es ist erklärte Absicht der Militärplaner und -entwickler, die Autonomie von Killerrobotern weiter voranzutreiben. In naher Zukunft werden bewaffnete Drohnen nicht erst schießen, wenn sie einen entsprechenden Befehl aus der Einsatzzentrale erhalten, sondern selbst darüber entscheiden. Die Entscheidung über Leben und Tod soll damit Maschinen überlassen werden. Killerroboter sollen selbsttätig töten, sobald sie einen generellen Einsatzbefehl erhalten. Daraus ergeben sich eine Reihe drängender Fragen:

- Darf die Entscheidung über Leben und Tod Maschinen überlassen werden?
- Können Maschinen das Kriegsvölkerrecht kennen und respektieren?
- Können sie zwischen gegnerischen Kampftruppen einerseits und Unbeteiligten und Wehrlosen andererseits unterscheiden?
- Können sie kulturelle Güter schonen?
- Können sie in diesem Sinne ethisch korrekt funktionieren?

**Maschinenethik und künstliches Gewissen!?**

Es gibt viele Fachleute im Umfeld der Killerrobotik, die diese Fragen bejahen. Stellvertretend sei hier die Auffassung von Ronald C. Arkin vom Georgia Institute of Technology wiedergegeben. Er führt in seinem Buch *Governing Lethal Behaviour in Autonomous Robots* aus, dass Maschinenethik nicht nur möglich, sondern wünschenswert sei. Als Gründe führt er an, dass Roboter im Gegensatz zu menschlichen Kriegern nie in Panik geraten und dass sie Befehle beurteilen und ohne Rücksicht auf die Konsequenzen gegebenenfalls auch verweigern können.

Ein solcher Glaube in die nahezu unbegrenzte technische Machbarkeit ist bei den Ingenieurswissenschaften, dem Militär und der Politik weit verbreitet. Ein Grund dafür ist insbesondere auch, dass mit Versprechungen dieser Art gigantische Fördermittel locker gemacht werden können. Die Erbauer von Killerrobotern und ihre Auftraggeber machen da keine Ausnahme – eher im Gegenteil.

Ich dagegen bin überzeugt, dass die Vorstellung von Maschinen, die selbständig ethisch handeln können, völlig illusionär ist und dass ein künstliches Gewissen vor allem künstlich ist und mit Gewissen nichts zu tun hat. Insbesondere denke ich, dass alle Fragen am Ende des vorigen Abschnitts mit einem klaren und uneingeschränkten NEIN beantwortet werden müssen. Das möchte ich im folgenden aus meinem wissenschaftlichen Verständnis von den Möglichkeiten und Grenzen der Informatik heraus begründen.

**Hans-Jörg Kreowski**

Prof. Dr. **Hans-Jörg Kreowski** ist Leiter der Forschungsgruppe Theoretische Informatik an der Universität Bremen. Er ist Gründungsmitglied des FIfF e.V. und war von 2003 bis 2009 dessen Vorsitzender.

### Alles eine Frage der Modellierung und Programmierung

Wenn davon die Rede ist, dass Maschinen Entscheidungen treffen, dann ist damit gemeint, dass in die Maschinen Computer eingebettet sind, auf denen Programme laufen, die die sogenannten Entscheidungen berechnen. Und alle solchen Programme werden von Menschen erdacht, modelliert und entwickelt, und berechnen, abgesehen von technischen Fehlfunktionen, nichts anderes als das Programmierte.

Nach der Turingschen These aus dem Jahr 1936 kann alles Berechenbare – egal mit welchem Programm auf welchem Computer – auch mit einer Turing-Maschine berechnet werden, die eine Art Buchhalter formalisiert. Wenn die These stimmt (und bisher spricht eigentlich nichts dagegen, aber vieles dafür), dann hat das einige interessante Konsequenzen:

- Es gibt Probleme, die nicht berechenbar sind, für deren Lösung es also gar kein Programm gibt.
- Es gibt Programme mit unbekanntem Verhalten.
- Es gibt Programme, die zu viel Zeit und/oder Speicherplatz brauchen, die also länger brauchen, als ein Mensch warten kann, und für deren Datenhaltung die Atome im Universum nicht reichen.
- Es gibt Programme, die unzuverlässig sind.
- Es gibt berechenbare Probleme ohne bekannte Lösung, für die also kein Programm verfügbar ist.
- Ob ein Problem von einem Programm exakt gelöst wird, ist fast nie bewiesen und im allgemeinen auch nicht beweisbar.

Was heißt das für ein Programmsystem, das „ethisches Verhalten" von Maschinen realisieren soll? Die obige Liste von Schwierigkeiten beim Umgang mit Berechenbarkeit lässt sich auf dieses spezielle Programmierungsproblem übertragen:

- Es könnte nicht berechenbar sein.
- Es könnte völlig undurchschaubar programmiert sein.
- Es könnte zu viel Zeit oder/und Speicherplatz brauchen.
- Es könnte unzuverlässig sein.
- Es könnte berechenbar sein, aber niemand weiß wie.
- Es könnte unbewiesen sein und bleiben, dass es richtig funktioniert.

Ich wäre nicht verblüfft, wenn sich ethisches Verhalten als unberechenbar erwiese, so dass sich eine maschinelle Realisierung auf den berechenbaren Teil beschränken müsste. Aber auch diese „berechenbare Ethik" ist in ihren Inhalten, Möglichkeiten, Gesetzmäßigkeiten und Charakteristika völlig unklar, und an einer operationalisierbaren Modellierung fehlt es gänzlich. Beispielsweise liegen die normativen Bestimmungen des Kriegsvölkerrechts nur in natürlicher Sprache vor. Es gibt für sie keine eindeutigen Interpretationen, und sie stellen in keiner Weise präzise Handlungsanweisungen dar. Wie soll daraus ein ausführbares Programm werden, das tut, was es soll? Das ist hoffnungslos.



Killerroboter, unbemannte Vehikel und autonome Waffen sind nach diesen Überlegungen nicht in der Lage, nach ethischen Prinzipien zu funktionieren und das Kriegsvölkerrecht zu beachten. Es ist deshalb unverantwortlich und gefährlich, solche Systeme zu entwickeln und einzusetzen. Die Entwickler und Einsatzleiter machen sich zu potentiellen Mördern. Wie Landminen werden autonome Tötungsmaschinen keinen Unterschied machen können zwischen kämpfenden Soldaten und Zivilpersonen. Als Waffen, deren Einsatz praktisch unweigerlich im Widerspruch zum Kriegsvölkerrecht steht und ein Kriegsverbrechen darstellt, gehören sie wie biologische und chemische Waffen verboten. Spätestens an dieser Stelle erweist sich die Titelfrage als rhetorisch. Denn es sind nicht die autonomen Killerroboter, die die Kriegsverbrechen begehen werden, sondern wie auch jetzt schon beim Raketeneinsatz mit Drohnen die Befehlshaber, die solche Waffen einsetzen. Die Entwickler und Programmierer können aber ebenfalls nicht freigesprochen werden, denn sie werden wissen, was sie tun.

### Künstliche oder echte Torheit

Wenn man postuliert, dass Maschinen mit ethischem Verhalten gebaut werden könnten und dass ein künstliches Gewissen programmierbar sei, und wenn man dann – wie in der Killerrobotik geplant ist – damit beginnt, solche Vorstellungen zu realisieren, gerät man aus meiner Sicht in ähnliche Kalamitäten wie die Künstliche Intelligenz (oder in noch schlimmere). Führende Vertreter des Fachgebiets wie McCarthy, Minsky, Kurzweil und Moravec behaupten und propagieren seit den 1950er Jahren, dass künftig Maschinen entworfen und gebaut werden können, die intelligent sein und besser denken werden als Menschen. Das ist glücklicherweise keine Mehrheitsmeinung in der Künstlichen Intelligenz. In dem Fachgebiet sind in den letzten Jahrzehnten sehr beachtliche Erkenntnisse gewonnen und viele bemerkenswerte Resultate erzielt worden. Aber alles, was hervorgebracht wurde, ist nach meinem Verständnis ganz ähnlich zu dem, was an wissenschaftlichen Fortschritten in der Informatik insgesamt erreicht wurde. Soweit es um „kognitive" Fähigkeiten geht, die von Maschinen und ihren Programmsystemen erbracht werden, handelt es sich um äußerst eng begrenzte Phänomene, die mit der Intelligenz von Lebewesen wenig bis gar nichts zu tun haben. Es sind – zugegebenermaßen teils sehr eindrucksvolle – technische Imitationen von Einzelleistungen, die bei Mensch und Tier Intelligenz erfordern. Aber wenn eine Maschine bellt, ist sie noch lange kein Hund.

Intelligenz, Denkvermögen, Gefühle, Moral, ethisches Verhalten und Gewissen sind vor allem auch deshalb nicht im Handumdrehen oder in wenigen Jahren als Programmsysteme realisierbar, wenn überhaupt je, weil niemand wirklich weiß, worum es sich dabei tatsächlich handelt und wie diese kognitiven Fähigkeiten vollständig, korrekt und algorithmisch machbar charakterisiert werden können. Auf kurzfristige Lösungen zu hoffen, ist aus meiner Sicht reine Torheit.

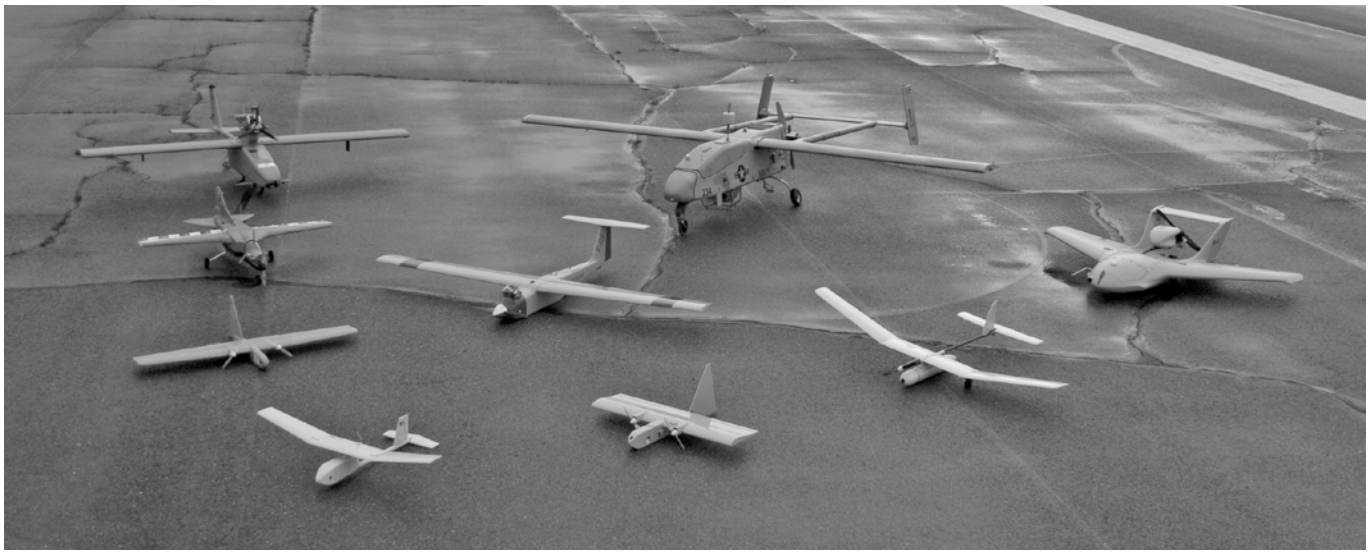
**Eric Töpfer**



# Die Himmelsstürmer

## Wie die Drohnenlobby ihren Kriegsrobotern den zivilen Luftraum öffnet

*Global Hawk, Predator, Reaper, Heron, Luna, Hunter, Aladin, Raven oder Mikado – seit mehr als 40 Jahren fliegen Drohnen in Kriegsgebieten und über militärischem Sperrgebiet. Den eigentlichen Durchbruch für ihren Einsatz brachte der „globale Krieg gegen den Terror": Flogen Drohnen des US-Militärs im Jahr 2001 12.500 Stunden am Himmel, waren es 2010 bereits mehr als 560.000 Stunden.*[1] *6.000 dieser Unmanned Aerial Vehicles (UAVs) gehören heute zur fliegenden Armada des Pentagon, und bis 2020 ist die Aufrüstung der Flotte für mehr als 36 Milliarden US-Dollar geplant.*[2]



*A group photo of aerial demonstrators at the 2005 Naval Unmanned Aerial Vehicle Air Demo*
*Quelle: http://www.news.navy.mil/management/photodb/photos/050627-N-0295M-021.jpg*

Auch die Bundeswehr setzt verstärkt auf den Einsatz von Drohnen. Zwar verfügt sie bislang „nur" über etwa 200 unbemannte fliegende Systeme,[3] aber die Marschrichtung steht. Im „Weißbuch 2006 zur Sicherheitspolitik Deutschlands und der Zukunft der Bundeswehr" heißt es: „Die Fähigkeiten zur luftgestützten, abstands- und allwetterfähigen Überwachung und Aufklärung sollen künftig vor allem durch unbemannte, in mittleren und großen Höhen operierende Luftfahrzeuge sichergestellt werden."[4] Weiterentwickelt werden die Vorgaben durch die „Konzeptionellen Grundvorstellungen (KGv) zum Einsatz unbemannter Luftfahrzeuge in der Bundeswehr" vom 21. Februar 2008, die als aktuelle Einsatzoptionen insbesondere die Aufklärung, langfristig aber auch den Einsatz von Waffen nennen.[5] Entsprechend finden sich Drohnen an fünfter Stelle in der Liste der „Gemeinsamen Erklärung zu wehrtechnischen Kernfähigkeiten" des Verteidigungsministeriums und der deutschen Rüstungsindustrie vom 20. November 2007.[6] Für die nächsten Jahre ist die Anschaffung von rund 500 weiteren Drohnen geplant.[7]

Das Problem für den militärisch-industriellen Komplex ist dabei allerdings: Trotz hoher Entwicklungskosten nimmt das Militär nur vergleichsweise geringe Stückzahlen ab. Begrenzt sind entsprechend die Gewinne für die Industrie und hoch die Stückkosten für die Rüstungsbeschaffer. Die Lösung: Es gilt, gemeinsam den Markt für Drohnen zu entwickeln. Und so hat das Bundesverteidigungsministerium den deutschen Drohnenherstellern bereits zugesagt, sie beim Export ihrer Produkte zu unterstützen.[8] Als schwierig hingegen erweist sich die Expansion auf dem heimischen Markt. Denn für den nicht militärisch segregierten Luftraum sind UAVs – außer im Modellflugbereich – aus Gründen der Flugsicherheit nur als Ausnahme zugelassen. Diese „Innovationsbarriere" soll nun beseitigt werden.

### Visionen des militärisch-industriellen Komplexes

Für Kreise jenseits des Militärs und der Rüstungsindustrie wurden Drohnen erstmals zum Thema, als die Europäische Kommission im Juli 2002 ihren „Strategic Aerospace Review for the 21st Century" (STAR 21) vorlegte. Erarbeitet von einer „Advisory Group" aus fünf EU-Kommissaren, Topmanagern sechs großer europäischer Luft- und Raumfahrtkonzerne,[9] dem Hohen Vertreter für die Gemeinsame Außen- und Sicherheitspolitik, Javier Solana, sowie zwei Europaparlamentariern sollte der Bericht Empfehlungen liefern, wie der industriepolitische Rahmen für die europäische Luft- und Raumfahrtindustrie zu gestalten sei, um Europa ökonomisch wettbewerbsfähig und militärpolitisch unabhängig zu machen. Nicht zuletzt vor dem Hintergrund des Kosovo-Krieges, bei dem erstmals Drohnen verschiedener NATO-Staaten in größerem Maßstab Echtzeitbilder von den Schlachtfeldern lieferten,[10] heißt es:

> *„Das Wesen der Kriegsführung erlebt einen fundamentalen Wandel. […] Hierzu gehört der Einsatz von unbemannten Luftfahrzeugen sowohl zur Überwachung als auch zur Projektion militärischer Stärke. Die meisten*

*Technologien, die für diese neue Fähigkeit benötigt werden, sind generisch. Der Einsatz von unbemannten Systemen kann ein verlässliches und kosteneffizientes Mittel zur Überwachung und Datenmanagement beim Schutz von Fischbeständen, bei Grenzkontrollen, Polizeieinsätzen, Rettungsaktionen und für viele andere Anwendungen mit einem beachtlichen Marktpotenzial sein. Sowohl zivile als auch militärische Anwendungen können und sollten von der europäischen Luftfahrtindustrie adressiert werden. […] Falls Europa keine eigenen unabhängigen Kapazitäten in diesem Bereich aufbaut, […] wäre dies eine ernsthafte Einschränkung der Fähigkeiten, eine wichtige Rolle in Militäroperationen an Seiten der USA zu spielen und, noch wichtiger, unabhängige Aktionen durchzuführen."*[11]

In den späten 1990er Jahren hatten sich in Europa verschiedene, teilweise konkurrierende Netzwerke von Drohnenherstellern und militärnahen Forschungseinrichtungen organisiert, die dem Appell von STAR 21 den Weg geebnet hatten und nun in den Startlöchern standen, um die Vermarktung ihrer Produkte voranzutreiben. Bereits 2001 hatte sich der Rüstungskonzern Israel Aircraft Industries (IAI), u.a. Hersteller der Drohnen Heron und Hunter, im Rahmen des 5. Forschungsrahmenprogramms der Europäischen Kommission einen „UAV Civil Application Workshop" organisiert, um die „Aufmerksamkeit in Europa für Grundlage und Nutzen potenzieller ziviler Missionen von UAVs zu erhöhen" und weitere Förderaktivitäten der Kommission in diesem Bereich vorzubereiten.[12] Mit Erfolg: Fast fünf Millionen Euro steckte die Kommission zwischen 2001 und 2005 in die IAI-geführten Projekte UAV-NET und CAPECON. Beide Projekte zielten auf die Ausarbeitung von Visionen zur Nutzung von Drohnen im zivilen Bereich. Mit dabei u.a. EADS, Thales, BAE Systems sowie Luft- und Raumfahrtforschungszentren aus Frankreich, Deutschland, Schweden und den Niederlanden.[13] Daneben finanzierte die Kommission mit weiteren 2,5 Millionen Euro mit USICO ein Projekt, das sich explizit Fragen der Luftsicherheit des zivilen Einsatzes von Drohnen widmete. Auch hier wieder mit an Bord: IAI.[14] 2005/2006 schließlich legten diese Projekte unter der großspurigen Überschrift „25 Nationen für einen Durchbruch im Luftraum" gemeinsam eine detaillierte „Roadmap" für „European Civil Unmanned Air Vehicles" vor, redaktionell betreut vom israelischen Rüstungsmanager Mark Okrent.[15] Das Ziel: ein „pan-europäisches Programm" für den zivilen Einsatz von Drohnen. Zwar blieb die direkte Umsetzung der ambitionierten Pläne durch die Kommission ein Wunschtraum, doch die von den Projekten entwickelten Blaupausen für die Diffusion der Kriegsroboter ins Zivile wirken bis heute fort; und auch das UAV-NET blieb trotz Auslaufen der Finanzierung aus Brüssel als Forum für den Austausch und die Lobbyarbeit am Leben.[16]

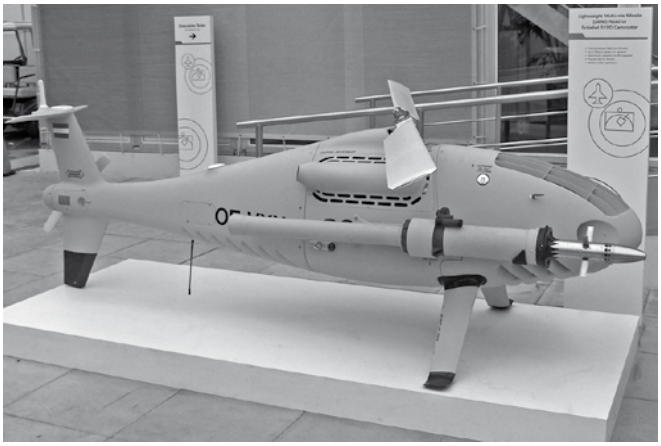
Entscheidende Verstärkung kam durch die Vereinigung EURO UVS, die 1995 – damals noch als informelles Netzwerk – von einem umtriebigen niederländischen Consultant als Interessenvertretung der europäischen Drohnenindustrie ins Leben gerufen worden war.[17] Inzwischen heißt der Verband UVS International und hat nach eigenen Angaben knapp 270 Mitglieder in 36 Ländern. Sein Vorstand wird dominiert von Großkonzernen wie EADS-Cassidian, Thales, Sagem, Boeing, Honeywell und der israelischen Firma Elbit Systems. Man versteht sich als globale Stimme der „UVS community". Zentrales Ziel ist auch hier die Zulassung von Drohnen für den zivilen Luftraum. Es sollen internationale Standards entwickelt, das Luftverkehrsrecht geändert, die Flugsicherung angepasst und Zertifizierungssysteme entwickelt werden. Neben den mehr als 150 Beitrag zahlenden Firmenmitgliedern gehören dem Verband 109 „Ehrenmitglieder" an, i.d.R. Vertreter von Militär, Verteidigungsministerien sowie nationalen und internationalen Luftfahrtbehörden.[18] Sinn und Zweck der Einbindung von „Ehrenmitgliedern", so schreibt Verbandspräsident Peter van Blyenburgh, ist die Schaffung eines internationalen Netzwerkes, das es erlaubt, sich „jenseits offizieller Kanäle" auszutauschen und „nützliche Beziehungen" zu knüpfen.[19] Zur Pflege des Netzwerkes informiert UVS International seine Mitglieder mit Industrieinformationen und dem Jahrbuch „Unmanned Aerial Systems"; es werden Workshops und Konferenzen organisiert, Fotowettbewerbe ausgeschrieben, und – kleine Schmeichelei unter Freunden – einmal im Jahr wird der „Catherine-Fargeon-Preis" an Leute vergeben, die sich um die Verbandsziele verdient gemacht haben.[20]



**Im Dschungel der Standardisierung**

Hatte der Verband 2001 noch vergeblich mit dem UAV-NET um Fördergelder der Kommission konkurriert, installierte er letztlich unabhängig von Brüssel sein UCARE-Programm. UCARE steht für „UAVs – Concerted Actions for Required Regulations" und zielt auf die Entwicklung globaler Regeln für den unbegrenzten Drohnenflug. Einen ersten Erfolg verzeichnete diese Strategie, als die Lobbyisten, damals noch als EURO UVS, im Jahr 2002 die Joint Aviation Authorities (JAA) [21] und EUROCONTROL[22] überreden konnten, eine gemeinsame „UAV Task Force" einzurichten, um ein erstes Konzept zur Integration von Drohnen in den zivilen Luftraum zu entwickeln. Schriftführer der Arbeitsgruppe wurde EURO-UVS-Präsident Blyenburgh. Mehr als die Hälfte des etwa 40-köpfigen Gremiums waren Vertreter der Industrie, allein fünf kamen von EADS.[23] Der 2004 vorgelegte Abschlussbericht[24] gilt als Referenzdokument, das bis heute die Arbeit von Gremien wie der europäischen Flugsicherheitsagentur EASA und der International Civil Aviation Organization (ICAO) inspiriert. Abgesteckt waren damit die zu klärenden Problemfelder: die Flugtauglichkeit von UAVs und ihre Zertifizierung, die Ausbildung und Lizensierung von Drohnenlenkern, der Schutz der Kommunikation von Bodenstation und Luftfahrzeug vor Störungen, die Organisation des Luftverkehrsmanagements inklusive der Frage, wie Kollisionen zu vermeiden sind („Sense and Avoid").

