VEREIN SICHERHEITSPOLITIK
UND WEHRWISSENSCHAFT

POSTFACH 65, 8024 ZÜRICH

**Sicherheitspolitische Information**

Herausgegeben vom Verein Sicherheitspolitik und Wehrwissenschaft (VSWW)
Postfach 65, 8024 Zürich (PC 80–500-4)

www.Chinfo.ch/vsww

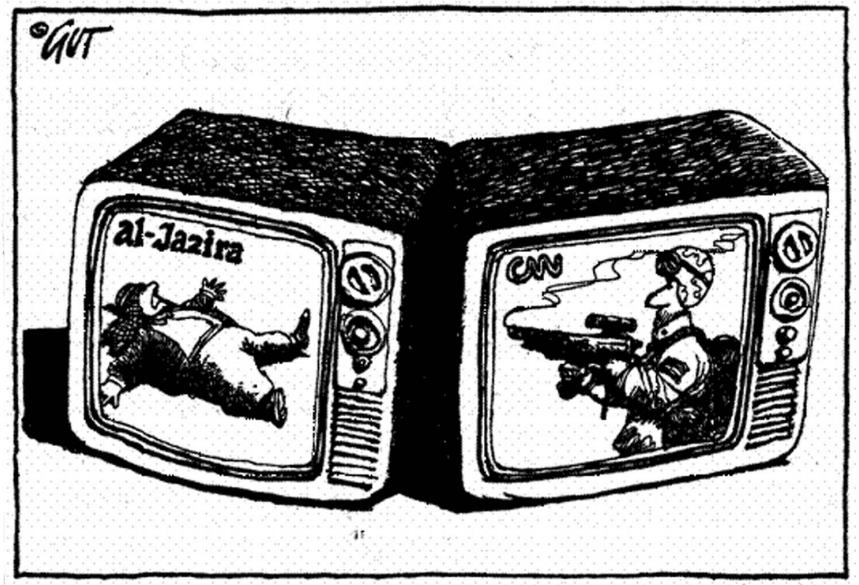
Präsident: Dr. Günter Heuberger
Redaktion: Dr. Daniel Heller (heller@farner.ch)

Juni 2003

# Information Warfare und behördliche Informationsführung

## Bestandesaufnahme und Thesen zur Weiterentwicklung unserer diesbezüglichen Vorkehrungen in der Schweiz

Oberstlt i Gst Daniel Heller, Erlinsbach




Krieg der Bilder.

## Inhaltsverzeichnis



## Vorwort

Wissen ist Macht. Jeder kennt diesen Ausspruch. Wenn Wissen Macht ist, ist auch die aufbereitete Form von Wissen – die Information – Macht. Macht kann für oder gegen jemanden oder für oder gegen etwas eingesetzt werden – so kann sie auch zur Waffe werden. Informationskriegsführung und Informationsführung in ausserordentlichen Lagen sind brennend aktuelle Themen. Der Irak-Krieg hat uns wieder einmal vor Augen geführt, welche Bedeutung der Information im Konzert der Mächte zukommt.

Die Diktaturen haben die Bedeutung der Beeinflussung der Massen durch die Information rasch erkannt. Sie setzten die Information manipulativ, das heisst als Waffe oder präziser als Instrument zum Machterhalt virtuos ein. Sie bemächtigten sich dazu aller jeweils verfügbaren Medien. Am umfassendsten hat wohl der Propaganda-Apparat des Dritten Reiches Macht ausgeübt durch Manipulation und Beeinflussung der Informationsverbreitung.

In der offenen Gesellschaft, mit aufgeklärten Staatsbürgern, demokratisch gewählten Behörden und einer Vielfalt von sich konkurrierenden Medien könnte für den oberflächlichen Beobachter der Eindruck aufkommen, wir seien vor derartigem gefeit. Das stimmt wohl, wenn wir den Staat als *Akteur* im Auge haben. Stimmt es auch, wenn wir den demokratischen Staat und seine Behörden als *mögliche Opfer* ins Auge fassen? Wie schützen sich die Schweiz resp. die Schweizer Behörden vor Desinformation? Wie wird die behördliche Information in Krisenlagen sichergestellt?

Wenn es um den Schutz der offenen Gesellschaft oder aber von Personen oder Institutionen vor Kampagnen, Manipulation und Desinformation geht, tauchen heikle Fragen auf. Denn die freien Medien sind das unabdingbare Gegenstück zur Demokratie. Von Alvin Toffler stammt die Aussage: *«Versuchen wir, die Medien zu kontrollieren, unterhöhlen wir die Demokratie. Unterlassen wir es, unterhöhlen die Medien die Demokratie».*

In der vorliegenden Studie geht es darum, die neuen Gefährdungen aufzuzeigen, bezüglich ihrer inhaltlichen und technologischen Dimension zu analysieren und unsere wesentlichen Vorbereitungen im Hinblick darauf zu beurteilen.

Daniel Heller[1]

1 Der Autor ist Historiker, Direktor bei Farner PR, Unterstabschef Medien im Informationsregiment 1 und Geschäftsführer des VSWW.

# 1 Entwicklung der Rahmenbedingungen

## 1.1 Informationsrevolution im Gefolge des Technologiefortschrittes

Unter Informationsrevolution versteht man die (andauernde) Integration von neu entwickelten Informations- und Kommunikationstechnologien in ein multimediales Kommunikationssystem mit globaler Reichweite.

Wesentliche Faktoren sind dabei zunehmende Geschwindigkeit und grössere Kapazität. Hinzu kommen ausgebaute Flexibilität bei der Aufnahme und Verarbeitung von Daten und dadurch deren vereinfachte Transformation in Wissen. Drei wesentliche Merkmale der Technologiesprünge basieren auf

- dem Internet und
- der Verbreitung von Mobiltelefonen (Satellitentelefonen).

Sie finden ihre Entsprechung in laufend modernisierten militärinternen Informationstechnologien.

Hauptsächlichste Auswirkungen und Merkmale dieser Informationsrevolution sind:

- Berichterstattung in Echtzeit
- Verbesserter Zugang zu Informationstechnologie

Dass wir im medialen Zeitalter leben, ist bereits ein Allgemeinplatz. Unsere Welt ist – gerade auch wegen der Unmittelbarkeit der medialen Vermittlung – zum Global Village geworden. Sender wie CNN bringen live den Beginn von Kriegen in unsere Stuben. Der Bericht des US-Sonderstaatsanwaltes, der die Lewinsky-Affäre untersuchte, war im Moment, in dem er dem Amerikanischen Kongress zugeleitet wurde, via Internet auch der ganzen interessierten Weltöffentlichkeit zugänglich. Kaum ein Behördendokument, das nicht seinen Weg in die Medien findet, meist schon bevor es definitiv verabschiedet ist. Neuartig an diesem Medienumfeld sind die Unmittelbarkeit, die Raschheit und die Reichweite der modernen Medien. Der traditionelle über Jahrhunderte funktionierende Wissensvorsprung der Behörden ist dadurch zunehmend verschwunden. Man spricht deshalb auch von den Medien als von der *«vierten Gewalt»* im Staat.

## 1.2 Entwicklungstrends im Mediensystem[2]

**Asymmetrischer Zugang:** Die weltweiten Entwicklungen im Mediensystem verlaufen asymmetrisch. Eine «digitale Kluft» zwischen Industrie- und Entwicklungsländern ist weiterhin vorhanden und wird auf absehbare Zeit die Trennung zwischen den *«Information-Rich»* und den *«Information-Poor»* wie bereits bei den klassischen Medien aufrechterhalten. Insofern ist für grosse Bevölkerungsgruppen auf der Welt nur ein begrenzter Zugang zu Medien gegeben.

