Editorial

Cyberpeace – Frieden gestalten mit Informatik. Das war der Titel unserer Jahrestagung 2013 und das ist der Titel des Schwerpunkts in diesem Heft, der die Jahrestagung dokumentiert und aufarbeitet.

Dass diese Forderung sehr aktuell ist, zeigen die Ereignisse der letzten Monate: die weiterhin andauernde Ausspähung duch Nachrichtendienste, verbunden mit Angriffen auf die Integrität unserer Kommunikationsinfrastruktur – allein bereits eine Form des Cyberkriegs – und die Kriegführung durch Drohnen, die die Erkenntnisse der Ausspähung nutzt und Recherchen zufolge bereits den Tod tausender von Menschen verursacht hat – vermeintliche Terroristen ebenso wie Unschuldige –, praktisch immer ohne rechtsstaatliches Verfahren.

Dass ein unbegrenzter Cyberkrieg gegen Freund und Feind geführt wird, machen *Ingo Ruhmann* und *Ute Bernhardt* in ihrem umfassenden Dossier *Information Warfare und Informationsgesellschaft – Zivile und sicherheitspolitische Kosten des Informationskriegs* sehr deutlich. Das Dossier entstand in Zusammenarbeit mit der Zeitschrift *W&F – Wissenschaft und Frieden* und ist deren Ausgabe 1/2014 sowie dieser Ausgabe der *FIfF-Kommunikation* beigelegt.

Der Schwerpunkt der Ausgabe zur Jahrestagung besteht aus zwei Teilen: Der erste Teil dokumentiert Vorträge und Arbeitsgruppen der Tagung. In seinem im Umfeld des FIfF sicherlich Widerspruch provozierenden Beitrag *Datenschutz bei datenzentrischen Diensten: Auslaufmodell oder nur 30 Jahre zurück?* vertritt *Günter Müller* die Grundthese, Daten seien als handelbare Ware aufzufassen. Er schlägt einen wirtschaftlich basierten Datenschutz vor, der auf Transparenz in Verbindung mit Privatheitsregeln fußt. Heutige Datenschützer erscheinen ihm eher wie anachronistische Idealisten – ein frei bestimmtes *Opt-out* ohne soziale und wirtschaftliche Kosten sei über Regulierung nicht erreichbar.

Das Imperium schlägt zurück, so überschreibt *Sebastian Schweda* seinen Bericht *zur Lage der Menschenrechte im digitalen Zeitalter*. „*Cyberwar ist die Fortführung des kinetischen Kriegs mit anderen Mitteln*", stellt er fest. „*Der Kollateralschaden dieses virtuellen Krieges mit realen Folgen ist die weitgehende Vernichtung der unkörperlichen Integrität des Einzelnen: seiner Privatsphäre.*" Schweda arbeitet am Aufbau einer Koordinationsgruppe *Digitale Technologien und Menschenrechte* bei *amnesty international* und wünscht sich dazu Austausch und Kooperation mit dem FIfF.

„*Die Infrastruktur unserer digitalen Welt wird ganz bewusst unsicher, extern zugreifbar und flächendeckend überwacht gestaltet*", so *Rainer Rehak* in seinem Beitrag *Die Grenzen des Systems sind die Grenzen der Person*. Er fordert unter anderem die Beendigung der Zusammenarbeit des BSI mit Geheimdiensten, die Aufhebung der staatlichen Abhängigkeit deutscher Datenschutzkontrollinstanzen und den ausschließlichen Einsatz freier Software in staatlichen Stellen und Organen. Rainer Rehak bezweifelt, dass „*eine Demokratie überhaupt mit dem Prinzip des Geheimen (von unfreier Software bis hin zu Geheimdiensten) kompatibel ist.*"

Ausführlich wird die Arbeitsgruppe *Mitten im Cyberkrieg – Angriff auf die Zivilgesellschaft* behandelt. In ihrem einleitenden Beitrag stellen *Ute Bernhardt* und *Ingo Ruhmann* fest, dass durch die Ausspähung des NSA-Skandals nicht allein unsere Privatsphäre, sondern die gesamte Infrastruktur in Gefahr ist, deren Voraussetzung sichere IT-Systemen sind. Die Autoren vermissen jegliche politische Gestaltungsidee und erwarten von IT-Sicherheitsverantwortlichen in der Wirtschaft und von Bürgerinnen und Bürgern, notfalls ihre Interessen gegenüber Politik und Cyber-Kriegern durchzusetzen.

Ein erster Schritt dazu ist der Selbstdatenschutz. *Karin Schuler* gibt in ihrem Beitrag *Wer nicht kämpft, hat schon verloren* einen Überblick über dessen Möglichkeiten und Werkzeuge: „*Weder der Gesetzgeber noch Fatalismus bringen uns unsere Grundrechte zurück, wenn wir nicht auch die Möglichkeiten des Selbstdatenschutzes ausschöpfen.*" Eine umfassende Darstellung zur *deutschen Sicherheitspolitik, Bundeswehr und Cyber-Warfare* gibt der frühere Bundestagsabgeordnete *Paul Schäfer*. Zur Einhegung und Kontrolle fordert er mindestens die Beseitigung bestehender Sicherheitsmängel, die Durchsetzung des Grundwerts *Schutz der Privatsphäre* als Teil der Netzpolitik, Rüstungskontrolle und Abrüstung anstatt eines neuen Rüstungswettlaufs auch im Bereich der Cyberwarfare, und das ständige kritische Hinterfragen der Kriseninterventionen *out of area*.

Der zweite Teil des Schwerpunkts dokumentiert den *FIfF-Studienpreis 2013*. Nach einer einleitenden Übersicht folgen die Beiträge von *Daniel Spittank*: *Too smart for you? – Anforderungen an den Einsatz von mobilen Informatiksystemen in der Schule,* von *Agata Królikowski*: *‚Due to legal Issues' – Packet Inspection* und von *Julia Hofmann*: *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface*.

Der aktuelle Teil enthält eine Analyse von *Christian Schrader*: *Edward Snowden – Held oder Verräter*. „*Letztlich ist er ein Held*", stellt er darin fest, „*weil er uns hoffen lässt, dass die in ihrem Krieg gegen den Terror so verblendeten USA doch wieder das Land der Freiheit sein können.*" In der kurzen Fortsetzung seines Beitrags aus der *FIfF-Kommunikation* 4/2013 liefert *Stephan Geelhaar* ein Update zum *Ausbau der Internet-Polizei*. Ergänzt wird der aktuelle Teil durch Konferenzberichte von *Sylvia Johnigk* und *Sebastian Jekutsch* zum 30. *Chaos Communication Congress* und die bereits etablierten Kolumnen.

Die Retrospektive, erneut von *Ingo Ruhmann* zur immer noch aktuellen *Politik der Chiffren* aus Sicht von 1996 und unsere Rezensionen von Büchern und Filmen ergänzen diese Ausgabe der *FIfF-Kommunikation*.

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

Stefan Hügel
für die Redaktion