Zur Fortsetzung des Standardisierungsprozesses kündigte die EASA im Sommer 2005 ein ambitioniertes Programm an: In enger Abstimmung mit der US-amerikanischen Federal Aviation Authority (FAA) wollte man bis 2006 konkrete Vorschläge für die europäische Zertifizierung von Drohnen entwickeln. Ausgenommen: Drohnen von Militär, Zoll oder Polizei sowie sogenannte „Light UAVs" unter 150 Kilogramm; ihr Einsatz sollte national bzw. multilateral durch NATO-Gremien geregelt werden. Doch offensichtlich hatte die neu gegründete EASA die Aufgabe unterschätzt, die zahllosen Interessen der europäischen Luftfahrt unter einen Hut zu bringen.[25] Zudem verortete sie die Frage von „Sense and Avoid" im Bereich des Luftverkehrsmanagements und überließ sie damit ihrer Schwesterorganisation EUROCON-



*Der Camcopter der österreichischen Firma Schiebel (hier eine bewaffnete Version) wird von Europäischer Rüstungsagentur und Frontex getestet, um als „taktische Drohne" die EU-Außengrenzen zu überwachen*
*Quelle: http://de.wikipedia.org/w/index.php?title=Datei:S-100-OE-VXX.jpg&filetimestamp=20080716174800*

TROL.[26] Anfang 2006 warf die Agentur dann faktisch das Handtuch, als sie erklärte, dass die Aufgabe ihre Verantwortlichkeit übersteige und es einer explizit politischen Entscheidung bedürfe.[27] Ihr Vorschlag, gar eine eigene Regulierungsagentur für den Drohnenflug zu schaffen, rief neue Akteure auf den Plan. Bereits wenige Monate später übernahm die European Organization for Civil Aviation Equipment (EUROCAE) im Auftrag von EUROCONTROL die Koordinierung der schwierigen Standardisierungsverhandlungen.[28]

### Forschen für Europas Militärmacht

Doch insbesondere die neue Europäische Verteidigungsagentur (European Defence Agency – EDA), erst 2004 zur Steuerung der Rüstungspolitik in der Europäischen Union ins Leben gerufen, ergriff nun die Initiative. UAVs gelten als „Schlüsselelement" der militarisierten EU-Außen- und Sicherheitspolitik und gehören seit Gründung der EDA zu den Prioritäten ihrer Arbeit.[29] „Um die notwendige Informationsüberlegenheit zu erreichen, müssen europäische Truppen entsprechend ausdauernde und verlässliche ISR-Kapazitäten [Intelligence, Surveillance, Reconnaissance] unterhalten. Dies beinhaltet ein breites Spektrum an Sensoren und Systemen, inklusive Satelliten, bemannte Flugzeuge, das komplette Portfolio von UAVs und Landsysteme", heißt es in der „Long-term Vision" der Agentur von Oktober 2006.[30] Zum einen geht es um den Einsatz sogenannter taktischer Drohnen – gemeint sind unbemannte Kleinhubschrauber –, die gemeinsam mit der europäischen Grenzschutzagentur FRONTEX für Zwecke der „maritimen Überwachung", also für die Abschottung der europäischen Seegrenzen und Anti-Pirateerieeinsätze, aber auch für Infantrieeinsätze im Rahmen von EU-Militärmissionen entwickelt werden sollen.[31] Zum anderen geht es um die Unterstützung und Koordinierung nationaler Drohnenprogramme der EU-Mitgliedstaaten.

Williger Helfer und Stichwortgeber war von Anfang an der Lobbyverband UVS International. Bereits 2006 hatte er im Auftrag der Verteidigungsagentur eine Studie erstellt, um zukünftige Einsatzszenarien für Drohnen im Bereich Heimatschutz und Umweltmonitoring zu skizzieren.[32] Als Anfang 2007 der Auftrag für eine große EDA-Studie zur Integration von Drohnen in den Luftraum („Air4All") winkte, fusionierte der Verband seine Gruppe von Industrie-Consultants mit Vertretern anderer Firmen unter dem Dach der mächtigen AeroSpace and Defence Industries Association of Europe (ASD) in einer „UAS Working Group".[33] Im Rahmen des Air4All-Projektes machte sich die ASD-Drohnenarbeitsgruppe[34] nun gemeinsam mit EDA und unter Beteiligung der EU-Kommission daran, die Öffnung des europäischen Luftraums voranzutreiben. Im Juli 2008 legte man eine „Roadmap" vor: Bis 2015, so die Zielvorgabe, sollen die notwendigen Regularien und technischen Voraussetzungen geschaffen sein, um militärische und zivile Drohnen grenzüberschreitend an Europas Himmel fliegen zu lassen.[35] Auf diesen Startschuss folgte 2009/2010 der Auftakt von zwei großen technologischen Demonstrationsprojekten unter Schirmherrschaft der EDA: Für 50 Millionen Euro soll im Rahmen des MIDCAS-Projektes ein Konsortium von 13 Partnern aus fünf Staaten ein „Midair Collision Avoidance System" entwickeln und damit die Machbarkeit robuster „Sense-and-Avoid"-Technologie unter Beweis stellen. Das zweite Projekt soll demonstrieren, dass die Probleme des Steuerns und Lotsens von Drohnen außerhalb der Sichtweite mit Hilfe von Satellitennavigation zu lösen sind. Mit an Bord daher auch die Europäische Raumfahrtagentur (ESA) und ihr Galileo-Programm.[36] Zusätzlich organisiert die EDA das SIGAT-Projekt, um die militärischen Anforderungen an die Kommunikation mit UAVs zu klären und eine gemeinsame Position zu Frequenzen und Bandbreiten für die World Radio Conference 2012 zu formulieren.[37]

### Zivil-militärische Synergien

Parallel zu diesen Initiativen förderte die Europäische Kommission in ihren 6. und 7. Rahmenprogrammen Forschung zu Drohnen.[38] Neben experimentellen IT-Projekten zur Koordination von Drohnenschwärmen und dem Einsatz von Minidrohnen sowie wenigen Projekten zur Integration in den Luftraum[39] finanzierte Brüssel Drohnenforschung insbesondere im Bereich des mit 1,4 Milliarden Euro ausgestatteten Sicherheitsforschungsprogramms: Bei den Demonstrationsprojekten geht es im Wesentlichen um Grenzschutz und Migrationsabwehr, wie z. B. in den Projekten „Wide Maritime Area Airborne Surveillance" (WIMA2S) und „Open Architecture for UAV-based Surveillance System" (OPARUS) unter Führung der französischen Rüstungskonzerne Thales bzw. Sagem. Damit dient die finanzielle Förderung hier nicht nur Forschung und Entwicklung, sondern bereitet gleichzeitig den Boden für die Integration von Drohnen in das im Aufbau befindliche High-Tech-Grenzüberwachungssystem EUROSUR.[40]

So folgt die Generaldirektion Unternehmen und Industrie der Kommission, die für das Sicherheitsforschungsprogramm verantwortlich ist, den Empfehlungen einer Studie, die sie selbst 2007 bei Frost & Sullivan in Auftrag gegeben hatte. Um den europäischen Drohnenmarkt zu entwickeln, hatten die Marktforscher geraten, gezielt Fördergelder für Rüstung- und Sicherheitsinitiativen nutzbar zu machen und entsprechende Initiativen der EDA, aber auch von FRONTEX zu unterstützen.[41]

Doch die zivil-militärischen „Synergien“ gehen noch weiter: Anfang Juli 2010 organisierte die Kommission gemeinsam mit der Europäischen Verteidigungsagentur eine „High Level Conference on Unmanned Aircraft Systems“ mit 450 Teilnehmern. Präsentiert wurden u.a. Pläne, im Rahmen der 2010 gestarteten „European Framework Cooperation“ die Forschungspolitik von Kommission, EDA und ESA stärker zu verzahnen.[42] Angekündigt wurde die Gründung einer „High Level Group“ zur Beratung der Forschungs- und Entwicklungsaktivitäten. Diese kleine Expertengruppe, so hieß es in der Abschlusserklärung der Konferenz „wird Vertreter des Militärs integrieren, um die duale Natur von UAS-Operationen von Beginn an zu adressieren“.[43] Zwar kam die Gründung dieser Gruppe nicht zustande. Aber im Juni 2011 kündigte die Kommission auf der Internationalen Luftfahrtausstellung in Paris in kleiner Runde den Start einer „UAS Panel“-Initiative an: Eine Serie von Workshops soll bis zum Frühjahr 2012 die Kommission mit den nötigen Hintergrundinformationen versorgen, um anschließend eine Zukunftsstrategie für die europäische Drohnenpolitik zu entwickeln. Das Abschlusstreffen wird die Europäische Verteidigungsagentur ausrichten.[44]

Auch wenn es unwahrscheinlich ist, dass im Gefolge des „UAS Panels“ der große Wurf gelingt, so steht fest, dass die Allianz der europäischen Rüstungs- und Industriepolitik unter dem Druck der Lobbyisten alles daran setzen wird, der Normalisierung der fliegenden Roboter den nötigen Luftraum zu schaffen. Dass ein solcher Transfer von Kriegsmaschinen und der mit ihnen verbundenen panoptischen Fantasien ins Zivile neben den Sicherheitsproblemen auch erhebliche Gefahren für Bürgerrechte und Demokratie birgt, liegt nahe. Entsprechend ernst nehmen ihre Befürworter auch die Aufgabe, Akzeptanz zu schaffen und Drohnen als „Retter aus dem Himmel“ gesellschaftsfähig zu machen. Doch auch wenn die eine oder andere Anwendung durchaus sinnvoll erscheinen mag, sollten wir nie vergessen, dass das ursprüngliche Motiv hinter den Versuchen, Drohnen alltagstauglich zu machen, im Wesentlichen darin besteht, die Bezahlbarkeit militärischer Überlegenheit und kriegerischer Interventionen zu sichern.

## Anmerkungen

1 *Die Zahlen des Pentagon beziehen sich nur auf den militärischen Einsatz von Mittel- und Langstreckendrohnen wie Predators oder Global Hawks. Flugzeiten von Kleinsystemen sind dabei ebenso wenig erfasst wie die Predator-Flüge für die US-amerikanische Heimatschutzbehörde Customs and Border Protection an der Grenze zu Mexiko. The dead, the dollars, the drones: 9/11 era by the numbers. http://www.wired.com/dangerroom/2011/09/dangerroom_911toll_0909, Zugriff: 12.10.2011.*

2 *Bei der großen Mehrheit handelt es sich um kleine Drohnen zur Nächst- und Nahaufklärung insbesondere städtischer Schlachtfelder, darunter sind aber auch etwa 800 größere Maschinen für Fernaufklärung und Kampfeinsätze. Vgl. Congress of the United States: Policy Options for Unmanned Aircraft Systems. Congressional Budget Office Study. Washington D.C. June 2011.*

3 *Vgl. Thomas Petermann und Reinhard Gründwald: Stand und Perspektiven der militärischen Nutzung unbemannter Systeme. TAB-Arbeitsbericht Nr. 144. Mai 2011, S. 43.*

4 *Bundesministerium der Verteidigung: Weißbuch 2006 zur Sicherheitspolitik Deutschlands und der Zukunft der Bundeswehr. Berlin. Oktober 2006, S. 120.*

5 *Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage 16/12193 zur Einführung und Bedeutung unbemannter militärischer Fahrzeuge und Luftfahrzeuge. Drucksache 16/12481. 26.3.2009, S. 2-3.*

6 *Als Sprachrohr der Rüstungsindustrie fungierte hier der Ausschuss Verteidigungswirtschaft des Bundesverbandes der Deutschen Industrie. Vgl. Petermann & Grünwald, a.a.O., S. 172.*

7 *Petermann & Grünwald, a.a.O., S. 34-42.*

8 *ebda., S. 173.*

9 *Namentlich die Firmen BAE Systems, EADS, Finmeccanica, Rolls Royce, SNECMA (heute Safran) und Thales.*

10 *s. hierzu Michael Ignatieff: Virtual war. Kosovo and beyond. London 2000.*

11 *European Commission: Strategic Aerospace Review for the 21st century. Creating a coherent market and policy framework for a vital European industry. Brüssel. Juli 2002, S. 30.http://ec.europa.eu/enterprise/sectors/aerospace/files/report_star21_screen_en.pdf, Zugriff: 14.10.2011.*

12 *http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5060032, Zugriff: 15.10.2011.*

13 *http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5430411 und http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5674228, Zugriff: 15.10.2011.*

14 *http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5622413, Zugriff: 15.10.2011.*

15 *http://elib.dlr.de/44544/1/UAV_Roadmap_Overview33.pdf, Zugriff: 15.10.2011, S. 2.*

16 *http://www.uavnet.org*

17 *Das UVS steht hier für „unmanned vehicle systems“. Damit macht der Verband auch Lobbyarbeit für unbemannte Boden- und Wassersysteme. Im Zentrum der Arbeit stehen aber (noch) Drohnen.*

18 *So waren im Jahr 2008 bspw. die deutschen Ehrenmitglieder ein Vertreter der Rüstungsabteilung des Verteidigungsministeriums, zwei*

**Eric Töpfer**

**Eric Töpfer** ist Politikwissenschaftler. Er arbeitet als freier Mitarbeiter für die britische Bürgerrechtsorganisation Statewatch und ist Redakteur der Zeitschrift „Bürgerrechte & Polizei/CILIP“. Kontakt: *toepfer@emato.de*

*Luftwaffenoffiziere, zwei Vertreter des Heeresamtes, zwei Leute der Wehrtechnischen Dienststelle für Luftfahrzeuge des Bundesamtes für Wehrtechnik und Beschaffung und ein Vertreter der Deutschen Flugsicherung. Vgl. http://uasresearch.com/UserFiles/File/078-086_Contributing-Stakeholder_UVS-International.pdf, S. 79. Zugriff: 13.10.2011.*

19 *ebda., S. 78.*

20 *Benannt ist der Preis nach der ersten Preisträgerin, einer hohen Beamtin des Rates für Rüstung beim französischen Verteidigungsministerium. Weitere Preisträger sind u.a. Vertreter verschiedener Generaldirektionen der Europäischen Kommission, der europäischen Grenzschutzagentur FRONTEX, der Europäischen Verteidigungsagentur und diverser nationaler und internationaler Luftfahrtbehörden.*

21 *Die JAA war ein Zusammenschluss der zivilen Luftfahrtbehörden von 34 europäischen Ländern, der europäisch harmonisierte Luftsicherheitsstandards entwickelte. Als die JAA 2009 aufgelöst wurde, übernahm die Europäische Agentur für Flugsicherheit (EASA) die meisten ihrer Aufgaben.*

22 *Die 1960 gegründete European Organisation for the Safety of Air Navigation (EUROCONTROL) ist die zentrale Koordinationsstelle für die Luftverkehrskontrolle in Europa mit Sitz in Brüssel. Ihr Ziel ist die Entwicklung eines nahtlosen europäischen Flugverkehrsmanagement-Systems.*

23 *JAA/EUROCONTROL: Enclosures to UAV Task-Force Final Report. 2004. http://www.barnardmicrosystems.com/download/JAA_EUROCONTROL_UAV_Final_Report_Enclosures.pdf, S.15ff. Zugriff: 5.11.2011.*

24 *JAA/EUROCONTROL: UAV Task-Force Final Report. A concept for European regulations for civil unmanned aerial vehicles. 11. Mai 2004. http://www.easa.eu.int/rulemaking/docs/npa/2005/NPA_16_2005_Appendix.pdf. Zugriff: 5.11.2011.*

25 *Die Kommentare der ersten Konsultationsrunde, der „Advance Notice of Prior Amendment", umfassten 270 kleingedruckte Seiten. http://www.easa.eu.int/rulemaking/docs/crd/2005/CRD-16-2005.pdf. Zugriff: 5.11.2011.*

26 *„Atlantic harmony", in: flightglobal.com, 6. September 2005. http://www.flightglobal.com/news/articles/atlantic-harmony-201329/. Zugriff: 5.11.2011.*

27 *„EASA calls for UAV airspace rules co-ordinating body", in: flightglobal.com, 18. Januar 2006. http://www.flightglobal.com/news/articles/easa-calls-for-uav-airspace-rules-co-ordinating-body-204059/. Zugriff: 5.11.2011.*

28 *EUROCAE ist eine seit 1963 existierende Non-Profit-Organisation, in der sich Industrie, Luftfahrtbehörden, Flugsicherungen, Fluggesellschaften und Flughafenbetreiber zusammengetan haben, um technische Standards für Luftverkehrselektronik zu entwickeln. Seit April 2006 existiert die Working Group 73, die mit vier Unterarbeitsgruppen an Standards für den Drohnenflug arbeitet. S. http://www.eurocae.net/working-groups/wg-list/42-wg-73.html und http://uasresearch.com/UserFiles/File/033_Contributing-Stakeholder_EUROCAE.pdf. Zugriff: 5.11.2011.*

29 *http://www.eda.europa.eu/Libraries/Documents/Brochure_UAS_on_EDA_activities.sflb.ashx, S.1; http://www.eda.europa.eu/Otheractivities/UAStrafficinsertion. Zugriff: 7.11.2011.*

30 *European Defence Agency: An initial long-term vision for European defence capabilities and capacity needs. 3. Oktober 2006, S. 28.*

31 *http://www.eda.europa.eu/Otheractivities/Maritimesurveillance/Futureuas. Zugriff: 7.11.2011.*

32 *http://www.uas2011-latin-america.org/9_UVS-International_Background&Activities_June2011.pdf, S. 70f. Zugriff: 7.11.2011.*

33 *http://www.uas2011-latin-america.org/9_UVS-International_Background&Activities_June2011.pdf, S. 69. Zugriff: 7.11.2011.*

34 *„Stakeholder" waren Alenia Aeronautica, BAE Systems, Dassault Aviation, Diehl BGT Defence, EADS CASA, EADS Defence & Security Germany, Selex Galileo, QinetiQ, Rheinmetall Defence Electronics, SAAB AB, Sagem Defence Systems and THALES.*

35 *S. http://www.air4all.net/ sowie http://www.eda.europa.eu/Otheractivities/UAStrafficinsertion. Zugriff: 7.11.2011.*

36 *European Defence Agency: Annual Report 2009, S. 20f.*

37 *http://www.eda.europa.eu/Libraries/Documents/SIGAT_Leaflet.sflb.ashx. Zugriff: 7.11.2011.*

38 *Ein guter Überblick der EU-Drohnenprogramme findet sich bei Volker Eick: Das Dröhnen der Drohnen, in: Bürgerrechte & Polizei/CILIP 94 (3/2009), S. 28-40 (38).*

39 *Hervorzuheben ist hier das Vier-Millionen-Euro-Projekt „Innovative Operational UAV Integration" (INOUI) unter Führung der Deutschen Flugsicherung und mit Beteiligung von Rheinmetall Defence.*

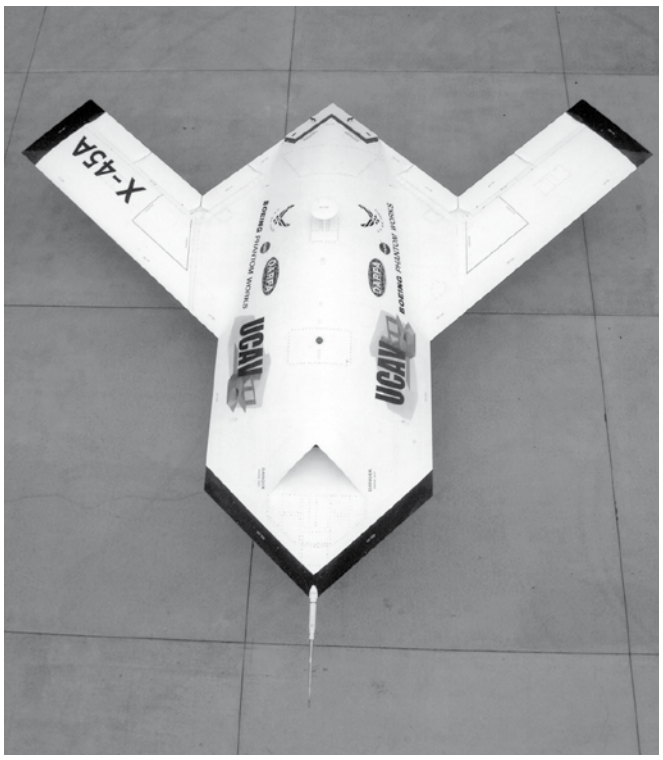
40 *s. hierzu ausführlicher Ben Hayes: The Neoconopticon. The EU Security-Industrial Complex. TNI/Statewatch: Amsterdam 2009. http://www.statewatch.org/analyses/neoconopticon-report-summary.pdf. Zugriff: 8.11.2011.*

41 *Frost & Sullivan: Study analysing the current activities in the field of UAV. Second element: Way forward. European Commission: Enterprise and Industry Directorate-General (ENTR/2007/065). http://ec.europa.eu/enterprise/policies/security/files/uav_study_element_2_en.pdf. Zugriff: 8.11.2011.*

42 *http://www.eda.europa.eu/News/10-07-01/EDA-EC_Conference_on_Unmanned_Aircraft_Systems_UAS_recommends_a_High_Level_Group; s. zur Framework Cooperation http://www.eda.europa.eu/Aboutus/Howwedo/Civmil/EFC. Zugriff: 8.11.2011.*

43 *Conclusions of the first European High Level Conference on Unmanned Aircraft Systems. Brüssel, 1. Juli 2010. http://ec.europa.eu/transport/air/doc/2010_07_01_conclusions_uas_conference_v__finale.pdf. Zugriff: 8.11.2011.*

44 *http://ec.europa.eu/enterprise/sectors/aerospace/uas/index_en.htm. Zugriff: 8.11.2011.*




*Erstes Stealth-UCAV der Welt: Boeing X-45*
*PD, copyright notice: http://www.darpa.mil/body/privacy.html*

**Otto Reger**

# Das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) in Karlsruhe und Ettlingen

## Wie eine renommierte Forschungsinstitution zum effizienteren Töten beiträgt



*Dass Karlsruhe einen mehr oder weniger erfolgreichen Fußballverein hat, wissen viele, und dass Karlsruhe zuweilen die Residenz des Rechts genannt wird, ist auch etlichen bekannt. Dass die badische BeamtInnenstadt außerdem über eine Universität mit Exzellenzimage verfügt, ist schon weniger bekannt. Nur einer verschwindenden Zahl von Wissbegierigen dürfte bewusst sein, dass in der „Fächerstadt" (und im benachbarten Ettlingen) das „größte europäische Forschungsinstitut im Bereich der Bildgewinnung, Bildverarbeitung und Bildauswertung"[1] angesiedelt ist und dort auch militärische Forschung und Entwicklung betrieben wird. Bei der nicht nur quantitativ bedeutenden Einrichtung handelt es sich um das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung, kurz IOSB.*

Die in der Fraunhofer-Gesellschaft (gegründet 1949) zusammengeschlossenen Fraunhofer-Institute verdanken ihren Namen dem gleichnamigen Münchner Forscher, Erfinder und Unternehmer, der von 1787 bis 1826 lebte. Sein Name steht heute für eine Wissenschafts-Institution von eindrucksvoller Größe: „Die Fraunhofer-Gesellschaft betreibt in Deutschland derzeit mehr als 80 Forschungseinrichtungen, davon 59 Institute. 17.000 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, bearbeiten das jährliche Forschungsvolumen von 1,6 Milliarden Euro. Davon fallen 1,3 Milliarden Euro auf den Leistungsbereich Vertragsforschung."[2] Ein Vergleich mit der Beschäftigtenzahl von Vodafone mit 13.000 Arbeitsplätzen und Telefonica O2 Germany mit 5.000 Stellen verdeutlicht, welche Rolle die Fraunhofer-Institute im Wissenschaftsbetrieb spielen. Etwa zwei Drittel ihrer Vertragsforschung erwirtschaftet die Fraunhofer-Gesellschaft (FhG) mit Industrieaufträgen (darunter Rüstungsunternehmen) und öffentlichen Auftraggebern, wie dem Bundesministerium für Bildung und Forschung (BMBF) und dem Verteidigungsministerium (BMVg).

Das IOSB ist in der FhG ein bedeutender Player, weil es darin das größte Institut für Information und Kommunikation darstellt. Diese Stellung verdankt die Einrichtung ihrer geballten personellen und finanziellen Ausstattung. Unter der Leitung von **Professor Jürgen Beyerer** (in Karlsruhe) und **Professor Maurus Tacke** (in Ettlingen) sind insgesamt 500 Mitarbeiterinnen und Mitarbeiter beschäftigt (darunter 100 Studierende).

> *„Für 2010 sind ein Institutsvolumen von knapp 42 Mio. Euro kalkuliert, wobei rund 14 Mio. (= 1/3) als Basisfinanzierung fungieren und 28 Mio. durch Akquisitionen gedeckt werden. 10 Prozent unseres Aufwands wird in Investitionen fließen."*[3]

### Was hat das IOSB mit Kriegsführung zu tun?

Das IOSB beschäftigt sich mit einer ganzen Reihe von nichtmilitärischen Themen, wie etwa dem Aufspüren von Giftstoffen in Trinkwassernetzen oder der Unfallverhütung, widmet sich aber auch intensiv der militärischen Forschung und Entwicklung.

Die Begriffe „Krieg" oder „Kriegsführung" kommen in den nüchtern und scheinbar wertfrei formulierten Texten des IOSB nicht vor, ebenso wenig wie die Worte „Tod" oder „Zerstörung". Welche Sprache verwendet wird, sollen zwei Beispiele verdeutlichen, die in der BMVg-Publikation „Wehrwissenschaftliche Forschung. Jahresbericht 2009. Verteidigungsforschung für die Erfordernisse der Bundeswehr im Einsatz"[4] erschienen sind. IOSB-Beschäftigte beschreiben darin die Tätigkeit ihres Instituts.