Aufgrund ihrer kommerziellen Motivation werden global agierende Medienunternehmen ihre Produkte unter Berücksichtigung regionaler Besonderheiten auf allen Märkten absetzen wollen. Der Ausbau der propagierten Informationsgesellschaft dient in erster Linie den Interessen der OECD-Welt. Er verläuft trotz Verlautbarungen derzeit weitgehend unreguliert. Der Absatz von Medienprodukten wird auch durch sprachliche und kulturelle Unterschiede in den Regionen begrenzt. Mit Ausnahme von herausragenden weltpolitischen Ereignissen berücksichtigt das Informationsangebot die staatlichen, regionalen und kulturellen Grenzen. Beispielsweise sind die Printmedien in Europa auf länderspezifische Berichterstattung orientiert. Die einzige Tageszeitung, die eine europäische Öffentlichkeit herstellt, ist die *«Financial Times Europe».*

**Relativierung von Grenzen:** Medienaussagen können heute global verbreitet und prinzipiell von allen Nutzern aufgegriffen werden. Medienbilder zeigen besonders in Krisen- und Katastrophengebieten eine grosse Wirkung auf die öffentliche Meinung und lösen Reaktionen der politischen Akteure aus. Der Realitätsgehalt solcher Aussagen bleibt für den Mediennutzer meist nicht nachprüfbar.

Insgesamt kann man nicht uneingeschränkt von einer Internationalisierung des Mediensystems ausgehen resp. sprechen. Gewisse Versuche einer Dominanz von global agieren Medienkonzernen führen grundsätzlich zu keinem «einheitlichen» Weltbild. Dieses wird vielmehr immer noch aufgrund regionaler und kultureller Besonderheiten gebildet.

---

2 Wir folgen hier Schlussfolgerungen von Hans-Joachim Reeb (Oberstleutnant Dr. Hans-Joachim Reeb, Jahrgang 1955, ist Dozent Politische Wissenschaften an der Führungsakademie). Zahlreiche Veröffentlichungen, wie etwa: Die Medien im «Krieg gegen den Terror».
Reader Sicherheitspolitik unter: www.reader-sipo.de.

Allerdings fällt die Einheit von Staat, Gesellschaft und Wirtschaft als Folge der Globalisierung zunehmend auseinander, die Bedeutung von Grenzen sinkt. Macht und Einfluss gehen nicht länger nur von den «harten» Bereichen Territorium, Militär und Ressourcen aus, sondern vermehrt von «weichen» Bereichen wie Information, Technologie und flexiblen Institutionen.

**Kommerzialisierung:** Als universelles Leitbild des Mediensystems gilt die Presse- und Meinungsfreiheit. Es sind Korrelationen zwischen der Gewährung von Medienfreiheit und politischer Stabilität sowie sozialem Fortschritt erkennbar. Internationale Organisationen und NGOs sehen hier einen Arbeitsschwerpunkt. Während die Pressefreiheit in weiten Teilen der Welt unmittelbar gefährdet ist oder nur eingeschränkt gewährt wird, macht die Kommerzialisierung im Mediensystem sie in den anderen Regionen zu einem zerbrechlichen Gut. Gegen eine Fixierung auf Quoten, Auflagen und Gewinnmaximierung bedarf es dort der «Korrektive». Somit wirken sowohl politische als auch ökonomische Interessen auf eine freie Berichterstattung ein, die sich als «vierte Gewalt» versteht. Die «Skala» der Instrumentalisierung von Medien reicht von unabhängiger Berichterstattung bis zu ihrem missbräuchlichen Einsatz als Mittel zur vorsätzlichen Diskreditierung von Personen und Institutionen. Die zwischen diesen Polen liegenden Einflüsse auf die Medienarbeit sind vielfältig. Sie begünstigen in unterschiedlicher Art und Weise die Informiertheit und Manipulierbarkeit des Bürgers.

Ein *«free flow of information»* setzt in jedem Fall die Gewährleistung von Medien- und Pressefreiheit voraus. Diese ist weltweit nur in demokratischen Gesellschaften gegeben. Für eine globale Kommunikationsordnung ist die Durchsetzung dieses demokratischen Grundrechtes unabdingbar. An seiner Gestaltung sollten neben den Regierungen auch informelle Akteure (NGOs) mitwirken. Medien können international durchaus Wirkung entfalten und über die Beeinflussung der Weltmeinung Druck auf die Politik ausüben. Diese Meinung kann sich der *«Macht der Bilder und Botschaften»* leichter entziehen, wenn mündige Bürger die *«Spielregeln der Medien»* verstanden haben.

Aus diesen Errungenschaften resultieren neue Handlungsmöglichkeiten. Ihnen gegenüber stehen aber auch bisher unbekannte Verteidigungszwänge.

## 1.3 Information Warfare – ein neues Gesicht des Krieges?

Die Bedeutung der Information im Kriegsfall wurde lange vor unserer Zeit erkannt. Bereits 500 v. Chr. riet Sun Tzu in seiner Schrift *«Die Kunst des Krieges»*[3] zu aktiver Information auf der eigenen Seite, gegenüber dem Gegner aber zur Täuschung.

Seither hat sich viel getan. Die Bedeutung von Information und Desinformation hat sich in Zeiten des Internets und der satellitengesteuerten Aufklärung akzentuiert[4]. In den militärischen Doktrinen der technologisch fortschrittlichsten Länder – allen voran der USA – hat Information Warfare deshalb Eingang gefunden[5]: *«We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversar's ability to do the same.»* Information Warfare umfasst zunächst einmal sämtliche Formen der Interaktion, bei denen es um den Austausch von Informationen geht. Die zentrale Überlegung ist, dass militärische Konflikte zukünftig nicht mehr durch die qualitative und quantitative Überlegenheit der Streitkräfte gewonnen werden, sondern dass jene Partei Vorteile hat, die über die besseren Informationen verfügt. Die US-Denkfabrik Rand Corporation hat bereits 1993 den Begriff vom «Cyberwar» geprägt. *«Kriegsführung hängt nicht länger primär davon ab, wer wie viel Kapital, Arbeit und Technologie ins Feld führt, sondern wer die besten Informationen über das Schlachtfeld hat»,* schrieben die beiden Rand-Forscher John Arquilla und David Ronfeldt in einer Studie.

Diese Entwicklung wurde durch den Einsatz von neuen Technologien begünstigt und beschleunigt. Die Vorzüge der neuen Technologien sind vielfältig: Sie reichen vom Sammeln grosser Datenmengen (z.B. optische Informationen eines Satelliten oder Aufklärungsflüge einer Drohne) über deren Archivierung (exponentiell steigende Speicherkapazität) und Verarbeitung (Prozessorleistung) bis hin zur Weitergabe ohne Zeitverlust (schnelle und sichere Kommunikationswege), um «just-in-time» beispielsweise Präzisionswaffen ins Ziel zu lenken.

---

3 Sun Tzu: «Die Kunst des Krieges» gilt gemeinhin als älteste militärische Abhandlung der Welt.

4 Grundlegend dazu: Peter Forster: Aber wahr muss es sein. Frauenfeld 1999, sowie ders. «Lehren aus dem Irak Krieg», unveröffentl. Manuskripte 2003.

5 Joint Doctrine for Command and Control Warfare JP 3-13.1 (Ziel: O-O-D-A-loop = Observation, Orientation, Decision, Action).

Wie schwierig aber die erfolgreiche Gestaltung von solch extrem kurzfristig geplanten Operationen trotz modernster Technologie ist, zeigen die gescheiterten Überraschungsangriffe der USA auf Saddam Hussein im jüngsten Golfkrieg. Insbesondere der vor Beginn der eigentlichen Kampfhandlungen ausgeführte Schlag machte aber deutlich, welche entscheidende Bedeutung der Informationsführung im heutigen Krieg zukommen kann.