In dem von Susanne Angele und Alexander Bauer verfassten Artikel „RecceMan® – Interaktive Erkennungsunterstützung für die abbildende Aufklärung" schreiben sie:

> *„Zweck der abbildenden Aufklärung ist es, militärisch relevante Informationen über ein Interessengebiet durch Aufnahme und Auswertung von Luft- und Satellitenbildern zu gewinnen. Sie stellt damit ein geeignetes Mittel dar, um den Schutz der deutschen Streitkräfte im Einsatzland zu erhöhen und ihre Wirkgenauigkeit zu verbessern."*[5]

IOSB-Mitarbeiter Peter Solbrig vom Standort Ettlingen beschreibt die Bedeutung der intensiven IOSB-Forschung auf dem Gebiet der **Sensorik für Aufklärung und Überwachung**. Unter „zunehmend widrigen Bedingungen" bedürften nach Solbrig die deutschen Truppen „mehr denn je modernster Mittel und Methoden, um ihre quantitative Unterlegenheit in ihren ausgedehnten Verantwortungsbereichen durch Überlegenheit im Informationsraum als dem entscheidenden Operationsfeld aufwiegen zu können"[6]. Vernetzte Operationsführung vor allem mittels Nachrichtengewinnung und Aufklärung weise „den Weg zur optimalen Ausnutzung der technischen Überlegenheit auf den Gefechtsfeldern der Gegenwart und Zukunft."[7]

Was an den beiden IOSB-Standorten in Karlsruhe und Ettlingen für die Bundeswehr und die Rüstungsindustrie geforscht und entwickelt wird, beschreiben der 126-seitige **IOSB-Jahresbericht 2009/10** und der 104-seitige **IITB-Jahresbericht 2008** reichlich bebildert und mit in die Kamera lächelnden Wissenschaftlerinnen und Wissenschaftlern sowie den jeweiligen Kontaktpersonen detailliert. Mit deutlichem Selbstbewusstsein fasst das IOSB die Highlights seiner langjährigen Arbeit für militärische Zwecke so zusammen:

> *„Überzeugende Beispiele für Systeme aus dem Hause IOSB sind das Bildauswertesystem ABUL® für das unbemannte Aufklärungsflugzeug LUNA, das mittlerweile*



*bei der Bundeswehr mehrfach eingesetzt wird, das System RecceMan®, das eine effiziente interaktive Objekterkennung in der Luftbildauswertung erlaubt und als geschätztes Werkzeug ebenfalls bei der Bundeswehr eingeführt ist.*"[8]

Weil die Bundesregierung und die Bundeswehr bestrebt sind, weltweit immer mehr überwachen, kontrollieren und bekämpfen zu können, greift sie gern auf die Kompetenz der IngenieurInnen, InformatikerInnen und der anderen IOSB-WissenschaftlerInnen zurück. Das gilt genauso für viele Unternehmen, die das Knowhow für ihre Entwicklungen zu schätzen wissen.

### Sensoren und Kameras im Dienste der militärischen Aufklärung

Eine große Rolle für militärische Aufklärung spielen Sensoren. **Sensoren** sind diejenigen Bauteile in einer (**Video-)Kamera** oder in einer **Infrarotkamera**, die bewirken, dass Licht oder elektromagnetische Wellen oder die Wärmeabstrahlung, die von einem Objekt ausgehen, in Bilder umgewandelt wird. Sensoren sind in Kameras eingebaut, die wiederum in Satelliten oder in Drohnen verwendet werden. Ein Satellit, den die Bundeswehr zur Aufklärung aus dem Weltraum einsetzt, ist der **SAR-Lupe-Satellit**. SAR steht für Synthetisches Apertur Radar und damit für ein Radar, welches die elektromagnetischen Wellen nutzt und dadurch auch bei Nacht und schlechter Sicht (Nebel, Dunst) verwertbare Bilder liefert. So wie einem Patienten die Ultraschallbilder oder Röntgenbilder wenig sagen, weil sie anders als die Fachärzte nicht entsprechend ausgebildet sind, benötigt das Verstehen und Interpretieren der militärischen Radarbilder besonderes Wissen. Daher bildet das Militär eine steigende Zahl von so genannten **Bildauswertern** aus.

Die Sensoren bzw. Kameras werden durch unbemannte Flugkörper wie etwa **Drohnen** dort hingebracht, wo feindliche Stellungen oder die Schlupfwinkel der „weltweit operierenden Terroristen" vermutet werden. Das IOSB hat eine dafür geeignete mit vier Rotoren ausgestattete spezielle Drohne, den **Quadrocopter** entwickelt.

Sensoren werden aber auch ortsfest (beispielsweise in Überwachungskameras) oder in Land- oder (Unter-)Wasserfahrzeugen eingesetzt. Alle diese hochleistungsfähigen Geräte liefern eine Flut von Daten, die ohne ausgeklügelte Hardware und Software zur Signalübertragung und Signalauswertung nicht zu bewältigen ist. Um etwa Personen oder Fahrzeuge im Überwachungsgelände leichter lokalisieren und identifizieren zu können, hat das IOSB das **AMFIS-System** entwickelt.

Zwei weitere IOSB-Entwicklungen beschreibt die Mathematikerin Susanne Eckel in ihrem 2007 erschienen Artikel „Aufklärungsbedarfskarten am ‚Digitalen Lagetisch'". Schon im ersten Satz ruft sie in Erinnerung: „Am 15. April 2007 starteten ‚Recce-Tornados' der Bundesluftwaffe ... zu ihrem ersten Bildaufklärungsflug über Afghanistan."[9] „Recce" (sprich Rekki) ist eine englische Kurzbezeichnung für Reconaissance oder Aufklärung. Eckel beschreibt, wie Fortschritte in der **Sensor- und Datenübertragungstechnologie** und mehr internationale Zusammenarbeit das „Aufklärungspotenzial" anwachsen ließen. Ziel ist es, die „vielen und unterschiedlichen Ressourcen – von der Videokamera bis zum Radarbildsensor, von der unbemannten Kleindrohne bis zum Recce-Tornado oder sogar zum Aufklärungssatelliten – optimal aufeinander abzustimmen."[10]

Wofür die Militärs einst Sandkasten und Zinnsoldaten einsetzten, können sie heute ausgeklügelte Computer-Programme und ergonomisch optimierte Anzeigegeräte nutzen. Das IOSB hat eine spezielle Form von Karten entwickelt, so genannte „**Aufklärungsbedarfskarten**", die den SoldatInnen in der militärischen Leitstelle in kürzester Zeit leicht interpretierbare Ansichten liefern. Darstellen lassen sich die Karten am „**Digitalen Lagetisch**", einer auch wahrnehmungspsychologisch ausgetüftelten Hardware.

In der IOB-Abteilung „ZIE" („**Zielerkennung**") in Ettlingen befasst sich die Projektgruppe „Zielerkennung mit Laserradar" („ZiLa") mit den Einsatzmöglichkeiten von **Laserradar** für autonome Systeme im militärischen und zivilen Anwendungsbereich. Einer von mehreren Einsatzschwerpunkten ist dabei „die automatische Zieleinweisung, Mehrfachzielverfolgung und Zielannäherung für **Lenkflugkörper**"[11]. Der Auftraggeber ist die Wehrtechnische Dienststelle für Pionier- und Truppengerät (WTD 51) der Bundeswehr in Koblenz.

Eine andere ZIE-Arbeitsgruppe nennt sich „**Bildfolgenbasierte Situationserkennung**". Sie widmet sich der schnellen, d. h. automatischen und „robusten" Anwendung von Überwachungskameras. Die entwickelten IOSB-Systeme sind typische **Dual-Use-Produkte**, weil sie sich sowohl in Patrouillenfahrzeuge der Bundeswehr wie auch z. B. in Bahnhofshallen einsetzen lassen. „Für die videogestützte Erkennung von Bedrohungen jeder Art sollen Objekte nicht nur detektiert werden, sondern das Verhalten sichtbarer Personen und Fahrzeuge im Umfeldkontext soll ein ganzes Bild erzeugen und auf potentielle Gefahren hinweisen."[12] Das IOSB kann für seine Arbeit auf Gelder des Verteidigungsministeriums zurückgreifen.

### Common-Shield-Übung mit IOSB-Komponenten beeindruckt NATO-Generäle

Im August und September 2008 führte die Bundeswehr in Eckernförde die Übung „Common Shield" (etwa gemeinsames Schutzschild) durch. Deren Ziel war es, das „taktische Führen unter Bedingungen vernetzter Operationsführung (NetOpFü)"[13] und die vom Fraunhofer-Institut für Informations- und Datenverarbeitung IITB entwickelten Systeme und Geräte zu testen (das IITB wurde mit dem Fraunhofer-Institut für Optronik und Mustererkennung, FOM in Ettlingen zum 17.3.2010 zum IOSB fusioniert). Die Übung und eine abschließende Demonstration der Abwehr eines nachgestellten Terrorangriffs vor NATO-Generälen beim „VIP-Day" fielen sehr zur Zufriedenheit der Fraunhofer-Forscher aus, denn das Institut hat sich „hervorragend präsentieren und platzieren können." Auch die Bundeswehr geizte nicht mit Lob und schickte gleich zwei Dankesschreiben. Die einbezogenen BundeswehrsoldatInnen kamen, wie es heißt, mit allen Komponenten schnell und sicher zurecht und äußerten sich ebenfalls sehr positiv.

**Welchen Interessen und Zwecken dient das IOSB?**

Welchen Zielen und Zwecken man sich verpflichtet fühlt, beschreibt das IOSB so: „Als Fraunhofer-Institut hat das IOSB den klaren Auftrag, seine Forschung anwendungsbezogen und damit am Bedarf von Unternehmen und öffentlichen Auftraggebern zu orientieren."[14] Zu den öffentlichen Auftraggebern gehören das Bildungs- und Forschungsministerium und vor allem das Verteidigungsministerium. Anders als an Universitäten und Hochschulen geht es dem IOSB nicht um die Lehre, sondern um die „Umsetzung neuester Forschungsergebnisse in anwendungsreife Problemlösungen. Solche, die für unsere Kunden unmittelbar geldwerte Vorteile bedeuten und die deren Wettbewerbsfähigkeit nachhaltig stärken."[15] Die starke Orientierung auf die Interessen der Wirtschaft spiegelt sich auch darin wieder, dass 20 Prozent der Finanzierung des IOSB durch Unternehmen erbracht werden und in einer hohen Wiederbeauftragungsrate, d. h. die Unternehmen vergeben häufig Folgeaufträge.

Die starke Ausrichtung der Forschungsaktivitäten auf Wirtschaftsinteressen im Allgemeinen und die von Rüstungsunternehmen im Besonderen spiegelt sich in der Zusammensetzung des **Kuratoriums** des IOSB wieder. Dem Kuratorium gehören an: Rainer Kroth von der **Diehl BGT Defence GmbH & Co. KG** in Überlingen, Sven Olaf von der **EADS Deutschland GmbH** in Friedrichshafen und Bernd-Ulrich Wanner von der **Daimler AG** in Sindelfingen. Daneben ist auch das Verteidigungsministerium mit mehreren Personen vertreten.

Der Auftraggeber von „SD VIntEL – Simulationsbasierte Erprobungslandschaft für die Bundeswehr" ist das Bundesamt für Wehrtechnik und Beschaffung (BWB). Das Fraunhofer IOSB hat zusammen mit dem Institut für Technik Intelligenter Systeme e. V. (ITIS) die Rolle der wissenschaftlichen Begleitung und darüber hinaus die Aufgabe der Entwicklung von Anteilen des Systemdemonstrators. Die industriellen Partner **EADS, IABG, RDE** und **THALES** sind für die Entwicklung weiterer Anteile des Demonstrators zuständig.[16]

**Mit wem ist das IOSB vernetzt?**

Das IOSB ist ein schlagkräftiges Instrument des militärischen Flügels der Fraunhofer-Institute, die im **Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung VVS** zusammengeschlossen sind. Die Aufgabe des VVS wird wie folgt beschrieben: „In diesem Verbund haben sich Fraunhofer-Institute zusammengeschlossen, um ihre Forschungsaktivitäten im Bereich ‚Defense and Security' zu koordinieren und umzusetzen. Der Schwerpunkt liegt dabei auf der Abstimmung institutsübergreifender Strategien mit den staatlichen Zuwendungsgebern und der Förderung der Zusammenarbeit mit diesen Einrichtungen und der wehrtechnischen Industrie."[17]

Neben dieser Vernetzung mit Rüstungsindustrie und Bundeswehr bzw. Verteidigungsministerium gibt es aber auch intensive Kontakte in den Universitäts- und Hochschulbereich. Eine wichtige Schaltstelle ist dabei der **Lehrstuhl für Interaktive Echtzeitsysteme** am **Karlsruher Institut für Technologie KIT** von Prof. Jürgen Beyerer, dem Leiter des Karlsruher IOSB. Dieser Lehrstuhl hilft dem IOSB, seine anwendungsgerichtete Forschung grundlagenorientiert zu ergänzen und dient dem Austausch. „Über die Professur für Interaktive Echtzeitsysteme am Institut für Anthropomatik der Fakultät für Informatik, über die Mitwirkung in zwei Sonderforschungsbereichen (SFB) der Deutschen Forschungsgemeinschaft (DFG), über Beratungsaktivitäten von Universitätsprofessoren am IOSB, über die Mitgliedschaft von Professoren im Kuratorium, über Vorlesungstätigkeiten durch IOSB-Personal und vieles andere mehr hat die Kooperation mit dem KIT eine Fülle vitaler Facetten."[18]

Um ihre militärisch relevanten Entwicklungen bekannt zu machen, Aufträge anzubahnen oder persönliche Kontakte zu knüpfen, sind IOSB-Vertreter Mitglieder einschlägiger Organisationen wie der **Deutschen Gesellschaft für Wehrtechnik (DWT)** oder der **Carl-Cranz-Gesellschaft e.V. (CCG)**. Die CCG mit Sitz in Weßling-Oberpfaffenhofen widmet sich der technisch-wissenschaftlichen Weiterbildung insbesondere in der Rüstungstechnik. Durch Lehrtätigkeit oder Vorträge von IOSB-MitarbeiterInnen wird der Wissenstransfer genauso gepflegt wie auch durch die Teilnahme an Tagungen, Kongressen und Symposien oder die Mitarbeit in Arbeitskreisen.

Eine gern genutzte Möglichkeit der Information, Präsentation und Kommunikation sind Messen und Fachausstellungen. Am 6. und 7. Mai 2009 stellte das IOSB seine militärischen Entwicklungen beispielsweise bei der 23. AFCEA Fachausstellung in Bonn-Bad Godesberg aus. **AFCEA** steht für Armed Forces Communications and Electronics Association und damit für eine in Fairfax, Virginia, USA ansässige Organisation. Auf der Internetseite des Vereins „**AFCEA Bonn e.V.**" beschreibt sich die Organisation als „Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung" *(www.afcea.de/)*.

Intensivster Vernetzungsakteur ist zweifellos Prof. Jürgen Beyerer, der auch stellvertretender Sprecher des Fraunhofer-Verbundes für Verteidigungs- und Sicherheitsforschung ist. Im Jahresbericht sind weitere 22 weiteren Gremien aufgelistet, in denen

**Otto Reger**

**Otto Reger,** nach Wirtschaftsstudium erwerbstätig als (Online-)Redakteur, veranlasst durch die Kriegsdienstverweigerung engagiert in der Deutschen Friedensgesellschaft – Vereinigte KriegsdienstgegnerInnen (DFG-VK) und dann auch im Friedensplenum Mannheim sowie aktuell als Online-Redakteur für die Kampagne „Aktion Aufschrei – Stoppt den Waffenhandel!"

er mitarbeitet. Für gute Beziehungen zur Sicherheitsfront sorgen durch ihre Mitgliedschaft in der Deutschen Gesellschaft für Wehrtechnik auch Jürgen Geisler, der Leiter der IOSB-Abteilung Interaktive Analyse und Diagnose (IAD) sowie Rainer Schönbein, Leiter der Abteilung Interoperabilität und Assistenzsysteme (IAB). Schönbein ist auch als Referent tätig u. a. bei einem Seminar der Carl-Cranz-Gesellschaft über Luft- und raumgestützte Bildaufklärung im Systemverbund (Karlsruhe, 15-18. Juni 2009) oder beim Kurzlehrgang „Aufklärungsverbund" an der **Bundesakademie für Wehrverwaltung und Wehrtechnik**. (19-23. Oktober 2009). Die in Mannheim sitzende Bundesakademie ist ebenfalls dafür bekannt, dass sie Verteidigungsbürokratie, Streitkräfte, Rüstungsunternehmen und Forschung vernetzt und an der Beschaffung und Indienststellung von Waffensystemen bei der Bundeswehr beteiligt ist.

## Anmerkungen

1 *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB), Jahresbericht 2009/2010 (eigentlicher Titel: Jahresbericht 2009/2010 Fraunhofer-Institut für Informations- und Datenverarbeitung. IITB Fraunhofer-Institut für Optronik und Mustererkennung FOM); Karlsruhe 2010 (IOSB 09/10), S. 6; Bericht online unter: http://www.iosb.fraunhofer.de/servlet/is/6121/Jahresbericht_2010.pdf*
2 *Ebenda, S.17*
3 *Ebenda, S. 16*
4 *Bundesministerium der Verteidigung Unterabteilung Rü IV (Herausgeber); Wehrwissenschaftliche Forschung. Jahresbericht 2009. Verteidigungsforschung für die Erfordernisse der Bundeswehr im Einsatz; Stand: März 2010; Bonn 2010 (Wehrforschung 2009); Bericht online unter: www.bmvg.de*
5 *Ebenda S. 28*
6 *Ebenda S. 22*
7 *Ebenda S. 22*
8 *IOSB 2009/2010, S. 8*
9 *visIT [Sicherheit] 1/2007, Herausgeber Prof. Dr.-Ing. Jürgen Beyerer, Fraunhofer-Institut Informations- und Datenverarbeitung IITB, 8. Jahrgang, ISSN 1616-8240, Karlsruhe 2007 (visIT), S. 14 f.*
10 *Ebenda S. 14*
11 *IOSB 2009/2010, S. 98*
12 *Ebenda S. 100*
13 *Fraunhofer-Institut für Informations- und Datenverarbeitung IITB, Jahresbericht 2008; Karlsruhe 2009 (IITB 2008)*
14 *IOSB 2009/2010, S. 8*
15 *Ebenda S. 6*
16 *Ebenda S. 74*
17 *http://www.iosb.fraunhofer.de/servlet/is/8173/*
18 *IOSB 2009/2010, S. 9*

**Ingo Ruhmann**

# Cyber-Krieg oder Cyber-Sicherheit –

## wächst aus Abhängigkeiten auch die Einsicht?

*Cyber-Kriegsführung als militärisch-geheimdienstlich motivierte Manipulation von Computern bedroht die Sicherheit der IT-Systeme, von deren Funktionieren mittlerweile die meisten sozialen und politischen Systeme auf diesem Globus abhängig sind. Cyber-Kriegsführung als kleiner Teil der Informationskriegsführung verändert zugleich militärische Organisationen und Operationsformen grundlegend.*

Cyber-Kriegsführung – der Einsatz von Schadsoftware gegen Computer und Netzwerke durch staatliche Akteure – war für viele IT-Sicherheitsexperten lange Jahre ein schein-riesenhaftes Szenario: Es wurde überschaubarer, je intensiver man sich damit auseinandersetzte. Diese Bewertung wird mittlerweile jedoch nicht mehr geteilt.

Ein Grund dafür sind die Beispiele ernst zu nehmende Cyber-Kriegsaktionen. 2007 störte eine Serie von Cyberattacken die digitalen Infrastrukturen Estlands. Im August 2008 begann der kurze Krieg zwischen Georgien und Russland mit gezielten Cyber-Kriegshandlungen, wie ein Jahr später die private U.S. Cyber Consequences Unit (CCU) in einer detaillierten Untersuchung darlegte[1]. Die CCU belegte, dass die Angreifer im Cyberspace Zivilisten ohne direkte Beteiligung russischer Behörden oder Militärs waren, die allerdings im Voraus über russische Militäraktionen informiert waren. Das wichtigste Ergebnis dieser detaillierten Untersuchung war jedoch, dass eine Analyse von IT-Sicherheitsvorfällen heute in sehr ähnlicher Weise möglich ist, wie eine Untersuchung der Auslöser und des Verlaufs eines konventionellen Konflikts durch herkömmliche Militärbeobachter. 2010 schließlich wurde mit Stuxnet ein Computerwurm identifiziert, der hochspezifisch für die Kompromittierung eines Anlagensteuerungssystem der Firma Siemens entwickelt wurde. Die Umstände seines Auftretens im Zusammenhang mit Anlagen des iranischen Atomprogramms, der primäre offline-Verbreitungsweg und der extrem hohe Aufwand zur Programmierung des Wurms legen den Schluss nahe, dass durch die Schadsoftware eine gezielte Sabotage des iranischen Atomprogramms durch staatliche Stellen beabsichtigt war.

### Cyberwar – Infowar

Cyber-Kriegsführung ist eine gezielte Manipulation von Computern und Rechnernetzen mit Mitteln der Informatik und richtet sich daher gegen eine Infrastruktur von militärischer Relevanz. Militärs nutzen Computer aber weit umfassender zu ihren Zwecken: Sie sammeln Daten, übermitteln Kommandos, koordinieren ihre Aktionen mit vielen Beteiligten. Gegen alle Aspekte dieser Art der Informationsverarbeitung durch das Militär als Organisation richtet sich die „Informationskriegsführung" in einer „Informationsumgebung", die aus Sicht der Militärs nur ein Teil der militärischen Operationsumgebung ist.

Zur „Informationsumgebung" gehören die eigenen und gegnerischen militärischen Informationsinfrastrukturen – eigene Computer und abgeschottete Netzwerke – genauso wie das offene

Internet, die Medien und die Akteure, die Informationen in diesen Kanälen verbreiten.

In der 1996 veröffentlichten Informationskriegsführungs-Doktrin der U.S. Army, dem Field Manual 100-6, wurden erstmals Information Operations definiert. 2003 wurde das Manual 100-6 ersetzt durch das Field Manual 3-13[2]. Darin heißt es:

> *„Information operations is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking."*[3]

Die Mittel für Informationskriegsführung lassen sich entsprechend ihrer Intensität und Abfolge in einer Hierarchie ordnen, die eine Abfolge von Eskalationsschritten sichtbar macht. Die niedrigste Eskalationsstufe ist die Beeinflussung von Medien vor einem bewaffneten Konflikt, es folgt das Ausspähen von Daten über potentielle gegnerische Akteure – im Kern: Spionage oder mit dem neutralen Begriff: Aufklärung – und geht über in einen Schadsoftware-Einsatz – also eine Cyber-Kriegsführung. Eine eindeutig militärische Ebene ist die Zerstörung von Infrastrukturen durch „physische Destruktion", die als letzte Stufe bis zum Einsatz von Atomwaffen zur Erzeugung eines elektromagnetischen Impulses reicht, durch den elektronische Geräte in großem Umkreis überlastet und zerstört werden.

Die Integration von Informationskriegsführung in reguläre militärische Operationen zeigt, dass Information Operations – geordnet nach ihrer Gewaltintensität – als Eskalationshierarchie begriffen werden muss, bei der die Grenzen zwischen Krieg und Frieden zusehends verschwimmen.

Trotz dieser umfassenden Sicht nutzen Information Operations nur eine begrenzte Zahl neuer Elemente. Für IT-Systeme, militärische Organisationen sowie Medien und Öffentlichkeit als Ziele von Information Operations wird im Wesentlichen auf bekannte Operationsformen zurückgegriffen. Eingesetzt werden sie

- gegen IT-Systeme: Mittel des *electronic warfare*, Destruktion mit herkömmlichen Waffen sowie neuartigen EMP-Generatoren,
- gegen militärische Organisationen: das Tarnen und Täuschen gegen jede Form der Aufklärung und Spionage, die Störung der Kommunikation durch Mittel der elektronischen Kriegführung sowie psychologische Mittel,
- gegen Medien und Öffentlichkeit: Mittel der psychologischen Kriegsführung, aber auch direkte Gewalt, beispielsweise gegen Journalisten und deren Kommunikationssysteme.

Psychologische Kriegsführung, Spionage, elektronische Kriegsführung und die Destruktion von Kommunikationsknotenpunkten sind schon weit über 60 Jahre im militärischen Einsatz. Schon seit den 80er Jahren wurde über erste Erfahrungen mit dem Einbruch in gegnerische Computernetze berichtet, mangels Vernetzung vielfach jedoch noch durch Einbruch und Einspielen vor Ort[4]. Neu bei diesen Mitteln sind nur technologische Entwicklungen wie nicht-atomare EMP-Generatoren und die systematische Nutzung von Computerviren gegen vernetzte IT-Systeme bei der Cyber-Kriegsführung.