Die zunehmende Wichtigkeit von Informationsüberlegenheit bewirkt eine Verschiebung der militärischen Ziele weg von den klassischen Militärgütern hin zur Informationsstruktur. Es ist vor dem Hintergrund der Militärkampagnen der letzten Jahre davon auszugehen, dass die Informationsstruktur eines Gegners zunehmend zum Ziel von Kampfhandlungen wird. Durch deren Zerstörung ist der Gegner im Extremfall «blind», d.h. er kennt – wenn überhaupt – nur die Standorte der eigenen Truppen, während es die moderne Technologie der eigenen Seite ermöglicht, sowohl alle eigenen, als auch die gegnerischen Bewegungen zu kennen. US-General Tommy Franks konnte die Schlacht um Bagdad in Echtzeit auf einem eineinhalb Meter grossen Fernsehschirm verfolgen. Dank Satelliten und unbemannten Aufklärungsflugzeugen hatte er in seinem Hauptquartier in Doha (Katar) sogar den Feind auf dem Bildschirm. Das digitalisierte Schlachtfeld ist längst keine Vision mehr, sondern Realität.

In Anlehnung an Myriam Dunn[6] kann man sechs Theoreme im Zusammenhang mit der «wechselnden Natur» von informationsbasierter Macht und deren Verteilung aufstellen:

1. Informationsüberlegenheit wird in der neuen operationellen Umgebung als Schlüssel zum Erfolg angesehen;

2. asymmetrische Glaubwürdigkeit wird zur Kernressource von Macht;

3. Grenzen zwischen Staaten, militärische Politik, und der militärisch-zivile Bereich verwischen zusehends im Informationszeitalter;

4. Netzwerke vs. Hierarchien: zentralisierte hierarchische Organisationen verlieren an Boden im Vergleich zu dezentralisierten flachen Organisationen;

5. Asymmetrie vs. Doktrin der Dominanz: kleine Players können die traditionell mächtigeren leichter schwächen/beeinträchtigen.

6. Im Bereich der staatlichen und militärischen Führung führt die Informationsrevolution zu einem höheren Stellenwert der Information in der strategischen Planung.

# 2 Die daraus entstehenden Gefahren

## 2.1 Verletzliche Infrastrukturen der Informationsgesellschaft

Die Informationsrevolution hat in der Gesellschaft tiefe Spuren hinterlassen. Mobile Kommunikationsgeräte erlauben den Kontakt zu jeder Zeit und an jedem beliebigen Ort. Die starke Verbreitung hat die Informationsstruktur gleichsam zu einer Art Nervensystem unserer hoch entwickelten Gesellschaft gemacht. Dennoch haben sich nicht alle Prophezeiungen bewahrheitet. Mit der Luftblase der kometenhaft aufgestiegenen New Economy platzten auch andere Träume, beispielsweise jener der Verschmelzung von Arbeitsplatz und privatem Raum. Die Vision vom mobilen Laptop-Büro unter Palmen wurde nie wahr. Im Zuge der wirtschaftlichen Baisse wurde sie stillschweigend beerdigt.

Die erste Ebene der Konfrontation dreht sich deshalb um die *Verfügbarkeit und Intaktheit der Technologien.*[7]

### *2.1.1 Cyberwar – Kriegsführung im virtuellen Raum*

Schon Wochen vor Kriegsbeginn überschwemmte der US-Geheimdienst CIA die politische und militärische Elite Iraks mit E-Mails. Das irakische Regime wehrte sich gegen die Mail-Flut durch Filter, die alle Nachrichten mit amerikanischem Absender abblockte. Die CIA umging diese Sperre wiederum, indem sie E-Mail-Provider aus Europa oder Nah-Ost einsetzte.

Trotz oder gerade wegen ihrer Überlegenheit im virtuellen Raum ist die USA wesentlich anfälliger

6 Myriam Dunn: Information Age Conflicts, Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, Nr. 64, Zürich 2002.

7 Umfassend: International CIIP Handbook; an Inventory of protection Policies in eight Countries; Ed. By Andreas Wenger, Jan Metzger, Myriam Dunn, Zürich (ETH) 2002.

gegen Cyber-Attacken als der Irak. Denn das Internet ist ein wesentlicher Teil der Infrastruktur der Vereinigten Staaten. Allein in den ersten drei Stunden des Krieges hat der finnische Antivirenhersteller F-Secure tausend manipulierte Internet-Seiten registriert, darunter auch die der US-Marine.

Andere Seiten, beispielsweise jene des britischen Premiers Tony Blair[8], wurden mit Massenmails überlastet und mussten kurzzeitig vom Netz genommen werden. Ähnlich erging es dem Internetauftritt des in Qatar beheimateten Fernsehsenders Al-Jazeera[9], der von unbekannten Hackern vermutlich aus Protest gegen die gezeigten Bilder von amerikanischen Kriegsgefangenen lahm gelegt wurde. Solche Angriffe sind nicht neu. Bereits 2001 wurde nach dem Absturz eines amerikanischen Spionageflugzeugs des Typs EP-3E in China von unbekannten Tätern eine massive virtuelle Attacke gegen chinesische Webpages lanciert.

Die genannten Attacken zeigen, dass im Cyberwar die Angriffsziele nicht zwingend militärischer Natur sind. Zivile Informationsseiten können durch kritische Berichterstattung oder von der Kriegspropaganda abweichende Meinungen schnell zum Ziel von virtuellen Angriffen werden.

### *2.1.2 Cyberterror bedroht Satellitensystem*

Eine Fehlfunktion des Satelliten Galaxy IV macht 1998 die Verletzlichkeit der US-amerikanischen technischen Infrastruktur deutlich und zeigte, welche verheerenden Auswirkungen ein *Angriff auf das amerikanische Satellitensystem* haben könnte. Gemäss Vertretern des Pentagons hatte die als Unfall bezeichnete Störung einen Ausfall von 80 Prozent der Mobilfunkempfänger in den USA zur Folge. Für die Zukunft ist aber das Bedrohungsszenario denkbar, dass solche Dysfunktionen vorsätzlich herbeigeführt werden.

Im Januar 2001 legten militärische und zivile Experten die Ergebnisse einer im Anschluss an den Vorfall in Auftrag gegebenen Studie zur Bedrohung von US-Satelliten vor. Die Bandbreite möglicher Angriffe reicht von physischen Attacken auf Satelliten-Bodenstationen und das Eindringen von Hackern in sensible Netzwerke zur Satelliten-Steuerung über das Blenden des Sensoriums oder der Kamera der Satelliten bis hin zu deren Ausspionierung mittels Mikro- oder Nanosatelliten.

Dank auf dem internationalen Markt zunehmend erhältlichen Systemen können Staaten zudem die Fähigkeiten und Umlaufbahnen von Aufklärungssatelliten erkennen und bei deren Überflug gesuchte Objekte verstecken. Manche Staaten – beispielsweise Russland, China, Nord Korea, Iran und Kuba – verfügen ausserdem über Mittel, um Satelliten-Operationen durch elektronische Störmanöver zu unterbrechen. Russland brachte unlängst einen Sender in der Grösse einer Zigarettenschachtel auf den Markt, der GPS-Übertragungen im Umkreis von 50 Meilen blockieren kann. In den letzten Jahren wurden solche Geräte laut der schwedischen Defense Material Administration nachweislich genutzt, um den Polizeifunk oder elektronische Alarmsysteme ausser Kraft zu setzen.

### *2.1.3 Bedrohung wesentlicher Versorgungsnetze durch elektromagnetische Waffen*

Aufgrund der oben beschriebenen Vorteile, welche überlegene Informationsstrukturen im Kriegsfall mit sich bringen, ist es naheliegend, dass viele Staaten an der Entwicklung von elektromagnetischen Waffen arbeiten, die alle elektronischen Geräte im Umkreis von Kilometern unbrauchbar machen. Am weitesten fortgeschritten ist die Entwicklung in den USA. Im jüngsten Irak-Krieg setzten die Amerikaner zum ersten Mal elektromagnetische Waffen ein. Die modernste Entwicklung im US-Waffenarsenal ist eine «High Power Microwave»-Bombe, die durch einen starken elektromagnetischen Impuls im Umkreis von Hunderten Metern alle elektronischen Geräte, Telefone und Funkgeräte unbrauchbar macht. Computerfestplatten werden gelöscht, Autos bleiben stehen und Flugzeuge am Boden.