Einher ging mit der Formulierung von Operationen der Informationskriegsführung eine deutliche Ausdifferenzierung von Gefahren, Operationsformen und potentiellen Gegnern[5], deren Ursache vor allem in der Cyber-Kriegsführung liegt. Dank der im Internet inhärent vorhandenen Manipulationsmöglichkeiten mit erheblichem Schadenspotential ist die Vielfalt potentieller Gegner bei einer Cyber-Kriegsführung kaum mehr begrenzt. Aufgezählt als Beteiligte werden neben den Regierungen von potentiellen Gegnern daher die Medien, Industrie und Non-Government Organisations (NGOs). Da als potentielle Schadensverursacher in Computernetzen auch unautorisierte Nutzer, „Insider" und „Nonstate Activists" aufgeführt werden, ist im militärischen Verständnis letztlich jeder Internetnutzer potentieller Gegner in militärischen Informationsoperationen.

Eine relativ überschaubare Zahl neuer militärischer Mittel der Informationskriegsführung und die damit verbundene Sichtweise hat also zu einer ganz erheblichen Ausweitung der „Kampfzone" und der potentiellen Gegner geführt.

### Infowar – eine internationale Entwicklung

Diese Entwicklung wurde zwar in den USA intensiv vorangetrieben, von anderen Ländern aber in ähnlicher Weise adaptiert. Die USA sehen sich daher einer ganzen Reihe von Staaten gegenüber, deren Infrastruktur – also die „Informationsumgebung" – weniger auf vernetzte IT-Systeme angewiesen ist, die aber über ausreichende Fähigkeiten und Ressourcen für Manipulationen an IT-Systemen, also eine Cyber-Kriegsführung, verfügen. Hinzu kommt, dass sich Cyber-Kriegsführung durch militärische oder geheimdienstliche Organisationen ebenso wie Spionage nicht nur gegen militärische Gegner, sondern auch gegen Bündnispartner richten kann.

Selbst wenn man also keine „Nonstate Activists" berücksichtigt, so kommen als Beteiligte in Informationskriegen neben den Hochtechnologie-Staaten auch zahlreiche Schwellenländer in Betracht:

- Russland setzt weniger auf Computer als auf die Intensivierung konventioneller Methoden, vor allem der psychologischen und elektronischen Kriegführung[6], verfügt aber zumindest im Privatsektor eindeutig über eine ausreichende Basis an Technik und Kompetenzen zu moderner Cyber-Kriegsführung;
- China reklamiert nicht nur die Erfindung des Begriffs „Information Warfare" für sich, sondern verfügt über ähnlich umfassende Konzepte wie die US-Militärs[7] und setzt auf einen „Volksinformationskrieg"[8];
- Taiwan nutzt die Stärken in der Elektronikbranche und setzt auf den Einsatz von Computerviren und ähnlichen Manipulationsmitteln[9];



- Indien beginnt nach der Adaption amerikanischer Ideen mittlerweile damit, differenzierte und auf die eigenen Fähigkeiten im IT-Bereich zugeschnittene Ansätze der Cyber-Kriegsführung zu entwickeln[10].

In Deutschland hat sich die Bundeswehr seit Mitte der 90er Jahre dem Schutz vor Information Warfare-Attacken gewidmet und entwickelte Ansätze zu Information Operations als Planungsinstrument[11]. Unterschiedliche Teilaktivitäten im Rahmen von Informationskriegsführung werden von der Bundeswehr in unterschiedlichen Truppenteilen und Einrichtungen verfolgt. 2002 wurden die ersten organisatorischen Grundlagen gelegt, die 2007 um weitere Aufgaben ergänzt wurden.

Die Erhebung aus verschiedenen offenen Quellen war Aufgabe von zwei mittlerweile umstrukturierten Einrichtungen. Die Feldnachrichtenkräfte in der Bundeswehr sind für Personenbefragungen und Beobachtung zuständig, das Feldnachrichtenzentrum in Dietz wurde jedoch 2008 aufgelöst. Das Zentrum für Nachrichtenwesen der Bundeswehr in Gelsdorf betrieb die Aufklärung und Lagebewertung aus offenen Quellen. Es wurde 2007 aufgelöst und teilweise dem Bundesnachrichtendienst (BND) zugeschlagen.

Der Psychologischen Kriegsführung entstammt das Zentrum Operative Information in Mayen, das Psychologische Verteidigung („langfristige Einstellungs- und Verhaltensänderung erreichen") betreibt und mit dem Radio Andernach als Truppensender und Video-Trupps in Einsatzgebieten auf Sendung geht. Für Aufklärung und Informationsbeschaffung zuständig ist außerdem der Militärische Abschirmdienst (MAD), der mit dem BND Daten austauscht.

In der Bundeswehr ist das 2002 gegründete Kommando Strategische Aufklärung (KSA) der Truppenteil, dem bei Aufklärung, Psychologischer Kriegsführung und Computer-Netzwerkoperationen der größte Teil des Spektrums von Informationskriegsaufgaben zugewiesen wurde. Im KSA wurden alle bisher in den Teilstreitkräften der Bundeswehr vorhandenen Kräfte und Mittel der elektronischen Kriegsführung, also der ortsfesten und mobilen so genannten Fernmelde-/Elektronischen Aufklärung (Fm/EloAufkl), die des Elektronischen Kampfes des Heeres (EloKa) sowie der Satellitengestützten Abbildenden Aufklärung (SGA für SAR-Lupe) im KSA in Gelsdorf und anderen Orten zusammengeführt. Damit wurden im KSA zur Gründung 6.300 Militärs und 700 Zivilbeschäftigte zusammengefasst. 2007 wurde das KSA umstrukturiert, es wurden Standorte aufgegeben. 2009 kam dann die Abteilung „Informations- und Computernetzwerkoperationen" in Rheinbach zum KSA neu hinzu. Im Mai 2010 wurde die „Gruppe Informationsoperationen", die mit der Produktion von Medieninhalten betraut ist, dem Zentrum Operative Information (ZOpInfo) in Mayen zugeordnet[12].

Getrennt von diesen operativen Einheiten der Bundeswehr ist das ebenfalls im November 2002 nach zweijähriger Planung eingerichtete Computer Emergency Response Team der Bundeswehr, CERTBw, das beim IT-Amt der Bundeswehr in Euskirchen untergebracht ist. Das CERTBw hat – wie andere derartige Teams auch – die Aufgabe, Angriffe auf die IT-Infrastrukturen der Bundeswehr zu erkennen und Schutzmaßnahmen zu treffen. Zur Philosophie des CERTBw gehört, sich mit zivilen CERTs auszutauschen, und organisatorisch und konzeptionell eine konventionelle defensive Aufgabe zu verfolgen. Das CERTBw ist daher auch Mitglied im CERT-Verbund[13] und stellt seine Arbeit auch bei zivilen Veranstaltungen zur IT-Sicherheit dar[14].

### Kritische Infrastrukturen: Militarisierung der IT-Sicherheit?

Militärs, die in einem Informationskrieg gegnerische militärische Systeme mit Störsendern der elektronischen Kriegsführung oder anderen Mitteln angreifen, sind eine leider nur zu alltägliche Erscheinung. Mit Angriffen auf Computersysteme verändern sich die Gewichte. Die sicherheitsrelevanten militärischen Kommandonetze waren bislang vom Internet abgeschottet; Einzelheiten über Manipulationen an diesen Netzen gelangen nur selten an die Öffentlichkeit.

Zunehmend sind jedoch auch rein militärische Netze mit dem Internet vernetzt. Zum einen, um das Internet für die Informationsbeschaffung zu nutzen, vielfach aber auch, um weniger sensitive Daten zu übermitteln. Durch diese Vermischung von zivilen und militärischen IT-Netzwerken und die Abhängigkeit der Militärs von zivilen logistischen und organisatorischen Infrastrukturen gewinnt die Bedrohung an Bedeutung, dass sich potentiell gegnerische Militäreinheiten oder „Cyberterroristen" an zivilen IT-Infrastrukturen zu schaffen machen. Da „Cyberterroristen" im Normalfall keinen Zugang zu abgeschotteten militärischen Netzwerken haben, sind ihre Ziele jene offen verfügbaren Infrastrukturen, von deren störungsfreiem Funktionieren die zivile Informationsgesellschaft vital abhängig ist. Diese Abhängigkeit macht solche IT-Infrastrukturen zu „kritischen Infrastrukturen". Als kritisch werden Infrastruktursysteme definiert, deren Ausfall in einer technisierten Gesellschaft zu erheblichen Problemen führt. Diese sind Informations- und Kommunikationssysteme, die Energieversorgung und fossile Brennstoffe, das Banken- und Finanzsystem, Verkehr, Wasserversorgung, Notfall- und Rettungsdienste und Regierungsdienste.

Aus dieser Abhängigkeit erwächst der Anspruch, kritische zivile Infrastrukturen mit Mitteln der IT-Sicherheit in militärischer Hand zu schützen. Auch das CERTBw ist in dieser Sichtweise eine an zivilen Kooperationsstrukturen ausgerichtete Spezialistentruppe zu genau diesem Zweck.

Das führt zu der Frage, ob es nun möglich und denkbar ist, dass bei einer Manipulation von zivilen IT-Infrastrukturen schnell erkannt wird, wer die Urheber sind, um dann ebenso schnell zu entscheiden, zivile oder militärische Einrichtungen mit Gegenmaßnahmen zu beauftragen? Bisher gibt es jedenfalls noch keinen Beleg dafür, dass bei Cyber-Attacken so schnell und eindeutig bewertet und gehandelt wurde. Statt dessen wurden Attacken oft jugendlicher Hacker[15] vorschnell als gefährliche Cyber-Angriffe und „Cyberterrorismus" bezeichnet.

### Cyberterrorismus

Wer den Begriff Cyberterrorismus ausloten will, sollte sich zuerst vor Augen halten, dass „Terrorismus" schon in seiner konventionellen Bedeutung ein stark politisch geprägtes Etikett ist, das von Politikern äußerst willkürlich vergeben wird, aber auch von

den Strafverfolgungsbehörden wenig präzise verwendet wird. Der Vergleich von Strafermittlungen und Strafverfahren zum zentralen Terrorismus-Paragraphen, dem 129a, ergab: „So kam es lediglich in 5 % der vom Generalbundesanwalt geführten § 129a StGB-Verfahren und gegen 8 % der Beschuldigten überhaupt zu einer Anklage“[16], da kein Tatverdacht gegeben war.

Wenn schon konventioneller Terrorismus bei 90 % der Verdächtigten zu unrecht unterstellt wird, dürfte „Cyberterrorismus“ – bei dem man der verdächtigen Personen so gut wie nie habhaft wird oder politisch unbedarfte Jugendliche ermittelt – ein analytisch recht sinnloser Begriff sein, von dem sich manche Akteure allenfalls Nutzen als Aufmerksamkeit erheischender Domainname erhoffen[17]. Auch Sicht von IT-Sicherheitsfachleuten führt der Begriff vor allem zu „fundamentalen Missverständnissen“[18]: Es kann zwar sein, dass konventionelle Terroristen über Kenntnisse der Manipulation von Computern verfügen und für ihre Zwecke einsetzen. Die psychologischen und medialen Effekte aber, auf die bei asymmentrischer Kriegsführung und Terrorismus abgezielt wird, lassen sich durch „Cyberterrorismus“ kaum erreichen, da es medial bisher nicht gelungen ist, Manipulation an IT-Systemen überhaupt mit politischen oder anderen Zielen in Verbindung zu bringen.

„Cyberterrorismus“, dessen Bekämpfung sich Militärs zusätzlich zuwenden, ist damit in jeder Hinsicht eine äußerst vage Begründung für eine neue Verteilung von Aufgaben zwischen staatlichen Einrichtungen zum Schutz der IT-Sicherheit.

### Cyberterrorismus – und die Strafverfolgung

Cyberterrorismus wirft also die Frage auf, wer im Rahmen einer Cyber-Kriegsführung für deren Abwehr zuständig sein und für diese Aufgabe erweiterte Ressourcen – Personal und Finanzmittel – erhalten sollte: zivile oder militärische Organisationen. Nun ist die Terrorismusbekämpfung keine Aufgabe von Militärs, sondern der Strafverfolgungsbehörden. In der Bundesrepublik gibt es außerdem seit 1986 Straftatbestände für die Manipulation an und das Ausspähen von Computern, wenngleich die Zahl der damit juristisch verfolgten Straftaten jedoch nur ein verschwindend geringer Teil der tatsächlichen Fälle waren und sind. Zur exemplarischen Beantwortung der Frage für Deutschland ist es daher notwendig, den schon genannten militärischen IT-Einrichtungen ihre zivilen Pendants gegenüber zu stellen.

Als Bündelung von Fachkompetenz erfolgte 2007 die Einrichtung des Gemeinsamen Internetzentrum beim Gemeinsamen Terrorismusabwehrzentrum (GTAZ), in dem ein großer Teil der IT-Kompetenzen der Strafverfolger und zivilen IT-Sicherheitsbehörden von Bund und Ländern zusammen arbeiten.

Soweit es die dürre Datenlage hergibt, sind bei den Polizeibehörden von Bund und Ländern insgesamt etwa 350 Beamte mit der Überwachung des offenen Internets beschäftigt[19]. Überwiegendes Einsatzgebiet sind Delikte im Bereich der Kinderpornografie. Laut Bundesinnenministerium waren im GTAZ zumindest zu Beginn 190 Personen in der Terrorbekämpfung beschäftigt[20]. Es handelt sich um Experten aus dem BKA, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, den Kriminal- und Verfassungsschutzämtern der Länder, der Bundespolizei, dem Zollkriminalamt, dem Militärischen Abschirmdienst, dem Bundesamt für Migration und Flüchtlinge und dem Generalbundesanwalt. Das GTAZ bindet also ca. 100 der 350 bekannten und mit der Internetfahndung betrauten Polizisten der Republik. Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sind derzeit insgesamt ca. 400 Mitarbeiter beschäftigt, aber nur ein kleiner Teil davon mit der Analyse von IT-Sicherheitsfragen. Das 2011 gestartete Internet-Sicherheitszentrum beim BSI nahm seine Arbeite mit 10 Mitarbeitern auf[21]. Seit Juni 2011 wirken auch der Bundesnachrichtendienst (BND) sowie die Bundeswehr als assoziierte Behörden mit[22]. Bei der Bundeswehr ist die Zahl hoch spezialisierter IT-Sicherheitsexperten beim CERTBw nicht größer, die Gruppe „Informations- und Computernetzwerkoperationen“ des KSA sollte zu Beginn 76 Mitarbeiter umfassen[23].

Auch die Vermehrung von Organisationen in den letzten Jahren hat somit zu keiner nennenswert größeren Zahl von Personal bei staatlichen Stellen für genuine IT-Sicherheitsaufgaben geführt. Statt dessen kooperieren alle bisher bestehenden Zentren nun in neuen Formen miteinander. Dass dieselben IT-Sicherheits-Fachleute deutscher Behörden nun einen größeren Teil ihrer Arbeitszeit für den gegenseitigen Austausch und für die Abstimmung aufwenden, mag Doppelarbeit vermeiden helfen und der Verdichtung von Problemlagen dienen. Der eigentlichen zu leistenden fachlichen Arbeit hilft dies jedoch weniger. Es ist daher eine Frage der erst noch zu leistenden zukünftigen Evaluation der Ergebnisse, ob dieses Pooling von Ressourcen einen positiven Effekt hat.

### Begrenzung von Informationskriegsführung

Informationskriegsführung sieht das Internet als Kampfraum. Cyber-Kriegsführung bedient sich der Manipulation von Computersystemen als Kampfmittel. Die gegen Industrie-Steuerungsanlagen programmierte Stuxnet-Schadsoftware belegt, dass nicht nur die mit dem Internet vernetzten Computer Ziele

**Ingo Ruhmann**

**Ingo Ruhmann**, Informatiker, wissenschaftlicher Referent und Lehrbeauftragter, Gründungsmitglied und ehemaliges Vorstandsmitglied im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Arbeiten zu Datenschutz, IT-Sicherheit, sowie Informatik und Militär.



von Angriffen sind, sondern auch solche in abgeschotteten Industrieanlagen, sofern dasselbe Computermodell zufälligerweise auch in irgend einer strategisch wichtigen Industrieanlage genutzt wird.

Cyber-Kriegsführung durch Militärs und Geheimdienste – nicht „Cyberterrorismus" – bedroht die zivilen Infrastrukturen der Informationsgesellschaft. Der „Virtual Criminology Report" des IT-Sicherheitsunternehmens McAfee beschäftigte sich 2009 erstmals nicht mit allgemeinen IT-Sicherheitsproblemen und deren kriminellen Verursachern, sondern mit staatlichen Stellen und den Bedrohungen durch die „so gut wie eingeläutete" Cyber-Kriegsführung[24]. McAfee fordert eine offene Debatte über die Gefahren von Cyber-Kriegen. Es gehe darum, die weitgehend hinter verschlossenen Türen stattfindende Diskussion über Cyber-Kriegsführung, die gravierende Folgen für die Allgemeinheit haben werde, auch in der Öffentlichkeit zu diskutieren.

Immerhin haben die Aktionen der letzten Jahre zu der Einsicht geführt, dieses sicherheitspolitische Thema nicht allein aus militärischem Blickwinkel zu sehen, sondern auch zum Gegenstand einer politischen Abstimmung zu machen. Am 13. Dezember 2009 meldete die New York Times, dass die USA Verhandlungen mit Russland aufgenommen habe, um eine „Verbesserung der Internet-Sicherheit und eine Begrenzung der militärischen Nutzung des Internet"[25] zu erreichen. Weitere Gespräche seien 2010 in New York und Garmisch-Partenkirchen terminiert.

Allein die Existenz dieser Gespräche stellte eine deutliche Abkehr von einer jahrelangen Abwehr gegen Verhandlungen über dieses Thema dar. Ein nahe liegender Maßstab für die Bedeutung dieser Gespräche ist der Vergleich mit dem heute zur Informationskriegsführung zählenden elektronischen Kriegsführung. Dabei geht es um das Ausspähen elektronischer Signale und Kommunikation und entsprechende Schutzmaßnahmen. Der seit dem zweiten Weltkrieg ununterbrochen andauernde Einsatz der elektronischen Kriegsführung ist gekennzeichnet durch einen ganz speziellen Rüstungswettlauf. Dazu gehören nicht nur elektronische Gegenmaßnahmen, sondern auch elektronische Gegen-Gegenmaßnahmen, wie das Abstrahlen von Störsignalen oder das Aussenden hochenergetischer Strahlung, die elektronisches Gerät zeitweilig oder dauerhaft lahmlegt. Ein Ende dieses Wettlaufes ist nicht abzusehen. Die Schäden durch diese, meist auf militärische Systeme angewandte Form der Informationskriegsführung sind jedoch begrenzt.

Für Cyber-Kriege mit Computerviren und Netzattacken gilt diese Begrenztheit nicht. Es wäre daher für alle Seiten vernünftig, Schäden zu vermeiden und eine internationale Verständigung zu erreichen[26]. Nicht ganz so überraschend war aber nach den ersten Gesprächen zur Kontrolle von Cyber-Kriegsführung, dass im Wesentlichen über Differenzen berichtet wurde, die nur begrenzte Fortschritte erhoffen lassen. Ein Ansatz dafür könnte die von US-Präsident Obama im Mai 2011 vorgestellte globale Cyberspace-Strategie sein, die schon als kurzfristige Maßnahme vorsieht, ein „internationales Cybersecurity-Politik-Rahmenwerk" zu entwickeln, um gemeinsam mit anderen Staaten die Sicherheit im Internet zu verbessern[27].

**Fazit**

Fest steht, dass IT-Systeme unsicher und offen für Manipulationen sind. Zusätzlich zur grundlegend verbesserten Sicherheit von IT-Systemen sind Organisationen wie CERTs und deren Kooperation nötig zum Schutz gegen Manipulationen. Ohne zusätzliche Fachleute in diesen spezialisierten Organisationen wird die Verbesserung des Niveaus der IT-Sicherheit jedoch nicht erreichbar sein.

Wenn zwischenstaatliche Konflikthintergründe bei IT-Sicherheitsproblemen an Bedeutung gewinnen, wird die unweigerliche Folge eine weitere sicherheitspolitische Destabilisierung bei Bedrohungen der IT-Sicherheit sein. Durch ein stärkeres militärisches Engagement und einen damit einhergehenden Rüstungswettlauf analog zur elektronischen Kriegsführung kann aber weder eine höhere Effektivität in Sachen IT-Sicherheit erwartet werden noch eine Stärkung der Strafverfolgung.

Internationale Übereinkünfte zur Verbesserung der IT-Sicherheit – zusätzlich zu stärkeren Investitionen in die zugehörige Technik – und Begrenzung von Information Warfare[28] sind daher der einzige Weg zu einer zivil nutzbaren verlässlichen IT-Infrastruktur. Die politische Einsicht in die Notwendigkeit scheint vorhanden. Die Zukunft wird zeigen, ob sie ohne größere IT-Katastrophen auch zu einem tragfähigen Ergebnis führt.

## Anmerkungen

1 *US-CCU Special Report: Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008; August 2009; http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf*

2 *U.S. Department of the Army: FM 3-13 (FM 100-6) Information Operations: Doctrine, Tactics, Techniques, and Procedures, November 2003, URL: http://www.carlisle.army.mil/DIME/documents/FM%203-13%20-%20Info%20Opns%20Doc,%20Tactics,%20Tech,%20and%20Proced%5B1%5D.pdf*

3 *FM 3-13, ebd., S. 1-13*

4 *Jay Peterzell: Spying and Sabotage by Computer; in: Time, March 20, 1989, S. 41; Oberstleutnant Erhard Haak: Computerviren – ein Kampfmittel der Zukunft?; in: Soldat und Technik, Nr. 1, 1989, S. 34-35.*

5 *FM 3-13, ebd., S. 1-2ff*

6 *Igor Panarin: InfoWar und Autorität; in: G. Stocker, C. Schöpf (Hg.): Information.Macht.Krieg; Wien 1998, S. 105-110*

7 *Shen Weiguang: Der Informationskrieg – eine neue Herausforderung; in: G. Stocker, C. Schöpf (Hg.): Information.Macht.Krieg; Wien 1998, S. 67-91*

8 *Wei Jincheng: Der Volksinformationskrieg; in: G. Stocker, C. Schöpf (Hg.): Information.Macht.Krieg; Wien 1998, S. 92-104*

9 *Florian Rötzer: Taiwans Militär probt Angriffe mit Computerviren; in: Telepolis, 8.8.2000, http://www.heise.de/tp/deutsch/special/info/6955/1.html.*

10 *C. Uday Bhaskar: Trends in Warfare: A Conceptual Overview; in: Strategic Analysis, Dec. 2000, S. 1577-1589, vgl auch: Ajai K. Rai: Media at War: Issues and Limitations, Strategic Analysis, Dec. 2000, S. 1681-1694; sowie: Vinod Anand: An Integrated and Joint Approach Towards Defence Intelligence; in: Strategic Analysis, Nov. 2000, S. 397-1410.*

11 *Ralf Bendrath: Informationstechnologie in der Bundeswehr; in: Telepolis, 25.7.2000, http://www.heise.de/tp/deutsch/special/info/6933/1.html.*

12 *Informationsprofis arbeiten enger zusammen; Bundeswehr-Pressemeldung vom 29.06.2010; http://www.opinfo.bundeswehr.de/portal/a/opinfo/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uykPyCzLy0fL3SvOLUotT4HL0qqACIyC_QK01NSi1KT0xK1S_IdlQEAJFZpok!/*

13 *http://www.cert-verbund.de/*

14 *Vgl. u.a. den Vortrag an der Uni Koblenz: http://www.uni-koblenz-landau.de/koblenz/fb4/institute/iwvi/egov-network/egov-day/historie/egov-day-2007/Vortrag_Rohde.pdf*

15 *Vgl. dazu den Fall von jugendlichen Hackern, die vom FBI als internationale Verschwörung bezeichnet wurden, vgl.: Armin Medosch: FBI deckt internationale Verschwörung von Cyber-Terroristen auf; in: Telepolis, 17.1.2001, http://www.heise.de/tp/deutsch/special/info/4701/1.html*

16 *Staatsschutzkriminalität, Lexikon Kriminologie des Lehrstuhls für Kriminologie und Polizeiwissenschaft der Ruhr-Universität Bochum, http://vmrz0183.vm.ruhr-uni-bochum.de/krimlex/artikel.php?BUCHSTABE=S&KL_ID=177*

17 *wie etwa: www.cyberterrorism.org*

18 *Sarah Gordon, Richard Ford: Cyberterrorism? Symantec Whitepaper, Cupertino, 2003, http://www.symantec.com/avcenter/reference/cyberterrorism.pdf*

19 *Virtuelle Front; in: Der Spiegel, Nr. 30, 2007, S. 26 – 27, S. 27*

20 *http://www.bmi.bund.de/cln_028/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Gemeinsames__Terrorismusabwehrzentrum__de.html*

21 *Nationales Cyber-Abwehrzentrum nimmt Arbeit auf, BSI-Pressemitteilung vom 1.04.2011, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Cyber-Abwehrzentrum_01042011.html*

22 *Bundesinnenminister Dr. Hans-Peter Friedrich eröffnet das Nationale Cyber-Abwehrzentrum, BSI-Pressemitteilung vom 16.06.2011, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Eroeffnung-Nationales-Cyber-Abwehrzentrum_16062011.html*

23 *Der Spiegel: Bundeswehr baut geheime Cyberwar-Truppe auf, 07.02.2009, http://www.spiegel.de/spiegel/vorab/0,1518,606095,00.html*

24 *McAfee: Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare, Santa Clara, 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF*

25 *John Markoff; Andrew E. Kramer: In Shift, U.S. Talks to Russia on Internet Security; http://www.nytimes.com/2009/12/13/science/13cyber.html*

26 *Committee on Deterring Cyberattacks: Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for U.S. Policy; National Academy Press, Washington 2010*

27 *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, S. vi, Mai 2011, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*

28 *Ingo Ruhmann: Rüstungskontrolle gegen den Cyberkrieg? In: Telepolis, 4.01.2010, http://www.heise.de/tp/artikel/31/31797/1.html*



**Ute Bernhardt**

# Master of Peace Studies

*Wie kann sich eine Ärztin oder ein Jurist auf den Einsatz im Konfliktgebiet vorbereiten? Wo kann ein Journalist mehr über die Ursachen terroristischer Gewalt erfahren? Was sollten Zivilisten, die als internationale Beobachter in Konfliktregionen entsandt werden, von moderner Kriegsführung, ABC-Waffen, aber auch von Information Warfare wissen?*

Beim Studiengang **Master of Peace Studies** handelte es sich um einen interdisziplinären weiterbildenden Masterstudiengang der FernUniversität Hagen am Institut für Frieden und Demokratie. Der Studiengang startete 2001 und verstand sich als Antwort auf den in vielen Berufsfeldern wachsenden Bedarf an wissenschaftlichen Kompetenzen in den Bereichen Konfliktbearbeitung, Gewaltabbau und nachhaltige Friedenssicherung. Die Studierenden sollten, aufbauend auf ihre in einem ersten Studium erworbene Fachkompetenz, durch wissenschaftlich angeleitete kritische Reflexion ihrer beruflichen Praxis, Expertise für den Umgang mit gewaltförmigen Konflikten entwickeln.