Der Einsatz elektromagnetischer Waffen ist auch in zivilem Kontext denkbar und könne sich mittelfristig zu einer reellen Gefahr für die hoch entwickelten westlichen Gesellschaften entwickeln. Deren hohe Abhängigkeit von elektrischen und elektronischen Systemen führt dazu, dass Störungen der wesentlichen Versorgungsnetze (Strom, Wasser, Telekommunikation, öffentlicher Verkehr etc.) grosse Schäden verursachen können.

8 www.number-10.gov.uk.
9 www.aljazeera.net und www.english.aljazeera.net.

Störfelder lassen sich bereits mit sehr begrenzten Mitteln erzeugen. Mit kompakten Mikrowellen-Störsendern sind kriminell oder terroristisch motivierte Gruppen in der Lage, zivile elektrische Systeme zu bedrohen. Ein Mikrowellensender[10] besteht im Wesentlichen aus einer leistungsfähigen Energiequelle, einem Mikrowellengenerator und einer Parabolantenne, die die Wellen fokussiert und auf das Ziel richtet. In ihrer Wirkung auf elektronische Geräte sind diese Wellen mit den Wellen in einem Mikrowellenherd vergleichbar: Sie erzeugen Wärme. Die Folgen sind Fehlfunktionen oder gelöschte Datenspeicher. Bei entsprechender Leistung kann es sogar zu einem Durchbrennen, also zu einer physischen Schädigung von elektronischen Bauteilen kommen.

Eine andere Möglichkeit besteht darin, statt kontinuierlicher Wellen einen kurzen elektromagnetischen Puls auf das Ziel zu richten. Dadurch können kurzzeitig hohe elektrische Feldstärken entstehen, die den normalen Informationsfluss von Signalen stören und unter Umständen sogar zum Durchschlag von Halbleiterbauelementen führen können.

Um sich die Folgen solcher Anschläge auf die öffentliche Infrastruktur vorzustellen, braucht es nicht viel Fantasie: Zusammenbruch des öffentlichen Verkehrs, lückenhafte oder gänzlich ausfallende Versorgung der Bevölkerung mit Wasser, Strom und Lebensmitteln. Im wirtschaftlichen Sektor würde besonders der Finanzplatz Schweiz durch den ausser Kraft gesetzten elektronischen Finanzverkehr Schaden erleiden.

Wie gross die von solchen Geräten ausgehende Bedrohung tatsächlich ist, lässt sich nur schwer abschätzen. Denn die Wirkung eines Senders ist von vielen Faktoren wie beispielsweise der Entfernung zum Ziel und allenfalls vorhandener Hindernisse (Abschwächung der Strahlung) abhängig. Experimente wurden bis anhin nur spärlich durchgeführt. Eines der wenigen vorhandenen Experimente stammt von der Microwave Test Facility im schwedischen Linköping, wo die Auswirkungen von intensiver Mikrowellenstrahlung auf ein Auto untersucht wurden[11]:

*«Die Experimente zeigten, dass eine Quelle, die in einem Lieferwagen Platz hätte, noch in einer Entfernung von 500 Metern Ausfälle verursachen kann. Dauerhafte Schäden wurden bei Distanzen von weniger als 15 Metern beobachtet. Unter anderem wurden Kontrolleinheiten für den Motor, Drehzahl- und Geschwindigkeitsmesser sowie die Alarmanlage beschädigt. Ein Mikrowellensender, der in einem am Strassenrand stehenden Lieferwagen versteckt ist, hätte also das Potential, den Verkehr zum Erliegen zu bringen. Eine schwächere Quelle mit den Abmessungen eines Aktenkoffers rief immerhin noch in einer Entfernung von 50 Metern Störungen am Auto hervor. Nicht minder interessant wäre es, das Risiko zu kennen, dem Flugzeuge beim Start und bei der Landung ausgesetzt sind. Diese Phase ist besonders kritisch, weil sich tief fliegende Flugzeuge im Einflussbereich eines möglicherweise am Boden stationierten Störsenders befinden.»*

## 2.2 Verletzliche offene Gesellschaft: Desinformation und psychologische Kriegführung

In einem zweiten, nicht minder bedeutsamen Bereich geht es nicht primär um Technik, sondern *um den Krieg um Inhalte.* Auch hier liefert vor allem der Blick auf die Führungsmacht USA Aufschlüsse zu den neuesten Trends.

Nach dem Kalten Krieg wurde die psychologische Kriegsführung vom Pentagon in das umfassendere Konzept der *Information Operations* (IO) eingeordnet. Dazu gehören offensive und defensive Massnahmen, um «feindliche Information und Informationssysteme» zu beeinflussen und die eigenen Informationen und Informationssysteme zu verteidigen.

### *2.2.1 Information Operations nach «9-11»*

Die Informationspolitik der USA war insgesamt nach dem 11. September 2001 sehr komplex und folgte einer Strategie von IO. Neben traditionellen Elementen, wie beispielweise Pressekonferenzen, wurden verstärkt auch die neuen Medien eingesetzt und Psychologische Operationen *(«PsyOps»)* in der Region durchgeführt. Das politische Klima nach den Anschlägen erlaubte es der US-Regierung, zurückhaltend mit Informationen umzugehen. Das zeigte sich an der Aus-

10 Die besondere Eignung von Mikrowellen rührt von ihrer Wellenlänge, die sich zwischen einem Zentimeter und einem Meter bewegt. Damit entspricht sie ziemlich genau den Abmessungen von Antennen, Kabeln oder Gehäuseöffnungen. Über eine dieser «Eintrittspforten» können die Wellen in ein Gerät eindringen und dort empfindliche elektronische Komponenten stören.

11 Neuer Zürcher Zeitung, 03.03.1999: Elektromagnetische Wellen als Waffe. Wie gut sind zivile Systeme gegen Störversuche gewappnet?

kunftsverweigerung zur Wahrung der nationalen Sicherheit und in Absprachen mit den Verlegern zu Programminhalten. Gegenüber Journalisten äusserte sich der Präsidenten-Sprecher Ari Fleischer: *«Sie haben das Recht Fragen zu stellen. Wir haben das Recht nicht zu antworten».* Auch 59 Prozent der Amerikaner waren der Meinung, dass das Militär mehr Kontrolle über die Kriegsberichterstattung ausüben sollte. Die US-Regierung präsentierte ein ganzes Paket an Massnahmen, das offensichtlich zum festen Bestandteil ihrer Kriegsführung gehört. Das US-Aussenministerium wirkte auf den Auslandssender *«Voice of America»* (VOA) ein, um die Ausstrahlung eines Interviews mit Taliban-Führer Mullah Mohammed Omar zu unterbinden. In ihrem Bemühen um ein Informationsmonopol kaufte die Regierung des Weiteren die Rechte an den Aufnahmen des Satelliten «Ikonos» auf, der Bilder vom militärischen Operationsgebiet machte.

Wie bereits mit einem Media Operation Center in Brüssel während des Kosovo-Krieges richteten die USA und Grossbritannien entsprechende Informationszentren in Washington, London und Islamabad ein. Als weitere medienpolitische Massnahmen wurden Internet-Kampagnen, ein weltweites Medien-Monitoring und der Aufbau von Rundfunk- und Satellitenprogrammen in Auftrag gegeben. Einem Bericht der «New York Times» Anfang 2002 zufolge, sollte ein «Office of Strategic Influence» vom Pentagon aus mit Hilfe der PR-Agentur Rendom Group für die Verbreitung von Propaganda und Desinformationskampagnen in das Ausland sorgen. Demnach war beabsichtigt gewesen, irreführende Pressemitteilungen zu streuen, falsche Artikel zu lancieren oder Computernetzwerke zu stören. Nach massiver Kritik der US-Medien, die Rückwirkungen auf ihre Medienberichterstattung befürchteten, wurde das Projekt gestoppt.

Eine andere Form von «Newsmanagement» ist die geplante Dokumentarfilm-Inszenierung des Krieges «Profiles from the Frontline» durch den zum Walt Disney-Konzern gehörenden Fernsehsender ABC im Auftrag des Pentagon. Die eindrucksstarken und quasi authentischen Filmbilder sollen dafür sorgen, dass der «Afghanistan-Feldzug» beim Zuschauer nach vorgegebenem Muster haften bleibt. Nachrichten-Journalismus wird durch «Militainment» ersetzt.

An der Front setzten die Amerikaner die herkömmlichen und grösstenteils bekannten Mittel der PsyOps ein. Dazu gehörten der Abwurf von Flugblättern und Windup-Radioempfängern (fixe Frequenzen) sowie die Ausstrahlung von Programmen durch C-130 Spezialflugzeuge vom Typ «Commando Solo» seit Mitte Oktober. VOA strahlte seit dem 25. September ebenfalls Sendungen in der Region aus.

Die Medien sind eine wichtige Grundlage für die Demokratie, weil sie vor allem auch für eine kritische Öffentlichkeit gegenüber der Regierung sorgen. Dazu müssen sie so objektiv wie möglich berichten können und gerade deshalb auch Kritik äussern dürfen. Das Korrektiv der Medien hat sich gerade jetzt wieder einmal eindrucksvoll erwiesen, als bekannt wurde, dass das Pentagon beabsichtigte, mit seinem nach dem 11.9. eingerichteten «Office for Strategic Influence» möglicherweise den Medien auch heimlich gefälschte Informationen unterzujubeln. Nach massiver Kritik wurde davon Abstand genommen.

### *2.2.2 Operationsunterstützende IO-Strategien im ersten Irak-Krieg*

Als Ziele der IO wird die Beeinflussung der *«menschlichen Führung und der menschlichen Entscheidungsprozesse eines Gegners oder eines möglichen Gegners»* verstanden. IO umfassen *«psychologische Operationen, physische Zerstörung, elektronische Kriegsführung (EW), Angriffe auf Computernetze und deren Verteidigung, militärische Täuschung, Gegenpropaganda, Gegentäuschung, Informationssicherung (IA), Operationssicherheit (OPSEC) und Eindringen in Computer»*. Dabei sollen die IOs mit damit verbundenen Aktivitäten wie der *«internationalen öffentlichen Information»* (IPI) synchronisiert werden, um *«Informationsthemen zu unterstützen, feindlicher Propaganda entgegen zu steuern, ausländische Rezipienten günstig zu beeinflussen und alliierte oder neutrale Rezipienten zu informieren».*

Im zweiten Irak-Krieg wurde gemutmasst, das Pentagon arbeite weiter zusammen mit einer geheim operierenden PR-Abteilung. Es habe möglicherweise einen Mediencoup der Art im Auge, wie er bereits für den Golfkrieg 1991 erfolgreich geschmiedet worden war. Schon vor dem Krieg gegen den Irak hatte die Organisation Citizens for a Free Kuwait 1990 die PR-Agentur Hill and Knowlton engagiert, um der militärischen Befreiung Kuwaits Nachdruck zu verleihen. Die Organisation wurde wieder von der kuwaitischen

Regierung finanziert, die das gerade Gegenteil einer demokratischen Regierung war. Die PR-Agentur schaffte es, ein fünfzehnjähriges kuwaitisches Mädchen, die Krankenschwester «Nayirah», am 10. Oktober vor dem Menschenrechtsausschuss in einer öffentlichen Anhörung darüber berichten zu lassen, dass irakische Besatzer angeblich mit Gewehren in Krankenhäuser eingedrungen und Säuglinge aus den Brutkäsen geholt und auf den kalten Boden geworfen oder verkauft hätten. Die Agentur liess von der Aussage einen Film herstellen, der von verschiedenen Sendern auch ausgestrahlt wurde und bei den Zuschauern weltweit Entsetzen auslöste. Zudem gelang es der Agentur, während der Sitzung des Sicherheitsrats der UN am 27.11.1990 Bilder von angeblich gefolterten Kuwaitis zu präsentieren und angebliche Zeugen aussagen zu lassen. Zwei Tage später setzte der Sicherheitsrat dem Irak ein Ultimatum für den Rückzug aus Kuwait. Im Januar hatte man dann, um den Beginn des Kriegs zu beschleunigen, die Zahl der getöteten Säuglinge bereits auf 312 erhöht, wie vor dem aussenpolitischen Ausschuss des US-Kongresses berichtet wurde. Auch Amnesty International übernahm ebenso wie der Grossteil der Medien diese Zahl ungeprüft. Präsident George Bush sen. berief sich in seiner Argumentation für einen Einsatz in Kuwait auf die Säuglings-Geschichte, die Medien wiederholten sie beständig. Am 16. Januar 1991 begann die Bombardierung um drei Uhr Morgens am Golf und 19.00 Uhr in Washington, also zur besten Sendezeit. Später stellte sich heraus, dass «Nayirah» die Tochter des kuwaitischen Botschafters in Washington und die Story eine Fälschung war, die allerdings den Beginn des Kriegs entscheidend beschleunigte und nach aussen legitimierte.

### *2.2.3 «Embedded» – Neue Strategie der Zusammenarbeit mit Journalisten im zweiten Irak-Krieg*

Der Irak-Krieg von 2003 wird wohl als erster wirklicher Live-Krieg in die Geschichte der Kriegsberichterstattung eingehen. Zahlreiche Journalisten sendeten Aufnahmen direkt vom Kriegsgeschehen. Möglich machen diese Live-Berichterstattung neuartige technische Geräte, insbesondere das Videophone. Das vier Kilogramm schwere Gerät kann zusammen mit einer kleineren Stellitenschüssel, die über das Inmar-Satellitennetz funktioniert, Live-Bilder von jedem noch so entlegenen Ort senden, ohne dass lokale Infrastruktur nötig wäre. Das Videophone lässt sich vom Zigarettenanzünder des Autos betreiben und ist bei brenzligen Situationen in wenigen Minuten verpackt.

Eine andere wesentliche Voraussetzung für die Live-Berichterstattung vom Irak-Krieg war die neue Strategie der US-Streitkräfte in der Zusammenarbeit mit Journalisten. Zum ersten Mal konnten «eingebettete» Journalisten mit Verbänden der alliierten Truppen mitfahren. Die objektive Berichterstattung von den Kampfhandlungen wurde dadurch allerdings nicht gefördert. Das hat verschiedene Gründe. Zum einen wird allgemein bezweifelt, dass Journalisten, die im Tarnanzug mit Truppen mitfahren und beispielsweise unverhofft unter feindlichen Beschuss geraten, noch unparteiisch berichten können. Zu stark ist wohl die «Verbrüderung» mit den eigenen Beschützern. Der Weg zur unfreiwilligen Heroisierung der begleiteten Soldaten ist kurz. Zum anderen können kritische Informationen von den Kommandierenden immer mit der Begründung zurückgehalten werden, sie gefährdeten die Sicherheit der Truppe.

Am unzimperlichen Umgang der US-Streitkräfte mit so genannten unilateralen, also nicht eingebetteten Journalisten (sie berichteten wiederholt von Verhaftungen, stundenlangen Verhören, etc. – einige wurden gegen ihren Willen nach Kuwait ausgeflogen) ist erkennbar, dass die Einbettung von Journalisten wohl nicht zuletzt dem Zweck ihrer Kontrolle diente. Anderseits berichteten auch einige unilaterale Journalisten, dass sie von US-Militärs aus brenzligen Situationen befreit wurden.