Das Studienangebot wandte sich insbesondere an Mitarbeitende internationaler staatlicher und nicht-staatlicher Organisationen, Fachkräfte der Entwicklungszusammenarbeit, Pädagogen/innen, Sozialwissenschaftler/innen, Trainer/innen und Journalisten/innen.

Die Entwicklung und der Betrieb des Studiengangs wurde erst durch die Förderung durch die Deutsche Stiftung Friedensforschung möglich. Diese Förderung lief Ende 2008 aus. Seit diesem Zeitpunkt wurden keine neuen Studierenden aufgenommen. Mit dem Ende der Masterabschlussarbeiten 2010 endet auch der Studiengang. Die 40 Studienplätze pro Jahr wurden durchweg belegt. Gespräche zur Fortführung des Studiengangs an anderen Hochschulen waren bisher leider erfolglos.

Den Wahlpflichtbereich zu Frieden und Naturwissenschaften wurde von Dr. Jürgen Altmann, Ute Bernhardt, Prof. Dr. Kathryn Nixdorf, Ingo Ruhmann, Prof. Dr. Dieter Wöhrle verantwortet. Die Inhalte waren schwerpunktmäßig Abrüstung, Naturwissenschaft und Informatik sowie militärische Nutzung derselben zur Forschung und Entwicklung. Dazu entstand auch das Lehrbuch

> *Jürgen Altmann, Ute Bernhardt; Kathryn Nixdorf, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung. Lehrbuch. Wiesbaden, VS-Verlag, 2007.*

Weitere Informationen zum Studiengang sind zu finden unter:

*http://www.fernuni-hagen.de/FRIEDEN/downloads/5305konfliktundfriedennetz.pdf*

**Ralf E. Streibl**

# Für eine zivilisierte Bildung und Wissenschaft



*Aus dem DUDEN-Herkunftswörterbuch (DUDEN Bd. 7, 2001):*

***Zivilisation***
*„die Gesamtheit der durch den Fortschritt von Wissenschaft und Technik geschaffenen [verbesserten] Lebensbedingungen"*

***zivilisieren***
*„gesittet machen, verfeinern, kultivieren; mit der Zivilisation vertraut machen"*

## Kein bisschen Frieden ...

Johan Galtung, der bekannte norwegische Friedens- und Konfliktforscher, unterscheidet verschiedene Arten von Gewalt: direkte, strukturelle und kulturelle Gewalt. *Direkte Gewalt* bezeichnet den Typus von Gewalt, bei der es einen spezifischen Akteur gibt und die daher auch eher sichtbar ist. *Strukturelle Gewalt* geht zurück auf (repressive oder ausbeuterische) Machtverhältnisse, auf ökonomische, rechtliche, organisatorische Strukturen etc. Unter den Begriff der *kulturellen Gewalt* fasst Galtung insb. die Legitimationsprozesse, die innerhalb einer Kultur direkte oder strukturelle Gewalt rechtfertigen. Direkte Gewalt manifestiert sich somit – nach Galtung (1998) – als ein Ereignis, strukturelle Gewalt hingegen ist ein Prozess. Kulturelle Gewalt wiederum zeichnet sich seiner Ansicht nach durch eine längerfristige Stabilität aus, weshalb er sie beschreibt als *„eine Invariante, eine ‚Permanenz', die aufgrund der nur langsamen Transformationen grundlegender Aspekte der Kultur über lange Zeiträume hinweg im wesentlichen unverändert bleibt"* (S. 348). Beispiele hierfür findet Galtung u.a. in Religion, Ideologien, Kunst, Sprache und auch Wissenschaften (1990, S. 296ff).

Die drei genannten Gewalttypen sind dabei nicht unabhängig voneinander, sondern können sich gegenseitig befruchten: *„Gewalt kann ihren Ausgang nehmen an jeder Ecke des Dreiecks direkte-strukturelle-kulturelle Gewalt und leicht zu den anderen Ecken überspringen"* (1998, S. 365). Vor dem Hintergrund institutionalisierter struktureller Gewalt und internalisierter kultureller Gewalt manifestieren sich beispielsweise Tendenzen, direkte Gewalt selbst auch zu institutionalisieren (1990, S. 302). Umgekehrt kann direkte Gewalt ihrerseits wieder strukturelle und kulturelle Gewalt verstärken.

Solch ein differenzierter Gewaltbegriff impliziert auch ein erweitertes Friedenskonzept: Galtung unterscheidet daher zwischen *negativem Frieden*, der einzig durch die Abwesenheit von direkter Gewalt (z. B. in Form von zwischenstaatlichem Krieg) gekennzeichnet ist, und dem Konzept eines *positiven Friedens*, der durch Wegfall von Ausbeutung, Unterdrückung, Entfremdung sowie Verwirklichung von Entwicklungschancen und sozialer Gerechtigkeit gekennzeichnet ist. Frieden in diesem Sinne ist Bedingung für eine Entwicklung ohne Gewalt (vgl. Galtung 1998, S. 387). Weiterhin betont Galtung, dass es hierbei aber nicht um eine statische Systemeigenschaft geht. Infolgedessen formuliert er ein „Dynamisches Friedenskonzept": *„Frieden haben wir dann, wenn eine kreative Konflikttransformation ohne den Einsatz von Gewalt stattfindet"* (S. 458) – Kriterium für Frieden ist somit die Fähigkeit, mit Konflikten umzugehen. Erforderlich hierfür ist gleichermaßen eine Friedensstruktur wie auch eine Friedenskultur. Dem entgegen steht jedoch die bis heute in vielen Köpfen fest verwurzelte Überzeugung, Frieden sei nur durch Stärke erreichbar. Boehnke, Christie und Anderson zeigen gleichermaßen die Langlebigkeit und die Verbreitung solcher kultureller Überzeugungen auf, wenn sie schreiben: *„Die dominante kulturelle Überlieferung unserer Zeit entstammt der Antike. Sie lautet: ‚Si vis pacem para bellum!'[1] und findet sich fast wortgleich im vormaligen Credo der Nationalen Volksarmee der DDR ‚Der Frieden muss bewaffnet sein!'"* (2004, S. 35).

Auch wenn Galtungs Gewalttypologie wegen ihrer mangelnden begrifflichen Schärfe oder Operationalisierbarkeit kritisiert wurde, bietet sie jedoch einen guten Ausgangspunkt, die unterschiedlichen Ebenen von Individuum, gesellschaftlichen Strukturen und Kultur in Zusammenhang mit den Fragen Gewalt bzw. Krieg zu betrachten.

## Weltpolitik und Kriegskultur

Die Debatten um Rüstungsforschung oder Dual-Use[2] an Universitäten und Forschungseinrichtungen sowie die Diskussionen über Werbeveranstaltungen von Militärkräften wie der Bundeswehr in Schulen und auf Bildungsmessen sind vordergründig oft gekennzeichnet durch eine klare Ablehnung und deutlichen Widerstand: Protest wird artikuliert *gegen* Militarisierung von Bildung, *gegen* direkte Kooperationen mit Militär oder Rüstungsbetrieben und – weitergehend – *gegen* die möglichen Dual-Use-Aspekte von Forschung und Entwicklung z. B. an Hochschulen.

Die einführenden Bemerkungen zu Galtungs Gewalt- und Friedensbegriff machen deutlich, warum eine derartige Position zwar sinnvoll und notwendig ist, aber so nicht ausreicht. Die real vorhandenen Rüstungsarsenale sowie das in vielen militärischen Strategiepapieren ausgedrückte Streben nach (u.a. auch technologischer) Überlegenheit belegen die immanenten Strukturen von Unfriedlichkeit.

Ein häufig geäußerter Vorwurf, wenn man diese Position vertritt, ist, dass ein „idealistischer Radikalpazifismus" nichts mit der Realität dieser Welt zu tun habe – schließlich gebe es dort Waffen, Konflikte, Bedrohungen, und damit seien Rüstung und militärische Stärke notwendig, um sich zu verteidigen bzw. ggf. anderen beistehen zu können. Dabei wird jedoch verkannt, dass

gerade diese Position im Galtungschen Sinne einen Teil kultureller Gewalt darstellt. Natürlich lassen sich solche Einstellungen und Haltungen in einer Gesellschaft und erst recht weltweit nicht kurzfristig verändern. Doch andererseits ist genau an dieser Stelle anzusetzen, um der Rechtfertigung direkter Gewalt in Konflikten langfristig entgegenzuwirken und ihr die scheinbare Legitimation zu entziehen.

#### Die *neue* Sicherheitspolitik

Die Umbrüche in Osteuropa ließen manch einen kurzfristig hoffen, dass die langjährige Dominanz militärischen Kalküls sowie die Ideologie von Abschreckung und der Notwendigkeit militärischer Stärke zu Ende gehen könnten. Es dauerte jedoch nicht lange, bis George Bush im Kontext der UN-Intervention gegen den Irak eine „neue Weltordnung" ausrief. Viele glaubten damals, Zeugen einer positiven Veränderung zu werden: Nach dem Ende des Ost-West-Konfliktes könnten die Großmächte zusammenkommen und im Auftrag der UN den gemeinsamen Kampf des *Guten* führen, wenn Frieden und Gerechtigkeit in der Welt von einzelnen *Bösen* bedroht würden. Gerne wurde dabei übersehen, dass – je nach Interessenlage – vorher gerne mit genau diesen *Bösen* kooperiert wurde. Deutlich wird dies z. B. an den Verbindungen der USA mit Saddam Hussein, der zeitweise als Gegner des im Iran regierenden Regimes geschätzt wurde. Als während dieser Zeit eine Delegation irakischer Oppositioneller in Washington um Unterstützung ihrer Bestrebungen nach Einführung einer parlamentarischen Demokratie ersuchte, wurde sie abgewiesen (vgl. Chomsky 1999b). Ähnliches wird nun in jüngster Zeit in Zusammenhang mit den Veränderungen im arabischen Raum offenkundig: Wie sehr wurden zeitweise die jeweiligen Machthaber Ben Ali, Mubarak oder Gaddafi im Westen hofiert!

Die Idee der Hilfe für bedrohte oder unterdrückte Menschen ist orientiert an humanitären Werten und zeugt von gesellschaftlicher Verantwortung. Sie ist nicht zu kritisieren. Zu hinterfragen ist allerdings, dass in den letzten zwei Jahrzehnten der „neuen Weltordnung" hierunter anscheinend mit zunehmend regelhafter Selbstverständlichkeit militärische Interventionen verstanden werden (wobei die realen Entscheidungskriterien, *in welchen Fällen* interveniert wird, nur teilweise transparent sind; vgl. hierzu auch Chomsky 1999a). Bezogen auf die Bundesrepublik und die neue Rolle der Bundeswehr korrespondiert diese Veränderung auf weltpolitischer Ebene mit den in den *Verteidigungspolitischen Richtlinien* vom November 1992 skizzierten Planungen, die eine „Wende in der bundesdeutschen Außenpolitik" markierten, den „Einsatz der Bundeswehr für praktisch beliebige Zwecke" ermöglichten und damit den Weg zu ziviler Konfliktlösung und Ursachenbeseitigung versperrten (Schluroff 1998, S. 199; für eine Analyse der diesbezüglichen Wende in der bundesdeutschen Presseberichterstattung vgl. Meder 1998; zu den aktuellen Prozessen der Normalisierung militärischer Gewalt im öffentlichen Diskurs vgl. u.a. Jäger 2011).

Die Entwicklungen seit den Anschlägen vom 11. September 2001 und dem damals ausgerufenen „Krieg gegen den Terror" trieben die Entwicklung weiter voran – militärische Lösungen werden direkt als geeignete Option der Politik und als gerechtfertigte Handlungsoption angesehen. Fuchs (2004, S. 241f) beschreibt diesen Weg von den „humanitären Interventionen" zur Wiedereinführung eines „Rechts auf Kriegführung" unter der Überschrift „Wiederbelebung der Kriegskultur". Mit dem Slogan „Kampf gegen internationalen Terrorismus" werden seither nicht nur Kriegseinsätze gerechtfertigt, sondern auch eine Intensivierung staatlicher Überwachung, Kontrolle und Datensammelei (d. h. die Intensivierung struktureller Gewalt im Sinne Galtungs) und sogar offensichtliche Verstöße gegen die Menschenrechte bis hin zu Folter.



## Militarisierung von Bildung in Deutschland

Will man mittel- und langfristig zu einer echten und nachhaltigen *Neuen Weltordnung* im Sinne einer kulturellen Änderung kommen, charakterisiert durch einen Frieden, der mehr ist als die Abwesenheit von Krieg (selbst von diesem Ziel ist man heute ja weiter entfernt als zuvor!), muss früh in Sozialisation und Bildung angesetzt werden. Wer frühzeitig Alternativen zu Gewalt in der Konfliktlösung kennenlernt, mag auch später darauf vertrauen. Die Ausweitung der Wahrnehmungs- und Handlungsspielräume im Zusammenhang mit Konflikten erleichtert es, Gewaltandrohung, Gewaltausübung und damit auch den Einsatz militärischer Machtmittel als in aller Regel inadäquate und konfliktsteigernde Mittel zu erkennen.

Doch der Trend weist derzeit einmal mehr in eine andere Richtung: Mit Blick auf den Umbau der Bundeswehr zu einer Truppe für flexible Einsätze in verschiedenen Teilen der Welt wird die Öffentlichkeitsarbeit pro Militäreinsätze und pro Bundeswehr auch im schulischen Bereich intensiviert. Neben die Frage der gesellschaftlichen Wahrnehmung ihrer Einsätze tritt – vor dem Hintergrund der Aussetzung der Wehrpflicht – für die Truppe die existentielle Notwendigkeit, geeigneten Nachwuchs zu werben.

#### Bundeswehrpräsenz in Schulen und auf Bildungsmessen

Aus verschiedenen Bundesländern sind Vereinbarungen der Bundeswehr mit Kultusministerien bekannt, die u.a. die Arbeit von Jugendoffizieren in den Schulen verbessern sollen. In anderen Bundesländern entscheiden die einzelnen Schulleitungen über mögliche Kooperationen. Eine aktuelle Dokumentation zum Thema *Bundeswehr und Schule* hat *terre des hommes* in Kooperation mit der *Gewerkschaft Erziehung und Wissenschaft* herausgegeben (tdh/GEW 2011). Im einleitenden Beitrag von Willinger heißt es darin u.a.:

> *„Besonders an Schulen versucht die Bundeswehr, ihr Image aufzubessern und Nachwuchs zu werben. 2010 erreichten alleine die Jugendoffiziere und Wehrdienstberater der Bundeswehr 340.000 Schüler, darunter auch Kinder von elf Jahren. (...)*
> *Bei ihren Schulbesuchen gibt es kaum Informationen über Risiken der Auslandseinsätze und getötete, verletzte oder traumatisierte Bundeswehrsoldaten sowie über die Gefahren der Konflikteskalation durch den Einsatz von Gewalt. Ebenso wenig kommen Themen wie Gewaltfreiheit und zivile Konfliktlösung zur Sprache. Stattdessen wird die Notwendigkeit militärischer Inter-*



*ventionen betont und ein heroisches, verharmlosendes Bild solcher Einsätze gezeichnet. Auch Computer- oder Strategiespiele der Bundeswehr wie ‚Politik & Internationale Sicherheit' werden systematisch genutzt, um den Einsatz militärischer Gewalt bis hin zur Atombombe zu legitimieren. Jugendoffiziere spielten alleine 2010 mit über 24.000 Schülern und Lehrern dieses Spiel."*
*(Willinger 2011, S. 22)*

Inzwischen manifestiert sich – getragen von Schüler/innen, Eltern, Lehrer/innen und Öffentlichkeit – immer öfter Widerstand gegen derartige Bundeswehr-Werbeoffensiven. Ziel ist es, entweder gar keine Soldaten einzuladen, oder nur in Kontexten, in denen kontrovers diskutiert wird.

Auch die *Gewerkschaft Erziehung und Wissenschaft* kritisiert scharf die Präsenz der Bundeswehr an Schulen und hat in einem Beschluss ihres Hauptvorstandes am 31.3.2011 u.a. festgehalten:

*„Die GEW wendet sich entschieden gegen den zunehmenden Einfluss der Bundeswehr auf die inhaltliche Gestaltung des Unterrichts und der Lehreraus- und Fortbildung, wie sie in den Kooperationsabkommen zwischen Kultusministerien und Bundeswehr deutlich werden. Die politische Bildung – auch in Fragen der Sicherheitspolitik – gehört in die Hand der dafür ausgebildeten pädagogischen Fachleute und nicht in die von Jugendoffizieren. Die GEW fordert die Landesregierungen auf, entsprechende Passagen in den Kooperationsabkommen zu kündigen."*
*(Link zum gesamten Beschlusstext siehe Kasten)*

Im Internet finden sich inzwischen viele Seiten, die sich kritisch mit den Aktivitäten der Bundeswehr an Schulen auseinandersetzen. Als Einstieg seien u.a. empfohlen:

GEW
*http://www.gew.de/Einfluss_der_Bundeswehr_an_Schulen_zurueckdraengen.html*

Junge GEW
*http://www.jungegew.de/index.php/schule-ohne-bundeswehr.html*

DFG/VK
*http://www.dfg-vk.de/thematisches/schulfrei-fuer-die-bundeswehr/*

IMI-Studie: Die Eroberung der Schulen
*http://imi-online.de/download/MSG_Jugendoffiziere_Studie.pdf*

Neben Veranstaltungen direkt in Schulen zeigt die Bundeswehr aktuell v.a. bei Bildungsmessen mit großen Ständen, viel Personal und Fuhrpark Präsenz und versucht Schülerinnen und Schüler, die auf der Suche nach Ausbildungsplätzen sind oder vor einer Entscheidung für ein Studium stehen, für Ausbildung und Karriere bei der Bundeswehr zu begeistern. Selbstverständlich nutzt die Bundeswehr auch Medien aller Art für die gezielte Ansprache von Jugendlichen, u.a. betreibt sie ein Community-Portal mit Namen *treff.bundeswehr.de* (Slogan: „... mehr erleben!"), wirbt für die Teilnahme an den *Bundeswehr Adventure Games* (Slogan: „Abenteuer pur") und ist selbstverständlich auch in Facebook präsent.

In ihrer vor kurzem fertiggestellten Bachelor-Arbeit hat Lena Sachs in dankenswerter Weise die Rolle der Bundeswehr an Schulen historisch und vor allem bezogen auf die gegenwärtige Debatte aufgearbeitet. Insbesondere kritisiert sie, *„dass die Bedingungen, welche der Bundeswehr die Türen zu den Schulen öffnen und durch welche die Zusammenarbeit gerechtfertigt wird, nicht eingehalten werden können. Wie auch die Analyse der Unterrichtsmaterialen zeigte, sind weder das Verbot von Nachwuchswerbung, noch die Grundsätze der politischen Bildung durch den Einbezug Bundeswehr in die Schulbildung gewährleistet"* (Sachs 2011, S. 78). Vernichtend klingt ihre Analyse der kulturell negativen Wirkung derartiger Zusammenarbeit von Bundeswehr und Bildungseinrichtungen: *„Mittels der Veralltäglichung militärischer Gewalt wird der Grundstein für die Akzeptanz des Einsetzens militärischer Mittel oder militärischer Aufrüstung in der Bevölkerung gelegt"* (S. 78).

### Erziehung zur Friedensfähigkeit

Der Widerstand gegen Militärwerbung und einseitige Informationskampagnen ist notwendig und muss weitergehen. Das alleine reicht jedoch nicht aus. Ebenso wenig würde in der heutigen Gesellschaft aber auch eine Schonraum-Bewahrpädagogik oder eine ausschließlich am Ideal einer gewaltfreien Gesellschaft orientierte Bildung sinnvoll funktionieren. Beides würde den Kindern und Jugendlichen den Blick auf die Realität und Schwierigkeiten der heutigen Welt verstellen oder verkleistern, was ihnen gegenüber in keiner Weise verantwortbar wäre.

*„Kriege als historisch, d.h. als vom Menschen herbeigeführt und deshalb als vermeidbar begreifen zu lernen"* ist das erstes Lernziel friedensorientierter Bildung (Nicklas 1996, S. 469). Friedensorientierte Bildung muss sich selbst verstehen *„als Teil des Prozesses, dessen Ziel der Abbau oder die Verringerung von Gewalt ist"* (S. 463). Dazu muss sie auf allen Stufen organisierter Lernprozesse zur Reflexion gesellschaftlicher Zusammenhänge auffordern sowie kritisches Selbstverständnis und konkrete Handlungsfähigkeit fördern. In diesem Sinne trägt Erziehung zur Friedensfähigkeit gleichermaßen zu einem *„Selbstbefreiungsprozess des Menschen"* (S. 471) bei.

## Wissenschaft in Verantwortung für Frieden

*„Ich möchte an alle eine allgemeine Mahnung richten: dass sie berücksichtigen, welches der wahre Zweck des Wissens ist und dass sie weder zum geistigen Vergnügen noch um des Streitens willen danach streben, sondern um des Wohls und des Nutzens für das Leben Willen, dass Hilfe für die Menschen daraus entstehen möge und Erfindungen, die in einem gewissen Maße die Not und das Elend der Menschheit mildern und überwinden können."*
*(Francis Bacon; zit. n. Rotblat 2009)*

### Impulse aus Pugwash und Göttingen

Unter dem Eindruck der Atombombenabwürfe auf Japan und des anschließenden nuklearen Wettrüstens zwischen den USA und der Sowjetunion formulierte der Mathematiker und Philosoph Bertrand Russell ein noch von Albert Einstein und acht weiteren namhaften Wissenschaftlern mitunterzeichnetes Manifest, in dem vor den Gefahren des Krieges mit Nuklearwaffen gewarnt und die bewusste Entscheidung gegen bewaffnete Konflikte gefordert wurde. U.a. heißt es darin:

> *„(...) In the tragic situation which confronts humanity, we feel that scientists should assemble in conference to appraise the perils that have arisen as a result of the development of weapons of mass destruction, and to discuss a resolution in the spirit of the appended draft. (...)"*
> *(The Russell-Einstein-Manifesto 1955)*

In der Folge kam es 1957 in Pugwash, einem kleinen Fischerdorf in Nova Scotia/Canada zu einem ersten Zusammentreffen von 22 hochrangigen Wissenschaftlern aus zehn Nationen. Der Name *Pugwash Conferences on Science and World Affairs* blieb, auch wenn spätere Zusammenkünfte an vielen verschiedenen Orten stattfanden. Das *Russell-Einstein-Manifest* war ein frühes Signal dafür, dass Wissenschaftlerinnen und Wissenschaftler sich zu ihrer gesellschaftlichen Verantwortung bekennen und in dieser Konsequenz auch politisch Position beziehen müssen.