### *2.2.4 Pressekonferenzen und zur Verfügung gestelltes Bildmaterial*

Für Journalisten, die nicht an der Front sind, stellen die täglichen Pressekonferenzen (Briefings) der Kriegsparteien oftmals die einzige Informationsmöglichkeit dar. Diese sind aber im Allgemeinen mit Kriegsrhetorik gespickte Propaganda-Bulletins, die kaum objektive Informationen enthalten. Die USA präsentierten (erstmals im Kosovo-Krieg) meist einige Fotos oder kurze Filmsequenzen, die entweder die gezielte Zerstörung eines feindlichen Objektes mit den eigenen «Präzisionswaffen» zeigen oder die Existenz irgendwelcher feindlicher Stellungen/Waffen/etc. belegen sollen. Durch die dauerhafte Wiederholung solcher Bildsequenzen wird Unfehlbarkeit

der Präzisionswaffen suggeriert, obwohl deren Trefferquote mit ca. 50–75% erstaunlich gering ist.

Wie sich gezeigt hat, birgt diese Vorgehensweise für die USA nicht nur Vorteile. Durch die Bilder wird zwar der Glauben an die Kampfstärke der US-Truppen gestärkt, gleichzeitig wird aber auch die Illusion eines «sauberen» Krieges gefördert. Diese hat im Golfkrieg unter anderem dazu geführt, dass bereits bei geringen amerikanischen Verlusten die US-Strategie gesamthaft in Frage gestellt wurde.

Im ersten Golfkrieg wurde von so genannten Poolreportern, einer Gruppe von Journalisten der wichtigsten US-Medien, jeweils ein Journalist zu den militärischen Aktionen zugelassen, der die Informationen dann an die anderen weitergeben musste. Alle Berichte wurden vor der Veröffentlichung zensiert. So unbefriedigend eine Pool-Regelung für das Gros der Journalisten auch ist – wenn lediglich US-Journalisten zugelassen werden, entfällt überdies die meist kritischere Aussensicht der europäischen Journalisten –, es gibt unter ihnen durchaus auch Zustimmung zur Zensur, wenn es um Fragen der nationalen Sicherheit geht. Er würde alles tun, worum ihn sein Präsident bitte, bekannte beispielsweise ein CBS-Nachrichtenmoderator in der David-Letterman-Show.

Zwar hatte das Pentagon 1992 – noch unter dem Eindruck des ersten Golfkrieges – gemeinsam mit führenden US-Medien einen Pressekodex verabschiedet. Darin wird ausdrücklich festgelegt, dass die Presse auch im Kriegsfall Zugang zu den militärischen Operationen bekommen soll, solange es die Aktion nicht gefährde. Gerade diese Einschränkung erlaubt den Militärs aber die willkürliche Handhabung des Kodex.

## 2.3 Analyse der spezifischen Bedrohungslage in der Schweiz

Es ist davon auszugehen, dass Computer-Hacking resp. Angriffe auf die Informationstechnologien und Desinformation in offensiven Informationskampagnen Hand in Hand gehen.

Ein Infowar-Angriff auf Banken, Börsen und Universitäten hätte gravierende Auswirkungen auf die zivile Bevölkerung und unbeabsichtigte Folgen, nicht nur für die direkt involvierten Konfliktparteien, sondern auch für neutrale oder verbündete Nationen. Desinformationskampagnen, wie sie auch von US-Behörden innerhalb des Pentagons und der Geheimdienste erwogen werden oder wurden, können heute ungeahnte Dimensionen erlangen. Es wäre möglich, mit Hilfe von Computer-Morphingtechniken das Bild eines feindlichen Staatschefs zu kreieren, der seine Truppen darüber informiert, dass eine Feuerpause oder ein Waffenstillstand unterzeichnet wurde. Derartige Beispiele führen vor Augen, wie mit dem Mass der Abhängigkeit vieler Gesellschaftsbereiche von technischer Infrastruktur und von medialer Beeinflussung auch ihre Verletzlichkeit steigt, sei es durch vorsätzlich vorgenommene Manipulationen oder durch unverschuldete technische Defekte.

Die Auswertung des im Juni 2001 durchexerzierten Cyberkrisenszenarios «INFORMO 2001» liefert bisher kaum Antworten auf die Frage, wie die Schweizer Behörden im Verbund mit der Wirtschaft auf so genannte KASII (Krisen, ausgelöst durch Störungen der Informationsinfrastruktur) reagieren sollen. Als wichtiger Nutzen der Übung beurteilten die Teilnehmer das Networking. *«In echten Krisen kann unmittelbar von diesem Kompetenzverbund und von den persönlichen Bekanntschaften realer Nutzen gezogen werden»,* schreibt Laurent F. Carrel, Projektleiter von INFORMO. Wann genau eine solche Krise oder eine ausserordentliche Lage eintritt, ist allerdings unklar. Insbesondere der Übergang vom Störfall zur Krise bleibt umstritten. Ausserdem stellt sich die Frage nach der Definitionsmacht. Welche Stelle hat die Kompetenz, ihre Terminologie für verbindlich zu erklären?

In den Raum gestellt wird nun die Möglichkeit eines wissenschaftlichen Forschungsprogramms, das dieser Frage nachgehen soll. Ebenfalls nicht ausreichend definiert ist die Rolle des Sonderstabs, der als zentrales Gremium die strategische Führung in einer Krisensituation übernehmen soll. Zwar wird die Existenz einer solchen Körperschaft, wie sie im Juni testhalber im Einsatz gestanden hatte, von einer Mehrheit der beteiligten Akteure befürwortet, doch bleibt unklar, welchen Behörden der Sonderstab im Ernstfall beratend zur Seite stehen soll.

Im Bereich der internationalen Vernetzung wird die Frage nach einer möglichen Beteiligung der Schweiz an der Cybercrime Convention des Europarats aufgeworfen. Als wenig taugliches Instrument in ausserordentlichen Lagen werden

militärische «Information Operations» beurteilt, wie sie als ultima ratio im Rahmen des Sonderstabs vorgesehen sind. Strategieexperte und INFORMO Projektleiter Carrel sieht darin ein Relikt aus vergangenen Zeiten. *«Die Definition der ausserordentlichen Lage geht von einer funktionalen Definition aus, die nach wie vor einem mechanistischen Verständnis verhaftet ist, wie es zur Zeit des Kalten Krieges vorherrschte.»*

Insgesamt wird den militärischen Bemühungen kein gutes Zeugnis ausgestellt. Das Verteidigungsministerium VBS muss sich in diesem Zusammenhang von INFORMO-Projektleiter Carrel Intransparenz und mangelnde Koordination mit den anderen Bundesstellen vorwerfen lassen.

Im Ende November 2001 veröffentlichten Schlussbericht zum Einsatzkonzept Information Assurance werden einige konkrete Bedrohungsszenarien[12] aufgeführt:

- **Virenbefall** von PCs in der Verwaltung und in der Privatwirtschaft. Beispiel: «I Love You», «Melissa», «Ana Kournikova».

- **Denial-of-Service Attacken** auf Webserver von Privatunternehmen. Dabei werden durch einen konzentrierten Angriff die Web-Server überlastet, bspw. über eine Unmenge gleichzeitig gestarteter Mailanfragen. Als Folge davon sind die betroffenen Unternehmen einige Tage nicht im Internet erreichbar. Dies führt unter Umständen zu massiven Umsatzeinbussen und einem Imageverlust.

  Beispiel: Attacken auf verschiedene amerikanische Internet-Unternehmen (Amazon, Yahoo, Ebay, Buy.com) in der ersten Februarwoche 2000.

- **Blockierung von Alarmnummern:** Hacker dringen in das Telefonsystem der Stadtverwaltung ein und leiten die Notfallnummern auf nicht existierende Nummern um. Als Folge davon sind die Notfalldienste während Stunden nicht erreichbar.

  Beispiel: Am 15. April 1996 drangen Hacker in das Telefonsystem der N.Y.P.D. ein und blockierten die Notfallnummer 911 während 12 Stunden.

- **Fehlerhaftes Software-Update** in KKW. Beispiel: Das britische KKW «Sellafield» öffnete wegen fehlerhafter Software zur Steuerung der Strahlentüren trotz hoher Radioaktivität die Türen in den Kammern. Seither blieb das KKW abgeschaltet. Der Fehler steckte in einer neuen Softwareversion, welche die alte Software ersetzte.

- **Erpressung** eines KKW-Betreibers: Eine militante Gruppe verschafft sich Zugang zur Steuerungssoftware eines KKWs und droht mit Manipulation.

- **Logische Bombe** (legt alle durch einen elektromagnetischen Impuls elektronischen Geräte in einem bestimmten Umkreis lahm) im neuesten Pentiumchip verursacht einen flächendeckenden Ausfall wichtiger Server der Verwaltung und Wirtschaft.

  Beispiel: eine frühere Generation der Pentium-Prozessoren führte unter bestimmten Randbedingungen Divisionen inkorrekt aus.

- **Ausfall wichtiger Infrastrukturkomponenten:**

  Beispiel 1: Ausfall der Strom- oder Wasserversorgung. In Neuseeland drangen politische Aktivisten 1997 in ein Elektrizitätswerk ein und schalteten die Produktionsanlagen ab. In der Folge fiel die Stromversorgung in Auckland während einer Woche zusammen. Dies führte zu wirtschaftlichen Schäden von mehreren hundert Millionen Dollar.

  Beispiel 2: In Lewston (USA) funktionierte 1998 wegen des Ausfalls eines Rechners bis zu 30 Stunden die Wasserversorgung nicht. 40'000 Bewohner waren betroffen.

  Beispiel 3: Ausfall beim Transportwesen: bei der SBB standen 1995 zur gleichen Zeit am gleichen Tag 15 Lokomotiven still. Dieser Vorfall ist höchst wahrscheinlich auf Hacker zurückzuführen.

Die Informationskriegsführung ist für die Schweiz ein erhebliches Risiko – technologisch wie inhaltlich, bezogen auf die Führungsfähigkeit. Infolge der europaweit höchsten Informatik- und Vernetzungsdichte und der starken internationalen Verflechtung der Wirtschaft ist sie stark von funktionssicheren Datenverbindungen abhängig. Die teilweise komplexen Vernetzungen verschiedener

12 Einsatzkonzept Information Assurance, Schlussbericht vom 30. November 2001, Anhang A1.

gesellschaftlicher Bereiche haben eine hohe Verwundbarkeit zur Folge. Die Bedrohung der Schweiz reicht von massiven Beeinträchtigungen oder Störungen unserer Wirtschaft bis zur Lähmung unserer politischen und militärischen Führungsfähigkeit.

## 2.4 Ein Blick auf Vorkehrungen und Massnahmen im Ausland

### *2.4.1 USA*[13]

Interessanterweise haben die USA die Grundlagen zu ihren Vorkehrungen bezüglich Information Warfare unabhängig vom «neuen Krieg gegen den Terror» schon Jahre vor dem 11.9. 2001 gelegt, dem Datum, das so gerne als Angelpunkt aller diesbezüglichen Bemühungen gesehen wird. Am 7. Januar 2000 enthüllte US-Präsident Clinton ein Zehn-Punkte-Programm, bekannt als *«Nationalplan zum Schutz von Informationssystemen».* Die Initiativen des Weissen Hauses in Sachen defensiver und offensiver Operationen im Cyberspace beenden eine Ära siebenjähriger Forschung, Entwicklung und Lobbyaktivitäten von Think Thanks und der Blue-Ribbon-Initiative.

Offiziell wurde die Initiative zum Schutz kritischer Infrastrukturen am 15. Juli 1996 eingeleitet, als Präsident Clinton die Executive Order 13010 unterzeichnete. Diese Verordnung etablierte die *«Kommission des Präsidenten zum Schutz kritischer Infrastrukturen»* (President's Commission on Critical Infrastructure Protection – PCCIP – www.pccip.gov). Sie definierte acht Sektoren, in denen die PCCIP Sicherheitsschwachstellen untersuchen sollte. Dabei handelt es sich um Telekommunikation, Stromversorgung, Gas- und Öltransporte und -lager, Banken und Finanzen, Verkehr, Wasserversorgungssysteme, Rettungsdienste und öffentliche Verwaltung. Im Oktober 1997 veröffentlichte die PCCIP ihre Ergebnisse. Praktisch wurde fast jede der PCCIP-Empfehlungen im Nationalplan zum Schutz der Informationssysteme (National Plan for Information Systems Protection) berücksichtigt.

Die PCCIP stellte fest, dass die USA von Infrastrukturen so abhängig sind, dass die Regierung das Land durch einen *«nationalen Sicherheitsfokus»* betrachten sollte. Bei der Betrachtung der Informationsinfrastrukturen stellte die PCCIP fest, dass diese *«sehr reale und wachsende Cyber-Dimension mit der Sicherheit von Infrastrukturen verbunden ist».* Allerdings verlor die Kommission kein Wort darüber, dass der Schutz kritischer Infrastrukturen für die Vereinigten Staaten eigentlich ein zweischneidiges Schwert ist. Obwohl die Pläne zum Schutz von US-Cyberspace-Infrastrukturen vorwiegend öffentlich erstellt werden, wird die Anwendung offensiver Taktiken im Bereich von Information-Warfare gegen staatliche und nicht-staatliche Protagonisten von der NSA, der CIA und dem Verteidigungsministerium geheim gehalten.

Der PCCIP-Report und der Nationalplan empfahlen die Einrichtung neuer verwaltungsorganisatorischer Sicherheitsmassnahmen – verbunden mit erweiterten staatlichen Befugnissen. Der Veröffentlichung des PCCIP-Berichts folgten eine Reihe weiterer Verordnungen durch den Präsidenten. In Folge des PCCIP-Berichts unterzeichnete Präsident Clinton am 22. Mai 1998 zwei Weisungen (Presidential Decision Directives – PDD) – die PDD-62 (Terrorismusbekämpfung) und die PDD-63 (Schutz kritischer Infrastrukturen). Beide Weisungen sollen die kritischen Infrastrukturen der Nation vor verschiedenen Bedrohungen verteidigen, unter anderem vor «Cyberattacken» durch Computerhacker und Terroristen.

PDD-63 richtete das Büro des *«Nationalen Koordinators für Sicherheit, Schutz der Infrastruktur und Bekämpfung von Terrorismus innerhalb des Nationalen Sicherheitsrates»* ein. PDD-63 autorisierte ebenfalls die Schaffung eines *«Rates zur Sicherheit nationaler Infrastrukturen»* – bestehend aus Vertretern des privaten Sektors sowie Vertretern von Landes- und lokalen Behörden –, eines Koordinationsteams für den Nationalplan (Nationalplan Coordination - NPC), eines Büros für die Sicherheit kritischer Infrastrukturen (Critical Infrastructure Assurance Office – CIAO), einer Koordinationsgruppe zu kritischen Infrastrukturen (Critical Infrastructure Coordination Group – CICG) sowie des Nationalzentrums zum Schutz von Infrastrukturen (National Infrastructure Protection Center – NIPC) innerhalb des FBI.

Das NIPC ist befugt, die Erkenntnisse des Verteidigungsministeriums und der Geheimdienste zur Überwachung von Hacker-Aktivitäten im Internet zu verwenden. Das NIPC koordiniert zudem das InfraGuard-Programm. Dabei handelt es sich um eine Initiative zum gegenseitigen Informa-

13 Wayne Madsen 07.06.2000: http://www.heise.de/tp/deutsch/special/info/6837/1.html

tionsaustausch zwischen Regierung, privaten Firmen und akademischen Einrichtungen.

PDD-63 autorisiert ebenfalls die Schaffung von Zentren für Informationsaustausch und -analyse (Information Sharing and Analysis Centers – ISAC) im Bereich der privaten Industrie. Diese ISACs sollen Informationen zu Sicherheitsrisiken mit der Regierung austauschen. Bis heute wurden diese ISACs im Finanz-, Public-Utilities- und Computer- bzw. Mediensektor eingerichtet. Wie aus Quellen im Weissen Hauses hervorgeht, werden diese Zentren ihre Informationen mit der US-Bundesregierung über eine Netzwerkverbindung der allgemeinen Bundesverwaltung austauschen. Die Organisation wird ein staatliches Überwachungsnetzwerk für das Internet betreiben, bekannt als Federal Intrusion Detection Network oder «FIDNET».