Über dieses erste Pugwash-Treffen 1957 schrieb der Mitbegründer und langjährige Präsident der *Pugwash Conferences* Józef Rotblat 1996: *„Es ist schwierig, sich das Klima aus Misstrauen und Angst vorzustellen, das zu dieser Zeit herrschte. Es erforderte ein hohes Maß an Zivilcourage zu kommen. Jeder im Westen, der zu solch einem Treffen kam, der über Frieden mit den Russen sprach, wurde als ein Kommunisten-Tölpel angesehen"* (Übersetzung G. Neuneck 2009, S. 378).

1995 erhielten die *Pugwash Conferences* und Józef Rotblat den Friedensnobelpreis. Bei der Verleihung kritisierte Rotblat den immer noch bestehenden Glauben an Wertfreiheit und Neutralität der Wissenschaft:

> *„(...) You are doing fundamental work, pushing forward the frontiers of knowledge, but often you do it without giving much thought to the impact of your work on society. Precepts such as »science is neutral« or »science has nothing to do with politics« still prevail. They are remnants of the ivory tower mentality, although the ivory tower was finally demolished by the Hiroshima bomb. (...)"*
> *(Rotblat 1995)*

In seiner Rede kritisierte er nicht nur die Wissenschaftler, die durch ihre Arbeiten dem Rüstungswettlauf im Kontext von Nuklearwaffen und Kaltem Krieg Vorschub leisteten. Rotblat stellte dabei auch den Bezug zur Gegenwart her. In unterschiedlichen Forschungsfeldern könne es zu negativen gesellschaftlichen Folgen kommen, deswegen seien stete Wachsamkeit gefragt und die Bereitschaft bzw. Verpflichtung, ggf. kritische Entwicklungen auch an die Öffentlichkeit zu bringen:

> *„(...) But there are other areas of scientific research that may directly or indirectly lead to harm to society. This calls for constant vigilance. The purpose of some governmental or industrial research is sometimes concealed, and misleading information is presented to the public. It should be the duty of scientists to expose such malfeasance. 'Whistle-blowing' should become part of the scientist's ethos. This may bring reprisals; a price to be paid for one's convictions. (...)"*
> *(Rotblat 1995)*

In Deutschland wurde am 12. April 1957 von 18 Atomwissenschaftlern die sogenannte *Göttinger Erklärung* herausgegeben, in der sie ihre tiefe Sorge hinsichtlich der Pläne einer atomaren Bewaffnung der Bundeswehr artikulierten. In der (richtigen) Erwartung, dass ihre Erklärung die Frage aufwerfen würde, mit welcher Berechtigung sich Wissenschaftler zu dieser politischen Frage äußerten, schrieben sie in der Erklärung:

> *„(...) Wir wissen, wie schwer es ist, aus diesen Tatsachen die politischen Konsequenzen zu ziehen. Uns als Nichtpolitikern wird man die Berechtigung dazu abstreiten wollen; unsere Tätigkeit, die der reinen Wissenschaft und ihrer Anwendung gilt und bei der wir viele junge Menschen unserem Gebiet zuführen, belädt uns aber mit einer Verantwortung für die möglichen Folgen dieser Tätigkeit. Deshalb können wir nicht zu allen politischen Fragen schweigen. (...)"*
> *(zit. n. Albrecht et al. 2009, S. 15).*

Obgleich die *Göttinger Erklärung* keine ethischen Überlegungen als Argumente heranzieht, wurde die Erklärung im Nachgang dennoch v.a. als „Aufstand des Gewissens" apostrophiert, der insb. durch die Selbstverpflichtung der Wissenschaftler über ein bloßes Manifest hinausging (vgl. Stölken-Fitschen 2009, S. 87).

### Verantwortung für den Frieden auch jenseits des Atomkrieges

> *„Ganz unabhängig von den Debatten über Nuklearwaffen halte ich es für das Wichtigste, dass man den Krieg als Ultima Ratio ächtet. Es ist keine Ultima Ratio, und zwar nicht nur, weil der Krieg die Falschen trifft, sondern weil er auch das Problem nicht löst. Krieg kann kein Instrument zum Durchsetzen von Interessen sein – ich frage mich, warum man nicht beginnt, Russell-Einstein in diesem Punkt ernst zu nehmen."*
> *(Hans-Peter Dürr; zit. n. Albrecht et al. 2009, S. 354)*

Bei der heutigen Diskussion über die Verantwortung von Wissenschaftlerinnen und Wissenschaftlern und über die Frage von Zivilklauseln an Hochschulen und Forschungszentren hat die Frage des Nuklearkrieges meist nur noch eine Randbedeutung. Dennoch lässt sich aus diesen historischen Beispielen vieles herleiten. Zentral sind insbesondere das Heraustreten aus dem Elfenbeinturm und die damit verbundene Übernahme gesellschaftlicher Verantwortung.

Seit dem *Russell-Einstein-Manifest* und der *Göttinger Erklärung* haben viele Wissenschaftlerinnen und Wissenschaftler für sich individuelle Entscheidungen getroffen und beschlossen,

die ein oder andere Forschungsfrage nicht anzugehen oder bestimmte Projekte nicht durchzuführen. Das Spektrum der angeführten Argumente reicht dabei weit über politische Erwägungen hinaus: Beispielsweise begründete David L. Parnas 1985 seinen Rücktritt aus einem Beratergremium zum SDI-Projekt[3] des amerikanischen Präsidenten Ronald Reagan nicht politisch, sondern er bezog sich auf seine Kompetenz im Bereich der Software-Technik und seine diesbezüglichen Zweifel an einer verantwortbaren Funktionsfähigkeit des geplanten Systems (Parnas 2009, S. 8). Weitere Beispiele – auch aus dem Bereich der Informatik: Benjamin Kuipers veröffentlichte 2003 ein Positionspapier, in dem er begründet, warum er keine Fördermittel vom Militär annimmt (Kuipers 2003) – auch um deutlich zu machen, dass man trotz einer derartigen Entscheidung eine erfolgreiche Karriere haben kann. Bereits 1984 hatte Terry Winograd mit seinem kleinen, im CPSR-Newsletter[4] erschienenen Aufsatz „Some thoughts on military funding" einige wesentliche Gedanken publiziert:

> *„Wenn sich ein Einzelner weigert, militärische Fördergelder anzunehmen, ist das ein ‚symbolischer Akt' oder etwas, was eine erkennbare politische Wirkung hat? In den letzten Jahren habe ich es vermieden, mich um militärische Förderung zu bemühen, aber insofern ich das privat getan habe, bin ich einer größeren Verantwortung, andere zu beeinflussen, aus dem Wege gegangen.*
> *(...)*
> *Der Punkt ist zu fragen, was wir alle zusammen tun und was wir statt dessen tun könnten; dann können wir nach Wegen suchen, wie ein Einzelner Veränderungen bewirken kann."*
> *(Winograd 1985, S. 169)*

Einzelne Wissenschaftlerinnen und Wissenschaftler können also – ganz im Sinne des bekannten Textes von Wolfgang Borchert[5] „NEIN" sagen – und damit ganz individuell für sich Verantwortung zeigen. Wie wäre es also, Wissenschaftlerinnen und Wissenschaftler diesbezüglich in die Pflicht zu nehmen? Rotblat thematisierte dies in seiner Abschlussrede zur 44. *Pugwash-Konferenz* 1994 und sprach über die Schwierigkeit, so etwas wie einen Hippokratischen Eid für die Wissenschaft zu formulieren, ohne dass dies mehr als einen symbolischen Wert hätte. Er hielt es für *„extrem schwierig, eine Formulierung zu finden, die für eine Mehrheit in der wissenschaftlichen Gemeinschaft sowohl bedeutsam als auch akzeptabel wäre"*. Er versprach sich hingegen sehr viel davon, den sozialen Einfluss und die ethischen Folgen wissenschaftlicher Arbeit in die Lehrpläne der Universitäten aufzunehmen (Rotblat 2009, S. 395f) – eine Forderung, die auch heute weiterhin mit Nachdruck vertreten werden muss!

Doch selbst wenn ein übergreifender Eid für alle Wissenschaftlerinnen und Wissenschaftler utopisch erscheinen mag, stellt sich die Frage, ob nicht über individuelle Entscheidungen hinaus zumindest Institutionen als substanzielle Teile gesellschaftlicher Strukturen in vergleichbarer Weise Zeichen setzen können und sollten – auch und gerade mit Blick auf die gesellschaftlich-kulturelle Wirkung solcher Beschlüsse.[6]

Vor diesem Hintergrund ist die aktuelle Diskussion um Zivilklauseln an Universitäten, Fachhochschulen und Forschungseinrichtungen ausgesprochen spannend. Ziel ist, an weiteren Institutionen derartige Beschlüsse zu implementieren. Gleichzeitig – so scheint es – hat die oben skizzierte *neue Weltordnung* nun diejenigen Einrichtungen erreicht, welche tatsächlich bereits Beschlüsse in dieser Richtung hatten, mit der Konsequenz, dass diese in Frage gestellt werden.

Als Argument dafür, dass derartige Zivilklauseln „nicht mehr zeitgemäß" seien, wird zum einen die veränderte weltpolitische Lage angeführt. So wird die Notwendigkeit militärischer Stärke zur Unterstützung humanitärer Einsätze als Argument herangezogen – es gehe ja nicht mehr darum, im Sinne des Wettrüstens Bedrohungspotential aufzubauen, vielmehr seien „friedenssichernde und friedensschaffende Maßnahmen" Ziel der Militäreinsätze. Wirkliche Belege für nachhaltige Erfolge derartiger Maßnahmen gibt es jedoch nicht – diese bleiben Postulate. Im Gegenteil: An vielen Orten, an denen in den letzten Jahren Militär mit entsprechenden Begründungen eingegriffen hat, ist dieses weiterhin zur notwendigen Stabilisierung im Einsatz – oder es wurden nach dem Abzug instabile Verhältnisse hinterlassen, in denen sich dann neue Machtstrukturen durch mehr oder weniger offene oder strukturelle Gewalt festigen.

Ein zweites, oft angeführtes Argument gegen Zivilklauseln und ähnliche als Einschränkung der Wissenschaftsfreiheit[7] interpretierte Regelungen, ist die Schwierigkeit ihrer Operationalisierung: Wer will wie festlegen, ob etwas militärische oder zivile Forschung ist, insb. wenn Erkenntnisse und Entwicklungen in

**Ralf E. Streibl**

**Ralf E. Streibl** ist Diplom-Psychologe und arbeitet als wissenschaftlicher Mitarbeiter an der Universität Bremen im Fachbereich 3 (Mathematik/Informatik). Seit 1993 Lehrtätigkeit an der Universität Bremen (Schwerpunkt u.a. „Informatik und Gesellschaft"), dazu seit 2000 Tätigkeit im Studienzentrum Informatik.

Er ist Mitglied der Gewerkschaft Erziehung und Wissenschaft (GEW) und derzeit Sprecher der GEW-Gruppe an der Universität Bremen, ferner Mitglied im Forum Friedenspsychologie (FFP) sowie im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF).

beiden Bereichen gleichermaßen wirksam werden (Dual-Use-Fähigkeit). Zugegebenermaßen gibt es viele dieser Grenzbereiche, somit wachsen die „zivil-militärischen Grauzonen", wie Liebert anschaulich beschreibt: *„Was früher noch eindeutig »schwarz« erschien und nur militärischen Interessen dienlich war, hat auch Einzug in zivile Zusammenhänge gehalten. Umgekehrt werden ehemals für ‚weiß' gehaltene Forschungsbereiche mit dem (oft unzutreffenden) Argument, ökonomisch günstiger auch militärische Zielvorgaben erfüllen zu können, in die Grauzone hineingeführt"* (2009, S. 445). Würde dadurch eine Zivilklausel nicht obsolet?

Ganz im Gegenteil: Gerade vor dem Hintergrund der geschilderten Problematik und Notwendigkeit des Umgangs mit Ambivalenz in der Forschung gewinnen diesbezügliche Leitziele von Forschungseinrichtungen[8] und institutionelle Zivilklauseln als klare Bekenntnisse und Rahmen zunehmend an Bedeutung. Nicht alles ist im Vorhinein endgültig beantwort- und entscheidbar, jedoch nimmt gerade dies die Wissenschaftlerinnen und Wissenschaftler in die Pflicht, hinsichtlich ihrer Forschungen und Entwicklungen frühzeitig mit einer Analyse zu beginnen, *„die Fragen stellt nach Intentionen, wissenschaftlich-technischen Potentialen, normativen Rand- und Vorbedingungen, ambivalenten Entwicklungslinien, gewollten Wirkungen, nicht-intendierten Folgen und sichtbaren Entwicklungsrisiken"* (Liebert 2009, S. 448). Die Existenz von Zivilklauseln fordern alle Beteiligten in Forschung und Lehre dazu auf, sich selbst und anderen in der Institution entsprechende Fragen zu stellen und in einen stetigen und öffentlichen Diskurs zu treten.

In der Erklärung der bundesweiten Initiative *Hochschule für den Frieden – ja zur Zivilklausel* vom Mai 2011, die von einer ganzen Reihe von Organisationen und Vereinigungen mit getragen wird, heißt es: *„Wir wollen sinnvolle Beiträge zur friedlichen Lösung der Probleme und Konflikte dieser Welt leisten."*

Um echten Frieden zu schaffen, ist Friedensfähigkeit notwendige Voraussetzung – hieran zu arbeiten ist eine große Herausforderung und zentrale Aufgabe für Bildung und Wissenschaft.

Si vis pacem, para pacem.

## Quellen


Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.) (2009): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag.

Boehnke, K.; Christie, D.J.; Anderson, A. (2004): Psychologische Beiträge zu einer Kultur des Friedens. In: Sommer, G.; Fuchs, A. (Hrsg.): Krieg und Frieden. Handbuch der Konflikt- und Friedenspsychologie. Weinheim: Beltz, S.31-43.

Chomsky, N. (1999a): Die neue Weltordnung. Vorlesung, Bates College, Lewiston, Maine, 1991. In: Chomsky, N. et al.: Die neue Weltordnung und der Golfkrieg. Grafenau: trotzdem, S.11-38.

Chomsky, N. (1999b): Desinformation und der Golfkrieg. In: Chomsky, N. et al.: Die neue Weltordnung und der Golfkrieg. Grafenau: trotzdem, S.100-122.

Denninger, E. (2009): Zur Zulässigkeit einer so genannten „Zivilklausel" im Errichtungsgesetz für das geplante Karlsruher Institut für Technologie (KIT). Gutachten im Auftrag der Hans-Böckler-Stiftung. http://www.boeckler.de/pdf/mbf_gutachten_denninger_2009.pdf

Fuchs, A. (2004): Vom »neuen Denken« zur »neuen Weltordnung«. In: Sommer, G.; Fuchs, A. (Hrsg.): Krieg und Frieden. Handbuch der Konflikt- und Friedenspsychologie. Weinheim: Beltz, S.237-249.

Galtung, J. (1990): Cultural Violence. In: Journal of Peace Research, 27 (3), pp.291-305.

Galtung, J. (1998): Frieden mit friedlichen Mitteln. Friede und Konflikt, Entwicklung und Kultur. Opladen: Leske + Budrich.

Hochschulen für den Frieden – ja zur Zivilklausel (2011): Gemeinsame Erklärung „Hochschulen für den Frieden! – Nein zur Kriegsforschung!- Ja zur Zivilklausel!". Braunschweig, 27.5.2011. http://www.asta.tu-bs.de/images/pdf_dokumente/arbeitsgruppen/zivilklausel/Gemeinsame_Erklaerung.pdf

Jäger, S. (2011): Militärische Gewalt. Ihre Normalisierung als Produkt multipler Denormalisierung. In: Wissenschaft und Frieden, 29 (3), S. 6-8.

Kuipers, B. (2003): Why don't I take military funding? http://www.eecs.umich.edu/~kuipers/opinions/no-military-funding.html

Liebert, W. (2009): Umgang mit Dual-Use von Technologien und Ambivalenz in der Forschung. In: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S.445-450.

Meder, G. (1998): Zur Neubestimmung der Rolle der Bundeswehr in den deutschen Printmedien. In: Kempf, W.; Schmidt-Regener, I. (Hrsg.): Krieg, Nationalismus, Rassismus und die Medien. Münster: Lit, S.201-210.

Neuneck, G. (2005): Das Gewissen der Wissenschaft für die Abschaffung der Nuklearwaffen. Nachruf auf Sir Joseph Rotblat. In: Wissenschaft & Frieden, (4).

Neuneck, G. (2009): Die deutsche Pugwash-Geschichte und die Pugwash-Konferenzen. – Ursprünge, Arbeitsweise und Erfolge – Das Ende des Kalten Krieges und die Herausforderungen der Zukunft. In: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S.378-392.

Nicklas, H. (1996): Erziehung zur Friedensfähigkeit. In: Imbusch, P.; Zoll, R. (Hrsg.): Friedens- und Konfliktforschung. Opladen: Leske+Budrich, S.463-480.

Parnas, D.L. (2009): Ein Brief aus dem Jahr 1985. Retrospektive. In: FIfF-Kommunikation, 26 (1), S.7-10.

Rotblat, J. (1995): Remember your Humanity. Rede zur Verleihung des Friedensnobelpreises. http://www.pugwash.org/award/Rotblatnobel.htm

Rotblat, J. (2009): Das vielschichtige soziale Gewissen der Wissenschaftler. Abschlussrede auf der 44. Pugwash-Konferenz 1994 auf Kreta. Abgedruckt in: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S.393-400.

Sachs, L. (2011): Die Zusammenarbeit von Bundeswehr und Bildungseinrichtungen. Eine kritische Analyse. Bachelorarbeit im Studiengang Erziehung und Bildung. Pädagogische Hochschule Freiburg.

Schluroff, M. (1998): Grundlagen der gegenwärtigen deutschen Militärpolitik. In: Kempf, W.; Schmidt-Regener, I. (Hrsg.): Krieg, Nationalismus, Rassismus und die Medien. Münster: Lit, S.195-199.

Stölken-Fitschen, I. (2009): Die Göttinger Erklärung im zeithistorischen westdeutschen und internationalen Kontext. In: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S.81-90.

Tdh/GEW (2011): terre des hommes Deutschland e.V. & Gewerkschaft Erziehung und Wissenschaft (GEW) (Hrsg.): Bundeswehr und Schule. In: „Die Zeitung", 2. Quartal 2011 sowie in „Erziehung und Wissenschaft, 9/2011.

The Russell-Einstein-Manifesto (Issued in London, 9 July 1955). http://www.pugwash.org/about/manifesto.htm

Willinger, R. (2011): Kinder im Visier. Wie die Bundeswehr an Schulen um Nachwuchs wirbt. In: Erziehung und Wissenschaft, (9), S.22.

Winograd, T. (1985): Einige Gedanken zur finanziellen Förderung durch das Militär. In: Bickenbach, J.; Keil-Slawik, R.; Löwe, M.; Wilhelm, R. (Hrsg.): Militarisierte Informatik. Schriftenreihe „Wissenschaft und Frieden", Bd. 4. Marburg/Berlin/Münster: BdWi/FIfF/Natwiss, S.169-173.

(Alle Internetquellen Stand 15.10.2011)

## Anmerkungen

1 *„Wenn Du den Frieden willst, bereite den Krieg vor!"*

2 *„Dual-Use-...": Bezeichnung für Forschungsergebnisse, Güter, Materialien etc., die sowohl militärisch wie auch zivil genutzt werden können.*

3 *Strategic Defense Initiative – ein Projekt der US-Regierung zur Abwehr von Interkontinentalraketen (1983)*

4 *CPSR = Computer Professionals for Social Responsibility*

5 *„(...) Du. Forscher im Laboratorium. Wenn sie dir morgen befehlen, du sollst einen neuen Tod erfinden gegen das alte Leben, dann gibt es nur eins: Sag NEIN ! (...)" – aus Wolfgang Borchert: Dann gibt es nur eins.*

6 *Vgl. auch den internationalen Appell „Commit Universities to Peace – Reject Research for the Military" von INES – International Network of Engineers and Scientists for Global Responsibility: „Freedom of thought and ideas for a peaceful, sustainable and just world are universal human rights. Today, they are threatened in many places, including even the universities around the world. Growing militarization of academic research in not only engineering and natural sciences, but also humanities, is further eroding those rights. Immediate steps need to be taken to reverse this process. The undersigned believe that universities must focus on promoting peace and understanding among peoples by rejecting any research and teaching for military purposes. We call for the abandonment of all research and teaching for military purposes and urge the university authorities and the responsible academic bodies everywhere to adopt binding commitments in the university statutes similar to Civil Clauses in some countries." – Quelle: http://www.inesglobal.com/commit-universities-to-peace.phtml*

7 *Zur verfassungsrechtlichen Verträglichkeit von Zivilklauseln liefert u.a. das Gutachten von Denninger (2009) Einschätzungen.*

8 *Auszug aus den Leitzielen der Universität Bremen: „(...) Lehrende und Lernende der Universität Bremen orientieren sich an den Grundwerten der Demokratie, Menschenrechte und sozialen Gerechtigkeit, die in vielen Bereichen auch Gegenstand von Forschung und Lehre sind. Sie werden sich auch künftig mit den Folgen der Wissenschaft in Wirtschaft, Politik und Kultur und mit den Möglichkeiten einer sozial- und umweltverträglichen Nutzung von Forschungsergebnissen (z. B. vorausschauende Technologie- und Wirtschaftspolitik, keine Rüstungsforschung) befassen. Die gesellschaftliche Verantwortung der Universität beginnt in der Region, d. h. mit dem Engagement für eine zukunftsfähige Entwicklung des Landes Bremen. Sie umfasst auch Fragen der sozialen Gerechtigkeit und Unterentwicklung (Nord-Süd-Gefälle). (...)" Quelle: http://www.uni-bremen.de/universitaet/profil/leitziele.html*

Wie der Schwerpunkt dieser FIfF-Kommunikation exemplarisch belegt, ist die Verknüpfung von Informatik mit Rüstung und Krieg in vielen Facetten erschreckend aktuell. Die Auseinandersetzung mit dieser Thematik hat vor rund dreißig Jahren maßgeblich zur Gründung des FIfF beigetragen, wobei es allerdings anfangs vor allem um die wachsende Gefahr eines Atomkriegs ging. Die folgende Retrospektive erinnert an diese Zeit.


**INFORMATIKER WARNEN VOR DEM PROGRAMMIERTEN ATOMKRIEG**

Bis Ende der 60er Jahre stand die Vergrößerung der Vernichtungskraft der Atomwaffen im Mittelpunkt der politischen und militärischen Überlegungen; heute ist es die Zielgenauigkeit. Mit hohem Aufwand haben Wissenschaftler und Ingenieure Waffensysteme entwickelt, die über große Entfernungen in außerordentlich kurzer Zeit mit hoher Treffsicherheit gegnerische Ziele erreichen. Hierbei spielen Computertechnik und und Mikroelektronik eine entscheidende Rolle. Frühwarnsysteme und Satellitennetze, mobile Führungs-und Kommunikationssysteme ergänzen das Arsenal der elektronischen Kriegsführung.

Aufgrund der zunehmenden Verflechtung von militärischen und zivilen Bereichen werden alle, die in Informatik- und Elektronikbereichen arbeiten, in die Entwicklung solcher Waffensysteme direkt oder indirekt einbezogen und dadurch gezwungen, Stellung zu nehmen. Wie die Göttinger Atomphysiker 1957 öffentlich gegen die atomare Bewaffnung der Bundeswehr eintraten, wenden wir uns heute als Informatiker, Ingenieure und Programmierer an unsere Berufskollegen und an die Öffentlichkeit:

**Mit der Stationierung von Pershing II und Cruise Missile in der Bundesrepublik Deutschland wird ein qualitativ neuer Schritt hin zu einem Computerkrieg getan, durch den die Bundesrepublik niemals verteidigt, wohl aber vernichtet werden kann.**

*Plakat der Friedensinitiative des Fachbereichs Informatik der Technischen Universität Berlin*
*Textausschnitte aus dem Flugbatt zu der Kampagne Informatiker warnen vor dem programmierten Atomkrieg*

**Hans-Jörg Kreowski**



# Informatik und Militär:

# Zusammen in den Abgrund

*Der folgende Artikel ist die schriftliche Fassung eines Vortrags auf dritten FIfF-Jahrestagung 1986 in Berlin, die im Tagungsband abgedruckt ist: Michael Löwe, Gerhard Schmidt und Rudolf Wilhelm (Hrsg.), Umdenken in der Informatik, Verlag für Ausbildung und Studium, VAS in der Elefanten Press, 1987, S. 37-42. Der Text beginnt mit dem Nachspiel.*



## Nachspiel

Die Spannungen zwischen den beiden Supermächten USA und Sowjetunion hatten sich in den letzten Jahren weiter zugespitzt; da unterbricht eines schönen Tages zwischen 1995 und 2005 der NDR sein Programm für folgende Meldung: „Die Bordcomputer von sieben Kampfstationen, die von den Vereinigten Staaten zur Abwehr von Interkontinentalraketen im Weltraum stationiert wurden, registrierten soeben eine Bedrohung ihrer Stationen durch einen noch nicht identifizierten Angreifer. Die lokalen und globalen Schlachtenführungssysteme haben sofort alle erforderlichen Gegenmaßnahmen eingeleitet. Die strategische Atomstreitmacht der USA ist in höchste Alarmbereitschaft versetzt worden. Stehen wir an der Schwelle eines Atomkriegs?“

Zehn Minuten später erfolgt erneut eine Durchsage: „Der Präsident der Vereinigten Staaten Donald McTrouve hat sein Einverständnis für den Einsatz von Atomsprengköpfen erteilt. Als Vergeltung für die versuchte Zerstörung der SDI-Systeme durch die Sowjetunion sind drei Interkontinentalraketen gezündet worden, um strategische Ziele in der weiteren Umgebung von Moskau zu zerstören.“

Die Sowjetunion reagiert mit einem ähnlichen Schlag, bei dem sie U-Boot-gestützte Raketen einsetzt, ehe sich der vermeintliche Angriff auf die SDI-Kampfstationen als ein Irrtum erweist und die Kampfhandlungen nach einem Gespräch über das Rote Telefon von beiden Seiten eingestellt werden. Nach drei Tagen zieht die Pressesprecherin des Weißen Hauses Lorry Unspeaks eine erste Bilanz und erhellt die Hintergründe dieses tragischen Vorfalls: „Am Morgen des fraglichen Tages haben Techniker einen Test durchgeführt, mit dem die Funktionsfähigkeit der elektrischen Systeme der Kampfstationen überprüft werden sollte. Dabei wurden die Energie zuführenden Systeme über Funk teilweise abgeschaltet, was die Bordcomputer wegen eines Entwurfs- und Programmierfehlers fälschlich als Bedrohung der Stationen deuteten, so dass sie Alarm schlugen. Da ein Angriff durch die Sowjetunion wegen ihres vorausgegangenen aggressiven Verhaltens im Nahen und Mittleren Osten als wahrscheinlich galt und der Fehler nicht rechtzeitig entdeckt werden konnte, entschloss sich der Präsident zu einem Gegenschlag, um die Verteidigungsfähigkeit der USA nicht einzubüßen. Als sich wenige Minuten später der verhängnisvolle Irrtum herausgestellt hatte, versuchte der Präsident über das Rote Telefon weitere Kampfhandlungen zu vermeiden. Das konnte jedoch nicht mehr verhindern, dass atomar bestückte Raketen, die von sowjetischen Unterseebooten aus gestartet worden waren, amerikanisches Territorium erreichten.

In der Sowjetunion sind bei diesem bedauerlichen Zwischenfall mehrere Raketensilos und eine Kommandozentrale zerstört worden. 114 Techniker und Wachsoldaten fanden den Tod. Ihren Angehörigen hat der Präsident sein Beileid ausgesprochen und materielle Unterstützung zugesichert. Bei dem Generalsekretär der KPdSU hat sich der Präsident formell entschuldigt und die Wiedergutmachung des Schadens angekündigt. Die sowjetischen Raketen haben ihre programmierten Ziele in Industriegebieten um Hunderte von Meilen verfehlt und sind in unwegsamen, dünn besiedelten Wüstengebieten explodiert. Bisher wurden 317 Tote gezählt und mehrere tausend Verletzte, von denen allerdings die meisten nach ambulanter Behandlung die Krankenhäuser verlassen konnten. Der eingesetzte Untersuchungsausschuss arbeitet fieberhaft, um die Hintergründe und Ursachen dieser Katastrophe aufzudecken.“

Die 1000seitige Studie, die einige Monate später die Ergebnisse der Untersuchung zusammenfasst, spricht von einer langen Kette unglücklicher Umstände, das Nichteintreffen nur eines einzigen davon hätte das Unglück vermieden. Die Auswirkungen der Atomexplosionen auf Klima und Nahrungsmittelversorgung hätten sich als überraschend gering erwiesen; die Strahlenbelastung für die Bevölkerung nahe den Explosionsorten sei nicht wesentlich höher als nach dem Reaktorunfall in Tschernobyl im Jahre 1986. Der Ausschuss empfiehlt, in mehreren Konferenzen mit den NATO-Partnern und den Warschauer-Pakt-Staaten Maßnahmen zu beschließen, die künftig menschliches Versagen ausschließen.

### 40 Jahre Computertechnik – Aufgerüstete Informatik

Die Informatik als die Wissenschaft, in der Funktion, Einsatzmöglichkeiten und Grenzen der elektronischen Datenverarbeitung untersucht werden, ist von ihren Anfängen bis heute innig verbunden mit der Rüstung. Die fortschreitende Computerisierung der Militärtechnik in den vergangenen vierzig Jahren ging einher mit einer massiven Einflussnahme von militärischer Seite auf die Entwicklung des Faches Informatik. Das Geld und die Wünsche des Militärs haben immer wieder die Phantasie und Tatkraft von Informatikern und Computerfachleuten angeregt und zu Spitzenleistungen der Informationstechnik getrieben.

Zu den markanten Stationen auf diesem Weg gehören:

(1) die erste vollwertige elektronische Rechenanlage ENIAC, die 1945 fertig gestellt wurde und für die schnelle Berechnung ballistischer Tafeln bestimmt war,

(2) die SAGE-Computer und -Programmierung, die in den 50er Jahren entwickelt wurden und die erste Computer-gestützte Steuerung eines Frühwarn- und Luftabwehrsystems leisteten,

(3) die Etablierung des Fachgebiets Softwaretechnik in den 70er Jahren, mit dessen Hilfe die „Softwarekrise", d. h. das Problem zu teurer und im Ergebnis nicht ausreichend zuverlässiger Programmerstellung im militärischen Kontext, bewältigt werden sollte,

(4) die Programmiersprache ADA, die von vielen hundert Wissenschaftlern in mehrjähriger Arbeit und über mehrere Stationen hinweg definiert wurde und als Standardsprache für militärische und kommerzielle Anwendungen im NATO-Bereich gedacht ist, und

(5) die insgesamt milliardenschweren Förderungsprogramme des US-amerikanischen Verteidigungsministeriums in den 80er Jahren wie VHSIC (Very High Speed Integrated Circuits), STARS (Software Technology for Adaptable, Reliable Systems) und SCI (Strategic Computing Initiative):

   (a) VHSIC soll zu größeren, schnelleren, zuverlässigeren, strahlenunempfindlichen Chips führen, wie sie ausschließlich bei militärischen Anwendungen und insbesondere bei der Automatisierung nuklearer Kriege gebraucht werden;

   (b) STARS soll endlich den eklatanten Engpass bei der Erstellung militärische Software beseitigen;

   (c) und SCI ist ein groß angelegter Versuch, die Künstliche Intelligenz für militärische Anwendungen vor allem bei der Konzeption zukünftiger konventioneller Kriege auszubeuten.

(6) Was mit ADA, VHSIC, STARS und SCI begonnen wurde, findet seine massive, heillose Fortsetzung in SDI (Strategic Defence Initiative), womit sich die USA auf den „Krieg der Sterne" vorbereiten wollen.

Literatur zu diesem Abschnitt: In [3, 6,12,15-18] wird die Verflechtung von Militär und Informatik im Überblick dargestellt, in [1,5,9,10,23] werden einzelne Aspekte genauer behandelt.

### SDI + Informatik = SDInformatik

Das SDI-Programm garantiert, dass die Aufrüstung in und mit der Informatik weitergeht. Als US-Präsident Reagon 1983 in seiner „Star Wars"-Rede die Wissenschaftler aufrief, Mittel und Wege zu finden, die Nuklearwaffen wirkungslos machen, richtete sich dieser Appell insbesondere auch an Informatiker. Software – man spricht von fast unglaublichen 10 Millionen Zeilen Programmcode – muss entwickelt werden, die automatisch alle Sensoren und Kampfstationen des SDI-Systems kontrolliert und ihren Einsatz koordiniert. Die SDI-Computerprogramme müssen im Ernstfall Tausende von Raketenstarts registrieren, ein Vielfaches an Nuklearsprengköpfen erkennen, verfolgen, von Attrappen unterscheiden und die erforderlichen Befehle zu ihrer Zerstörung geben. Das SDI-Programmsystem wird jedoch nicht nur im Umfang alle Rekorde sprengen, sondern müsste auch diverse bisher ungelöste algorithmische Probleme bewältigen und so zuverlässig und fehlerfrei arbeiten, wie es nach heutiger Kenntnis von Softwareerstellung für unmöglich gehalten wird.

Es gibt deshalb längst warnende Stimmen, aber sie werden nicht verhindern können, dass Dutzende von Forscherteams Teile der SDI-Software entwickeln und für vielversprechend erachtet werden, dass auf Tagungen und in Zeitschriften der Informatik Aspekte von SDI aufgegriffen und behandelt werden. Wenn schon nicht die Informatik insgesamt so umgedeutet wird, dass die Hardware- und Software-Probleme bei der Realisierung von SDI als Hauptaufgabe des Faches erscheinen, so wird zumindest ein neues Fachgebiet entstehen, werden sich Hunderte, ja Tausende von Informatikern durch die Thematik und die zu erwartende großzügige Mittelvergabe herausgefordert fühlen.

Literatur zu diesem Abschnitt: Informationen zu SDI findet man in [7, 8,19-21,26] und weitere, insbesondere kritische Stimmen dazu in [2,4,22,24,25].

### „Zivilitärische Informatik"

Forschungs- und Entwicklungsprojekte, die im militärischen Auftrag und direkt für die Rüstung arbeiten, haben einen eher kleinen Anteil an der Informatik. Das bedeutet jedoch nicht, dass der große Rest eine friedliche Alternative darstellt. Im Gegenteil, die Informatik ist gerade auch in ihren scheinbar zivilen Teilen tief vom militärischen Wunschdenken durchdrungen und von dem Umstand bestimmt, dass der Militärbereich der zahlungskräftigste und experimentierfreudigste Kunde für Informationstechnik ist, der alles kauft, wenn es nur die vage Aussicht bietet, für militärische Zwecke tauglich zu sein. Die Informatik verdient das Attribut „zivilitärisch", weil die Grenze zwischen militärischen und zivilen Teilen verwischt ist, weil durch die enorme Sogwirkung des Rüstungsbereichs praktisch jeder erfolgversprechende Ansatz militärisch gewendet wird. Zivile Informatik ist häufig nur eine andere Erscheinungsform von einer Informatik für die Aufrüstung.

Verschiedene Mechanismen bewirken, dass zivile und militärische Informatik sich einander bis zur „zivilitärischen" Unkenntlichkeit angleichen:

- Ursprünglich rein militärische Vorhaben, wie die Programmiersprache ADA oder Rechnernetze mit Pakettechnologie, werden als universell angepriesen, lang und breit diskutiert, auch bei nicht militärischen Aufgaben eingesetzt und büßen so allmählich das Attribut „militärisch" ein. Für den Rüstungsbereich ist das von Vorteil, weil die Methoden und Konzepte eher akzeptiert werden und mehr Fachleute vertraut damit umgehen.

- Eigentlich zivil ausgelegte Projekte, wie die japanische Entwicklung eines Supercomputers oder der Computer der 5. Generation, werden im militärischen Bereich vor allem in der USA kopiert. Die umgekehrte Richtung, die zivile Nachahmung militärischer Vorhaben, scheint sich bei der europäischen Umdeutung von SDI zu EUREKA zu vollziehen. Die Rüstung profitiert von dieser Parallelität, denn wenn die eigenen Entwicklungen scheitern und sich verzögern, können die Ergebnisse der zivilen Projekte gekauft werden. Japaner und Europäer werden sich da kaum verweigern.

- Aktuelle Themen der Informatik wie wissensbasierte Systeme, Robotik, Mustererkennung, Bildverarbeitung, Zu-

verlässigkeit, Nebenläufigkeit, Modularität u. ä. sowie damit zusammenhängende Fragen werden harmlos formuliert und oft ohne existierende oder mögliche Bezüge zu militärischen Problemen und Wünschen diskutiert. Mit großer Sicherheit jedoch werden Durchbrüche der Forschung in dem einen oder anderen Bereich zuallererst militärisch genutzt. Da bei Rüstungsanstrengungen Computertechnik als zentraler Faktor in brisanten und riskanten Situationen eingesetzt wird, lange bevor sie ausgereift ist, besitzt der Militärkomplex nicht nur die größte Kaufkraft, sondern hat zudem den größten Bedarf an technologischem Fortschritt.

Literatur zu diesem Abschnitt: Beispiele und Hinweise auf die Vermengung ziviler und militärischer Informatik können in [6,11,12,26] gefunden werden.

**Menschliches Versagen vorprogrammiert**

Computer machen Fehler. Über Beispiele dafür wird nicht ohne Häme von Zeit zu Zeit in der Tagespresse berichtet. Informatiker wissen, dass praktische Aufgaben mit Hilfe von Computern nicht fehlerfrei bewältigt werden können, dass darüber hinaus das erreichte konzeptionelle und methodische Wissen bei der Erstellung von Rechnerlösungen für Anwendungsprobleme absolut zuverlässige Resultate nicht zulässt. Deshalb gibt es diverse Stimmen, die vor dem Einsatz von Computern warnen, wenn wichtige Interessen auf dem Spiel stehen. Es mag verwundern, dass derartige Mahnungen immer wieder ungehört verhallen. Und doch gibt es dafür einfache Erklärungen.

Die Geschichte der Menschen bildet eine lange Kette fataler Fehler, Irrtümer, Unglücke und Katastrophen. Erdbeben, Überschwemmungen und Vulkanausbrüche verhindern nicht die Besiedlung gefährdeter Gebiete. Krankheit und Krieg werden als unvermeidliche Übel hingenommen. Autos stoßen zusammen, Züge entgleisen, Flugzeuge stürzen ab, Schiffe sinken. Vertrautes Geschehen. Technik fordert ihren Preis und ihre Opfer. Programm- und Computerfehler sind lediglich neue Details bei ansonsten gewohnten Unglücksfällen. Wo Technik allgemein akzeptiert ist oder als unvermeidlich gilt, darf sie sogar versagen, ohne gleich infrage gestellt zu werden.

Technik dagegen, die neu ist, noch nicht akzeptiert, durch politische Entscheidungen noch leicht vermeidbar, deren Preis vielleicht doch zu hoch erscheint, die vielleicht doch zu viele Opfer verlangt, eine solche Technik versagt nie, wenn man ihren Fürsprechern glauben darf. Fehler dieser Technik, die zu Katastrophen führen, beruhen merkwürdigerweise auf menschlichem Versagen, gepaart mit einer Kette unglücklicher Umstände. Der Absturz der Raumfähre Challenger und das Reaktorunglück in Tschernobyl sind zwei Beispiele aus diesem Jahr, wie der versagende Mensch herhalten muss, damit nicht etwa die Technik überdacht werden muss. Zukünftige Fehlfunktionen des SDI-Systems mit fatalen Folgen werden nur andere Nachspiele liefern, die nach demselben Muster ablaufen.

Literatur zu diesem Abschnitt: Fehleranfälligkeit von Militärtechnik vor allem im Zusammenhang mit dabei verwendeter Hardware und Software wird neben anderen Themen in [3,6,12,14,21,22,26] diskutiert.

**Utopie einer abgerüsteten Informatik**

Nach dem Willen vieler Politiker, der Lobby der Rüstungsindustrie und der Militärs ist Informatik zu einer entscheidenden Größe im Rüstungswettlauf geworden. In praktisch keinem modernen Waffensystem fehlt Computertechnik: die Zielsicherheit taktischer wie strategischer Waffen beruht auf programmierter Steuerung. Überwachung und Einsatzplanung auf den Schlachtfeldern der Gegenwert und der Zukunft wird mehr und mehr automatisiert. Die Menschen dürfen in zukünftigen Kriegen auch weiterhin sterben, das Töten besorgen die Computer dank der Fortschritte bei Schaltkreisminiaturisierung, in der Softwaretechnik, bei Kommunikationsnetzen, in der Künstlichen Intelligenz und bei Robotern. Der Einsatz von Informationstechnik beim Drehen der Rüstungsspirale erhöht das Risiko von Kriegen nicht nur, weil damit Kräfteverhältnisse zumindest vorübergehend verschoben werden, sondern auch durch die unabdingbar mit dieser Technologie verbundene Fehleranfälligkeit: Ein Krieg aus Computerversehen droht.

Die Informatik für Militärtechnik zu vereinnahmen, erleichtert das Töten im Krieg und bedroht unser Leben zusätzlich durch Versagen. Informatik für den Krieg ist deshalb nicht verantwortbar, es muss Schluss gemacht werden mit dieser unheilvollen Verknüpfung von Wissenschaft und Tötungsmaschinerie. Der wirksamste und letztlich einzig erfolgversprechende Weg dahin wäre, die wirtschaftlichen und gesellschaftlichen Bedingungen zu beseitigen, die Kriege möglich machen. Bis es soweit ist, lohnt es sich jedoch auch schon, darüber nachzudenken, wie sich die Informatik in ihren Themen und Arbeitsschwerpunkten abrüsten lässt. Wie sieht eine veränderte Informatik aus, deren Resultate nicht länger kriegstauglich sind? Welche neuen Wege münden in eine friedliche Informatik? Wir Informatiker müssen heute beginnen, die Utopie einer abgerüsteten Informatik zu formulieren und auszugestalten.

## Literatur


[1] M.M. Astrahm, J.F. Jacobs: History of the Design of the SAGE Computer – The AN/FSQ-7, IBM Comp. Sci. Research Report RJ3117, San Jose 1981.

[2] G. Ball: The War of Star Wars, The New York Review of Books, 11. April 1985.

[3] F. Barneby: Computer und Militär, in: N Müllert (Hrsg.): Schöne elektronische Welt, Rororo aktuell 4937, Reinbek 1982, S. 146-158.

[4] H.A. Bethe, R.L. Garwin, K. Gottfried, H.W. Kendall: Space-based Ballistic Missile Defense, Scientific American, Vol. 251, No. 4, Oktober 1984, S. 37-47.

[5] J. Bickenbach: Ada oder Das Verlangen – Eine Programmiersprache zwischen höchster Gunst und völliger Ablehnung, in [6], S. 51-62.

[6] J. Bickenbach, R. Kleil-Slawik, M. Löwe, R. Wilhelm (Hrsg.): Militarisierte Informatik, Schriftenreihe Wissenschaft und Frieden Nr. 4, Berlin 1985.

[7] C. Butterwegge, K. Jakubowski, E. Lentz, S. Ziegert (Hrsg.): Weltraumwaffen, VSA Verlag, Hamburg 1985.

[8] E. Deissinger, P. Moosleitner: SDI-Wafffen im Weltraum, P.M. Perspektive Weltraum, 2. April 1986, S. 54-59.

[9] Department of Defense: Software Technology for Adatable, Reliable Systems (STARS) Program Strategy, in: ACM SIGSOFT Software Engineering Notes, Vol. 8, No. 2, April 1983, S. 55 ff.

[10] Department of Defense: Strategic Computing – New Generation Computing Technology: A Strategic Plan for its Development and Application to Critical Problems in Defense, DARPA, Arlington 1983.
[11] R. Franck: Rechnernetze und Datenkommunikation, Springer-Verlag, Berlin-Heidelberg-New York – Tokyo 1986.
[12] R. Franck, J. Gerloff, W. Hardt, R. Isle, H.-J. Kreowski, I. Kuhlmann, K.-P. Löhr, A. Wilharm (Hrsg.): Informatik 2000 – Kampf um Märkte und Vorherrschaft, Informatik-Bericht 5/1987, Universität Bremen.
[13] G. Junne: Das amerikanische Rüstungsprogramm: Ein Substitut für Industriepolitik, Leviathan 1985, Heft 1, S. 23-37.
[14] M. Kaldor: Rüstungsbarock, Rotbuch-Verlag, Berlin 1981.
[15] R. Keil: Die neue Waffe – der Computer, Wechselwirkung Nr. 17 (1983), S. 48-53.
[16] R. Keil-Slawik: von der Feuertafel zum Kampfroboter – Die Entwicklungsgeschichte des Computers, in [6], S. 7-36.
[17] R. Keil, H.-J. Kreowski: Bis dass unser Tod sie scheidet: Atomwaffen und Computer – die Liaison des Jahrhunderts, lehren & lernen – Berufsfeld Elektrotechnik Jahrgang 1, Heft 3 (1984), S. 92-102.
[18] H.-J. Kreowski: Neue Militärtechnik – noch mehr Krieg, in: P. Alheit, J. Kjaer, H.J. Sandkühler (Hrsg.): Kein Frieden der Wissenschaft mit dem Krieg – Materialien der 1. internationalen Friedensuniversität, Universität Bremen 1985, S. 230-236.
[19] H. Lin: Software für Raketenabwehr im Weltraum, Spektrum der Wissenschaft, Februar 1986, S. 30-38.
[20] B. McMillan (Panel Chairman): Battle Management, Communications, and Data Processing (U), Volume V in: J.C. Fletcher (Study Chairman): Report of Study on Eliminating the Theat Posed by Nuclear Ballistic Missiles, Februar 1984, nicht klassifiziert.
[21] K.M. Michel, T. Spengler (Hrsg.): Krieg und Frieden – Streit um SDI, Kursbuch 83, März 1986.
[22] D.L. Parnas: Software Wars. Offener Brief an Mr. M. Offut, Ministerium für Verteidigung, Washington: Kursbuch 83, März 1986, S. 49-60.
[23] F.-M. Reisin: Softwaretechnik oder die Geschichte einer unbewältigten Krise, in [6], S. 37-50.
[24] F.-M. Reisin, R. Wilhelm: Der Wahn als Waffe – Informatik und SDI, unveröffentlichtes Manuskript.
[25] B. Rensberger: Computer Bugs Seen as Fatal Flaw in ‚Star Wars', Washington Post, 30. Oktober 1985, S. A1 und A14.
[26] E. Sköns: SDI und internationale Forschungszusammenarbeit, in: SIPRI-Rüstungsjahrbuch 6, Rororo aktuell 5917, Reinbek 1986, S. 113-143.



# Lesen –
# Neues für den Bücherwurm

**Stefan Hügel**

## Sandro Gaycken – „Cyberwar"

### Das Internet als Kriegsschauplatz

Angriffe auf informationstechnische Infrastrukturen gewinnen an Bedeutung. Die übergreifende Vernetzung durch das Internet macht IT-Infrastrukturen verletzlicher; gleichzeitig stützen sich immer mehr Dienste darauf ab – dadurch steigt unsere Abhängigkeit und damit der Schaden, wenn solche Infrastrukturen geschädigt oder zerstört werden.

Durch Medienberichte wurde uns in der Vergangenheit wiederholt vor Augen geführt, welche Angriffsmöglichkeiten sich selbst für Hacker mit geringem Mitteleinsatz bieten, in Systeme einzudringen. Umso größer sind die potenziellen Schäden, wenn große Organisationen mit entsprechenden Ressourcen – etwa im Rahmen von Militäroperationen – Rechnersysteme angreifen.

Sandro Gaycken, Technik- und Sicherheitsforscher an der FU Berlin, stellt in seiner Untersuchung dar, welche möglichen Bedrohungen sich durch Computerangriffe ergeben. Dabei sieht er vor allem die umfassende Vernetzung als Quelle von Risiken und erwartet, dass diese Vernetzung zum Schutz von Bedrohungen reduziert werden muss und werden wird – nur die „Entnetzung" wird uns aus seiner Sicht dauerhaft schützen.

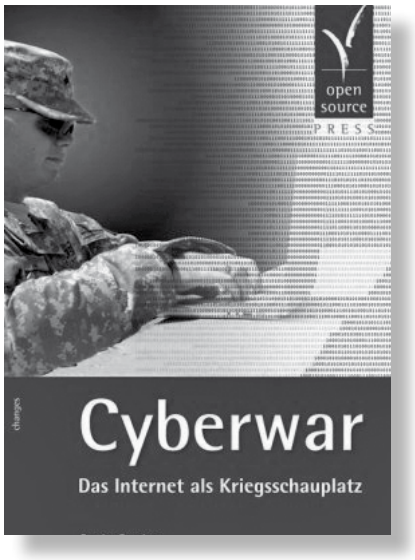
Im ersten Kapitel – Evolution – beschreibt der Autor die Entwicklung der elektronischen Kriegführung – als Cyberwarfare – aus deren strategischen und technischen Erfordernissen. Er stellt fest, dass alle Kriege nach den beiden Weltkriegen vom Prinzip her ebenfalls Weltkriege waren: Es waren immer mehrere Staaten an diesen Kriegen beteiligt; gleichzeitig werden Kriege hochtechnisiert und mit Massenvernichtungswaffen geführt – dem gegenüber stehen Guerilla-Taktiken mit Tarnung und hoher Mobilität bei technisch unterlegenen Gegnern. Für die Bekämpfung solcher mobilen Gegner und zur Steuerung und Kommunikation wird Informationstechnik – C4ISR: Command, Control, Computer, Communication, Intelligence, Surveillance, Reconnaissance – eingesetzt: Wir sind beim Cyberwar.

Das zweite Kapitel – Hacking – gibt einen Überblick über Hacker, die von ihnen genutzten Sicherheitslücken und ihre Techniken. Unterschieden wird zwischen *guten* White-Hat-Hackern, die ohne Schaden anrichten zu wollen, das Eindringen in fremde Rechner als intellektuelle und technische Herausforderung sehen und durch Hinweise auf Sicherheitslücken dazu beitragen, diese zu schließen und die Sicherheit letztendlich zu erhöhen. Sie folgen in der Regel einer eigenen Hacker-Ethik. Black-Hat-Hacker dagegen dringen in Rechnersysteme ein, um dort Schaden anzurichten – das System selbst zu manipulieren oder sich Vorteile zu verschaffen. Prinzipien des Hacking, Sicherheitslücken in Rechnersystemen und Reverse Engineering als Technik zum Entdecken von Zero-Day-Exploits werden beschrieben. In einem Anhang werden Strukturen und Prozesse des Hacking noch detaillierter behandelt, dabei geht der Autor auf Footprinting, Exploitation, Malware und Social Engineering ein.

Im dritten Kapitel – Strukturen – geht es um die Rahmenbedingungen für Operationen im Cyberspace insgesamt. Sie werden bestimmt durch die Komplexität informationstechnischer Sys-

teme und die daraus resultierende Verwundbarkeit, die Globalität von Rechnernetzen, die weltweite Interkonnektivität und die sich ergebenden Schwierigkeiten für die globale Regulierung. Vernetzung und Interoperabilität führt dazu, dass Angriffe mulitiplikativ geführt werden können – wie im Fall von Bot-Netzen können sie von einem Knoten aus über viele weitere Knoten geführt werden. Angriffe können aber auch unkontrolliert migrieren: Verwenden weitere Knoten dieselbe Technik wie das Angriffsziel können sie ungeplant ebenfalls Opfer des Angriffs werden.

IT-Sicherheit hat zum Ziel, gegen Angriffe auf Rechnersysteme zu schützen. Es zeigt sich aus Sicht des Autors jedoch, dass IT-Sicherheit in der Regel nur Schutz gegen Low- oder Mid-Level-Hacker bieten. Gegen High-Level-Hacker mit speziellen Fähigkeiten, Sicherheitslücken zu finden und Zero-Days zu entwickeln, helfen auch Verfahren der IT-Sicherheit nichts. Gerade bei militärischen Cyber-Angriffen wird man es aber zumeist mit Angreifern zu tun haben, die diese Fähigkeiten besitzen. An dieser Stelle hilft aus Sicht des Autors nur eins: Abkoppeln vom Netz.




Ein wichtiger Aspekt im Zusammenhang mit Cyberwar ist das Problem der Non-Attribution – dem Umstand, dass die Identität und der Ort eines Angreifers häufig nicht nachverfolgt und Identitätsinformationen zusätzlich verschleiert werden können. Im Bereich der Strafverfolgung wird versucht, dieses Problem durch Vorschriften wie der zur Vorratsdatenspeicherung zu lösen – ein Ansatz, der mit der rechtsstaatlichen Unschuldsvermutung und dem Recht auf Privatheit kollidiert. Fähige Angreifer werden stats Wege finden, ihre Attribution zu verschleiern. Auch die Motivation von Angreifern kann häufig nicht erkannt werden (motivationale Non-Attribution). Die Wirksamkeit von Gegenmaßnahmen ist aber häufig von der Motivation des Angreifers abhängig; damit können in solchen Fällen nicht ohne Weiteres geeignete Gegenmaßnahmen abgeleitet werden.

Im vierten Kapitel werden die Ziele von Angreifern behandelt. Dabei geht es zunächst um die Frage der Verwundbarkeit von Informationsgesellschaften, die Ziel eines Angriffs werden können. Angriffe können dabei Informationen gelten: Ziel ist dann, diese Informationen zu erhalten, um aufzuklären oder zu manipulieren, um den Gegner damit zu täuschen. Weiteres Angriffsziel sind Identitäten: die Überwachung von Identitäten zu Erkennung der tatsächlich dahinterstehenden Person oder die unbefugte Erlangung von Identitäten zur missbräuchlichen Verwendung und Verschleierung der eigenen Identität.

Großen Schaden bei einem Gegner kann ein Angreifer durch Attacken auf Infrastrukturen verursachen. Die Ausschaltung kritischer Infrastrukturen wie Strom, Wasser, Transport oder Gesundheitsversorgung kann für den Angegriffenen katastrophale Folgen haben und umgekehrt den Angreifer in eine strategisch günstige Position bringen. Damit ist der Schutz solcher Infrastrukturen von besonderer Bedeutung. Beispiel für einen Angriff auf Infrastrukturen ist Stuxnet, der zielgerichtet Kontrollsysteme kritischer Infrastrukturen angriff.

Im fünften Kapitel geht es um Strategien. Dabei spielen Erkennen und Täuschen, Angriff, Abschreckung und Verteidigung eine Rolle. Strategien bauen in der Regeln nicht auf die gegebene, sondern auf die mögliche Situation auf; es müssen also mögliche Zukunftsszenarien antizipiert werden.

Wichtigstes Element der Cyberwarfare ist die militärische Form des Hackens. Durch Einbruch und Manipulation gegnerischer Rechnerinfrastrukturen kann aufgrund deren universeller Nutzbarkeit eine große Bandbreite an Schäden angerichtet werden.

Erster Schritt ist der Zugriff auf den Rechner. In einfachen Fällen kann der Zugriff oberflächlich sein – bei DoS-Angriffen; meistens wird das Ziel eines Angreifers die Manipulation oder der Diebstahl von Daten sein, oder er schleust Software ein, die im Rechnersystem oder darüber hinaus Schäden verursacht. Neben der Art des Zugriffs müssen auch Zugriffswege auf die Systeme bedacht werden – zum Beispiel von außen über das Internet oder von innerhalb der angegriffenen Organisation, z. B. durch Einsatz im Kampfgebiet. Genutzt werden auch Backdoors, die den unbefugten Zugriff ermöglichen. Der Angegriffene muss sich dagegen durch geeignete Verteidigungsmaßnahmen schützen oder Maßnahmen zur Abschreckung ergreifen.

Das sechste Kapitel – Realitäten – stellt Beispiele für cyber-militärische Operationen dar – Estland, Georgien, die Operation Orchard, Conficker, Stuxnet – und nennt konkrete Planungen und Konzepte aus den USA und China. Zuletzt werden die Kapazitäten und Strukturen des US-Cybercommand beschrieben, soweit sie öffentlich bekannt sind.

Den Abschluss bildet ein Ausblick, der die Zukunft des Cyberwar behandelt. Er lässt keinen Zweifel, dass der Cyberwar kommen wird und heute Kapazitäten dafür aufgebaut werden. Rechtsfragen bilden den folgenden Abschnitt; dabei stellt die Non-Attribution ein großes Problem für die Regulierung dar. Regulieren kann man im Bereich des Schutzes, beispielsweise durch Vorgabe von Schutzanforderungen an die Betreiber kritischer Infrastrukturen. In diesem Zusammenhang spielen auch Haftungsfragen eine Rolle. Auch Freiheitsrechte sind zu berücksichtigen, zu denen Regulierungsmaßnahmen häufig im Konflikt stehen. Hier ist eine Abwägung notwendig.

Zentrale These des Bandes ist die Notwendigkeit zur Entnetzung insbesondere kritischer Systeme, die häufig als ein Rückschritt

gesehen wird. Doch bereits heute sind erste Ansätze zur Entnetzung – beispielsweise in den USA – zu erkennen.

Der Band gibt einen umfassenden Überblick über die verschiedenen Aspekte der Cyberwarfare. Dabei ist er stets sachlich und detailliert – er beschreibt die Sachverhalte ohne den vor allem in der Politik häufig anzutreffenden Alarmismus. Mit seiner These der Entnetzung greift er gleichzeitig in die öffentliche Debatte zur Sicherheit von Rechnernetzen ein – einer These, die sich augenscheinlich gegen die aktuelle Entwicklung stellt.

Sandro Gaycken (2011): Cyberwar. Das Internet als Kriegsschauplatz. München: Open Source Press



**Britta Schinzel**

## Hans-Jörg Kreowski (Hg.) – Informatik und Gesellschaft

### Verflechtungen und Perspektiven


Der Band fasst beispielhaft wichtige Themen aus dem Bereich von Informatik und Gesellschaft zusammen. Sie sind sowohl von InformatikerInnen als auch in interdisziplinärer Perspektive aus den Bereichen Jura, Technikgeschichte, Medienphilosophie und aus der Praxis geschrieben. Dabei sind einige Beiträge sehr allgemein gehalten, wie z. B. Dirk Siefkes' Plädoyer für die von Wolfgang Coy ins Leben gerufene Theorie der Informatik mittels seines Textes über informatische Muster, oder Marie-Theres Tinnefelds Beitrag zum Schutz der Menschenwürde als archimedischem Punkt einer Zivilgesellschaft. Andere wiederum sind sehr spezifisch herausgegriffen, wie Eric Töpfers Untersuchung zur Videoüberwachung, bei der zwar nationale Unterschiede interessant erscheinen, aber der Trend zur angelsächsischen Mammutüberwachung zu beobachten ist, oder Volker Grasmucks Beitrag zu DRM (digital rights management). Es gibt Technik-Historisches, wie Hans Dieter Helliges Untersuchung zur Entwicklung des Internet als Lernprozess, theoretisch Philosophisches wie Bernd Robbens Überlegungen zum Computer als Medium, und auch wieder sehr konkret Praktisches wie Dagmar Boedickers leider nur zu realistische Fallbeispiele zu gröbsten Verstößen gegen den Datenschutz, Rikke Frank Joergensens Darstellung der UNO-Deklarationen zu Human Rights im Zusammenhang mit der Informationsgesellschaft und Hans-Jörg Kreowskis Plädoyer für das FIfF.

Im Folgenden greife ich einige Texte aus dem Band heraus. Nach einer Einleitung durch den Herausgeber legt Arno Rolf zum Thema Informatik und Gesellschaft eine Anforderung an ein breiteres Orientierungswissen (Mittelstraß 2001) in Ergänzung zum inzwischen kanonisierten informatischen Verfügungs- und Expertenwissen vor, das es erlaubt, die Wechselwirkungen zwischen Informatik und Gesellschaft in den Blick zu nehmen und zu systematisieren. Rolf nutzt ein 3-stufiges Schalenmodell, ausgehend vom „soziotechnischen Kern", der in sozialen Kontexten entstandenen Formalisierung, Algorithmisierung und Maschinisierung der Kopfarbeit qua Dekontextualisierung (Coy 1992, Nake, 1992) und ihrer Rekontextualisierung in alten und neuen Zusammenhängen, über die „Mikrokontexte", in denen die mit IT beschäftigten und von ihr betroffenen Akteure sich in Arenen bewegen und handeln, und so reflexiv und rekursiv auf die von IT modulierten Strukturen einwirken, bis schließlich zu den „Makrokontexten", den Organisationen, Wissenschafts- und Innovationsmilieus mit ihren Werten, Traditionen in globalen Zusammenhängen. Aus diesem Modell entwickelt er einen systemtheoretischen Orientierungsrahmen zum Verständnis der globalen Netzwerke mit dem Ziel, InformatikerInnen Orientierung und Gestaltungskompetenz zu ermöglichen.

In ihrem zweiten Beitrag in diesem Band entwickelt Marie-Theres Tinnefeld aus historischen Rechtskulturen den Datenschutz als rechtskulturelle Leistung, sieht ihn jedoch massiv bedroht, nicht nur durch die offene Gesellschaft und aktive Gesetzesüberschreitungen, sondern auch durch die neuen technischen Möglichkeiten sowohl quantitativer als auch qualitativer Natur. Die Informations- und Bilderflut, verbunden mit den Möglichkeiten der Speicherung, Datenintegration, dem Data Mining und Warehousing sowie den Überwachungsmöglichkeiten mittels RFID und Biometrie im Verein mit Videoüberwachung und neuen Möglichkeiten der Integration und Auswertung aller Arten von Daten, erzeugt eine neue informationelle Gewalt, die der gebotenen öffentlichen Informationsaskese zuwider läuft und Rechtsgüter bedroht. Tinnefeld plädiert daher für eine dialogische Kultur zwischen Bürgern, Staat und Unternehmen, um grundlegende Datenschutzrechte trotz der Wünsche nach mehr Kontrolle im Interesse der Inneren Sicherheit aufrecht zu erhalten (Anmerkung der Rezensentin: Einer Sicherheit, die wie bekannt durch den Überwachungsstaat nicht erfüllt wird, sondern vielmehr der Kontrolle aller Bürger dient).

Volker Grassmuck höchst spannender Beitrag zur Erfindung des DRM (digital rights management) beschreibt ausführlich, wie mittels DRM eine Lösung gefunden wurde, um aus den eigentlich kostenlosen elektronischen Kopien im Internet enorme und unterschiedlich gestufte Gewinne zu ziehen. Doch das ist nicht das einzige Paradox, mit dem die Rechteinhaber kämpfen müssen, das nächste ist die Tatsache, dass etwas, was beliebig verfügbar ist, verknappt werden muss, also Zugang ermöglicht werden muss, anstatt ihn – wie für die Preissteigerung nötig – zu verhindern. Grassmuck zeichnet die Überlegungen und Entscheidungen der Verwertungsgesellschaften und ihrer Akteure akribisch nach, zitiert, welche geschäftspolitischen

Überlegungen und negativen Annahmen über InternetnutzerInnen, nämlich die, dass sie sämtlich unehrlich seien, die Akteure der Verwertungsgesellschaften zur Erfindung der so genannten „trusted systems“ geführt haben. Er zeigt auf, welche negativen Wirkungen die bisher entwickelten Systeme auf Systemsicherheit, Privatheit, Wahlfreiheit und Expropriation haben. Schließlich erwähnt er auch die politischen Probleme beim Versuch einer Durchsetzung globaler Lizenzen und die unterschiedlichen Widerstände, die dagegen in Europa, vor allem aus Frankreich aufgebracht werden. Dazu ist das letzte Wort nicht gesprochen, denn ebenfalls mächtige Gegner sind die Open-Access Bewegungen.

Hans-Dieter Helliges Analyse der Entwicklung des Internet beschreibt dieselbe als Agglomeration viefältigster Erfindungen und Entwicklungen, die weder von Anfang an beabsichtigt noch vorhergesehen wurden. Die (geringen) TCP/IP-Protokollfestlegungen standen in harter Konkurrenz zu den starreren europäischen OSI-Protokollen und haben sich gerade wegen ihrer Unvollständigkeit und Erweiterbarkeit letztlich durchgesetzt. Helliges sehr genaue und differenzierte Darstellung der Entwicklungswege des Internet zeigen deren Kontingenzen und soziotechnischen Bedingtheiten zwischen militärischen Anfängen, Firmeninteressen, studentischen Bedürfnissen und Einzelentwicklern. Die durch die auf Akteure zentrierte Technikgeschichtsschreibung nachträglich in die Welt gesetzten Heldenmythen deuten die Geschichte aus Sicht der „Sieger“, unterschätzen die strukturellen Bedingungen, und blenden Theorie- und Methodenprobleme bei der Verknüpfung der Einzelereignisse und Entwicklungsmomente aus. Stattdessen zeigt Hellige, dass die Leitbildfixierung der „heroischen“ Entwickler durch immer neue Gruppen von Nutzern gemäß ihrer Nutzungsbedürfnisse überwunden wurde.

Schließlich plädiert Eckhard Kanzow in seinem unkonventionellen Text „Zu lebenden und nicht lebenden Systemen – braucht die Infomedizin die Informatik?“ für eine neue, auf eine ganzheitliche Alternativmedizin gerichtete Teildisziplin der Informatik, die Infomedizin. Er entwickelt zunächst die aus den Gender Studies bekannten Deutungen zur Entwicklung der Natur- und Technikwissenschaften, zieht dann die aus Konstruktivismus und Systemtheorie geholten Theorien der Selbstorganisation und Autopoiesis zur Überwindung der Trennung von Geist und Körper heran, um schließlich zu seinem eigentlichen Thema überzuleiten, Leben basierend auf Information. Dabei meint er mit Informationsflüssen nicht nur die durch Transmitter, Botenstoffe und elektrische Signale auf Nervenbahnen transportierte Information, sondern auch solche, die über mit Lichtgeschwindigkeit oszillierende Felder gesendet werden, wie sie in der Physik schon seit langem bekannt sind. In Biologie und Medizin sind solche Theorien noch nicht allgemein anerkannt, sondern werden in der Alternativmedizin, etwa mit der Elektroakupunktur und den Bioresonanzmethoden vorwiegend diagnostisch, aber auch therapeutisch (Homöopathie) angewendet. Sie knüpfen auch an alte asiatische Medizinrichtungen, wie die TCM, an, indem etwa die Messungen der Schwingungen an Meridianen vorgenommen werden können. Viele dieser in den westlichen Alternativansätzen entwickelten Erprobungen bedienen sich softwaregesteuerter Mess- und Behandlungsmethoden. Sie sind weder kanonisiert noch wissenschaftlich ausreichend erhärtet, was zum Teil auch an den Standardisierungsanforderungen der Schulmedizin und Pharmazie für Medikamente und Therapien liegt, welche sich individualisierten Medizinen wie der Homöopathie verschließen, da sie gleiche Ergebnisse über eine größere Population erfordern. Alternative Begründungen, Methoden, Therapien und Standardisierungen erhofft sich Herr Kanzow nun von der Infomedizin.

Gegen Ende des Bandes sind die Stellungnahmen einer Anhörung zu Visionen für die Anforderungen an die Informatik im Jahr 2020 abgedruckt. Wie zutreffend sie sind, wird in gar nicht so ferner Zukunft festzustellen sein. Am Ende steht ein aus den 1970er Jahren stammender Text von Hans-Jörg Kreowski, der Zitate aus Konrad Zuses Buch „Der Computer – mein Lebenswerk“ in ein fiktives Interview montiert. Er zeigt so etwas holzschnittartig, wie Zuses vermeintlich apolitische Haltung beim Versuch, während des Dritten Reiches die Entwicklung der Zuse Z2 zu finanzieren und sie für die Fernsteuerungsberechnungen der V2 zum Einsatz zu bringen, dem NS-Regime zuarbeitete. Der Text schließt sehr gut ergänzt mit selbstkritischen Zitaten von Galileo Galilei aus Berthold Brechts „Leben des Galilei“.

Da das Buch vom Jahre 2008 stammt, d. h. 2006 bis 2007 geschrieben wurde, und sich in der Zwischenzeit Webanwendungen, Data Mining, die Integration der Medien, Cloud Computing, die sozialen Medien und der Internetkommerz sehr dynamisch weiter entwickelt haben und mit alledem Probleme der Sicherheit und des Schutzes von Persönlichkeitsrechten enorm zugenommen haben, wäre heute schon ein neues Buch zu schreiben, was dem FIfF empfohlen werden soll. Doch zeigt der Band exemplarisch, wie wichtig für die und innerhalb der Informatik ein ergänzender kritischer Blick auf ihre Theorien und Ziele, ihre Entwicklungen und Problemlösungen ist, um Sinnloses zu vermeiden und Schäden von der Gesellschaft abzuwenden.

Hans-Jörg Kreowski (Hrsg.): Informatik und Gesellschaft – Verflechtungen und Perspektiven, Reihe Kritische Informatik, LIT-Verlag, Band 4 des FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung), 2008

# FIfF e.V.



Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

## Das FIfF-Büro

**Geschäftsstelle FIfF e.V.**
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
*E-Mail:fiff@fiff.de*

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

**Bankverbindung:**
Sparda Bank Hannover eG
Spendenkonto: 800 927 929
BLZ 250 905 00
IBAN: DE66 2509 0500 0800 9279 29
BIC: GENODEF1S09

## FIfF im Netz

**Das ganze FIfF:**
*www.fiff.de*

**FIfF-Mailingliste**
An- und Abmeldungen an:
*http://lists.fiff.de/mailman/listinfo/fiff-L*
Beiträge an: *fiff-L@lists.fiff.de*

**FIfF-Mitgliederliste**
An- und Abmeldungen an:
*http://lists.fiff.de/mailman/listinfo/mitglieder*
Beiträge an: *mitglieder@lists.fiff.de*

**Mailingliste Videoüberwachung:**
An- und Abmeldung unter
*http://lists.fiff.de/mailman/listinfo/cctv-L*
Beiträge an: *cctv-L@lists.fiff.de*

## Beirat

**Michael Ahlmann** (Bremen); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München)**; Prof. Dr. Wolfgang Coy** (Berlin); **Prof. Dr. Wolfgang Däubler** (Bremen); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg), **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Michael Grütz** (Konstanz); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Dr. Eva Hornecker** (Glasgow/UK); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Klaus Köhler** (München); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Klaus-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Bremen); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Rossnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Prof. Dr. Gabriele Schade** (Erfurt); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Waldorfhäslach)

## FIfF-Vorstand

**Stefan Hügel (Vorsitzender)** – Frankfurt am Main
**Prof. Dr. Dietrich Meyer-Ebrecht (stellv. Vorsitzender)** – Aachen
**Sylvia Johnigk** – München
**Prof. Dr. Hans-Jörg Kreowski** – Bremen
**Kai Nothdurft** – München
**Jens Rinne** – Mannheim
**Raffael Rittmeier** – Bremen
**Prof. Dr. Britta Schinzel** – Freiburg im Breisgau
**Ingrid Schlagheck** – Bremen

## Impressum

| | |
|---|---|
| **Herausgeber** | Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) |
| **Verlagsadresse** | FIfF-Geschäftsstelle<br>Goetheplatz 4<br>D-28203 Bremen<br>Tel. (0421) 33 65 92 55<br>*fiff@fiff.de* |
| **Erscheinungsweise** | vierteljährlich |
| **Erscheinungsort** | Bremen |
| **ISSN** | 0938-3476 |
| **Auflage** | **1.200 Stück** |
| **Heftpreis** | 7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren. |
| **Hauptredaktion** | Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Jens-Holger Streck |
| **Schwerpunktredaktion** | Hans-Jörg Kreowski |
| **V.i.S.d.P.** | Stefan Hügel |
| **FIfF-Überall** | Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert@mtsf.de.*<br><br>Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional* |
| **Retrospektive** | Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de* |
| **Lesen, SchlussFIfF** | Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de* |
| **Layout** | Berthold Schroeder |
| **Titelbild** | defwheezer (CC BY-NC-SA 2.0)<br>http://www.flickr.com/photos/defwheezer/999161292 |
| **Druck** | Meiners Druck, Bremen |

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.


## Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

**FIfF-Jahrestagung 2012**

9. bis 11.11.2012 in Fulda

**FIfF-Klausur 2012**

„FIfF-Kommunikation und digitale Veröffentlichungen"
16. bis 18.3.2012 in Bochum – Details *fiff@fiff.de*

**FIfF-Vorstandssitzung**

4. Februar 2012 in Bremen

**FIfF-Kommunikation**

**1/2012** »Dialektik der Informationssicherheit«
Dagmar Boedicker, Sylvia Johnigk, Kai Nothdurft u.a.
(Redaktionsschluss: 3.2.2012)

**2/2012** »Verfassungsbeschwerden«
Jens Rinne, Raffael Rittmeier u.a.
(Redaktionsschluss: 4.5.2012)

**3/2012** »Visualisierung«
Britta Schinzel u.a.

**4/2012** »Enquête-Kommission Internet und digitale Gesellschaft«
Stefan Hügel u.a.

**W&F – Wissenschaft & Frieden:**

3/11 – Soldaten im Einsatz

4/11 – »Arabellion« Demokratie im Arabischen Raum

**DANA – Datenschutz-Nachrichten:**

2/11 – Datenschutzprobleme moderner Technik

3/11 – Online-Spiele

4/11 – Datenschutz im Bildungswesen

## Das FIfF-Büro


**Geschäftsstelle FIfF e.V.**
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
*E-Mail: fiff@fiff.de*
Die Bürozeiten finden Sie unter *www.fiff.de*

**Kontakt zur Redaktion der FIfF-Kommunikation:**
*redaktion@fiff.de*


**Wichtiger Hinweis:** Postvertriebsstücke wie die FIfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FIfF-Büro jede Adressänderung rechtzeitig bekannt zu geben!

# Schluss FIfF

## Zeitbild Wissen
## „Demokratie stärken – Linksextremismus verhindern“

**ist ein Projekt der Zeitbild Stiftung, gefördert vom Bundesministerium für Familie, Senioren, Frauen und Jugend, September 2011.**



*Foto carstenbach (CC BY 2.0)*

**Wir fragen die Ministerin:**

**Können Sie uns den Bezug zwischen Linksextremismus und diesem Foto auf Seite 15 der Zeitschrift erklären? Das Foto zeigt die Demonstration „Freiheit statt Angst“ im Jahre 2007.**

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.