*2.4.2 Deutschland*

In Deutschland wurde aufgrund der veränderten Gefahrenlage nach den Anschlägen vom 11. September 2001 die Struktur des Katastrophen- und Zivilschutzes grundlegend überprüft. Mit dem Ziel, die Bevölkerung im Bedarfsfall schnell und flächendeckend über Schadensfälle und Katastrophenschutzmassnahmen informieren zu können, hatte bei der Neuorganisation des Zivilschutzes in Deutschland die Einführung eines modernen bundesweiten Warnsystems höchste Priorität. Es wurde eine satellitengestützte Kommunikationsverbindung von den Zivilschutzverbindungsstellen zu den Rundfunkanstalten sowie zu den Lagezentren von Bund und Ländern geschaffen. Warnungen werden in Zukunft via Satellit an alle Lagezentren und zeitgleich an die Rundfunkanstalten abgesetzt.

Das neue Kommunikationssystem wird durch ein Nachrichtenverteilsystem abgestützt, das mehr als 650 Satellitenempfangsanlagen erreicht. Geplant ist auch der Einbezug der privaten Rundfunkanbieter in das System. Ausserdem wird in einem Feldversuch mit der Industrie ein System des Warnrufs über Funkuhren und Mobiltelefone geprüft.

Das seit 1. April 2002 neu eingerichtete «Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr» (IT-AmtBw) konzentriert die IT-Aufgaben im nachgeordneten Bereich; insgesamt geben 13 Dienststellen ihre bisherigen Zuständigkeiten im IT-Bereich dorthin ab. Neben der Realisierung dieses Vorhabens wird künftig eine IT-Gesellschaft die – bisher durch Bundeswehrangehörige oder durch Auftragsvergabe an die Industrie erbrachten – Leistungen erbringen. Geführt wird diese neu zu gründende Gesellschaft gemeinsam von der Bundeswehr und einem industriellen Partner. Diese Kooperation wird die Bundeswehr kurzfristig in die Lage versetzen, den Betrieb sicher zu stellen und zudem die erforderlichen Investitionen zu tätigen. Dabei geht es um ein Auftragsvolumen von mehr als 7 Mrd. Euro in den nächsten zehn Jahren. Zur Bewältigung seiner Aufgaben wird das IT-AmtBw in der Zielstruktur über etwa 1000 militärische und zivile Mitarbeiter verfügen. Zentrale Belange der IT-Sicherheit sowie technisch-betriebliche Aufgaben wird ein dem IT-AmtBw nachgeordnetes IT-ZentrumBw wahrnehmen.

# 3 Ein Blick auf die Grundlagen und Vorkehrungen in der Schweiz

Der Staat muss grundsätzlich im Normalfall und in ausserordentlichen Lagen eine Informationsstruktur gewährleisten, mit der zukünftigen Krisen auf allen Stufen Erfolg versprechend begegnet werden kann.

## 3.1 Sicherheitspolitischer Bericht 2000

Die Strategie für die Informationsgesellschaft Schweiz wurde vom Bundesrat am 18. Februar 1998 verabschiedet. Über ausbildungstechnische, wirtschaftliche und gesetzgeberische Massnahmen hinaus behandelt sie auch die Bereiche Sicherheit und Verfügbarkeit.

Der grundlegende und vom Parlament behandelte Sicherheitspolitische Bericht 2000 hält die Bedeutung der Informationsführung und die Notwendigkeit des Schutzes von Informationsstruktur und Bundesverwaltung klar fest.

Inhaltlich: *«Eine wahrheitsgetreue, rasche und verständliche Information ist in allen Lagen von grösster Wichtigkeit; . . . Die staatlichen Informationsorgane sorgen dafür, dass die sicherheitspolitische Entscheidungen und Massnahmen der*

*Behörden im In- und Ausland deutlich gemacht, die Bedürfnisse der Bevölkerung nach Information über Risiken und Chancen befriedigt werden und allfälliger Desinformation rechtzeitig durch lagegerechte und sachliche Information entgegengewirkt wird. Speziell in besonderen Lagen geht es darum, eine gegen die Interessen der Schweiz gerichtete fremde Informationsdominanz zu verhindern und den Anliegen unseres Landes gebührendes Gehör zu verschaffen.»*

Infrastrukturell: *«Oberstes Ziel des Bundesrates im Bereich der Sicherheit der Informatik- und Kommunikations-Infrastruktur ist es, die Entscheidungs- und Handlungsfähigkeit der Schweiz aufrechtzuerhalten und Rahmenbedingungen zu schaffen, um das Funktionieren der Informationsgesellschaft Schweiz zu gewährleisten.»*[14]

Inhaltlich ist der Auftrag dem Stab Bundesrat APF und seinem militärischen Element, dem multimedialen Informationsregiment 1 als Informationsorgan des Bundesrates in ausserordentlichen Lagen delegiert. Die APF und das Informationsregiment bestehen seit längerem, ihre Existenz wurde jüngst nicht im Rahmen der Armeereform XXI, sondern im Zeichen finanzpolitischer Knappheiten und bürokratischer Kompetenzstreitigkeiten in Frage gestellt.

Zur Frage der Informationssicherheit hat der Bundesrat die Koordinationsgruppe Informationssicherheit eingesetzt. Diese hat zunächst Grundlagenarbeit geleistet, die effektive Umsetzung ist weitgehend offen und von den Finanzmitteln abhängig.

### 3.2 Einsatzkonzept «Information Assurance»

Die zivilen (privaten) elektronischen Medien sind nach dem seit dem 1. April 1992 geltenden Radio- und Fernsehgesetz nicht mehr verpflichtet, die SRG- und damit die APF-Programme aufzuschalten. Trotzdem sind die privaten elektronischen Medien, oder mindestens ein Teil davon, nicht verpflichtet worden, ihre Sende- und Studioeinrichtungen zu schützen. Hier ist Handlungsbedarf auf konzeptioneller Ebene nötig, da einzelne private elektronische Medien über eine krisenresistente Infrastruktur verfügen, andere aber nicht.

Ende 2001 wurde der Schlussbericht zum «Einsatzkonzept Information Assurance Schweiz» veröffentlicht. Basierend auf den in diesem Bericht erläuterten Einsichten sowie auf der Übung INFORMO 2001 der Strategischen Führungsbildung wird in Ergänzung zum Sonderstab Information Assurance (SONIA) die Einrichtung einer permanenten Melde- und Analysestelle Informationssicherheit (MELANIE) angeregt. Eingebettet *«in ein enges nationales und internationales Netzwerk mit IT-Betreibern in Wirtschaft und Verwaltung und anderen Stellen mit vergleichbarem Aufgabenspektrum»*[15], soll ihre Aufgabe die Lagebeobachtung, die Analyse von Meldungen und die Alarmierung des SONIA umfassen.

Der SONIA ist als Beratungsorgan für die Bewältigung von Krisen im Bereich Informationssicherheit konzipiert. Als nicht stehende Organisation wird SONIA nur nach einem Aufgebot operativ. Um sein Funktionieren im Krisenfall sicherzustellen, wurden Infrastruktur und Führungsunterstützung benannt und Einsatzdokumentationen für mögliche Einsatzfälle erstellt. Ausserdem werden zur Gewährleistung der Einsatzbereitschaft Alarm- und reale Übungen durchgeführt. Der Aufgabenbereich von SONIA umfasst die folgenden vier Punkte[16]:

1. *Er berät den Bundesrat im Falle schwerwiegender Ereignisse im Bereich der Informationssicherheit und stellt diesem sowohl Entscheidungsgrundlagen als auch Lösungsvorschläge zur Verfügung.*

2. *Er beurteilt laufend die Lage zum Krisenverlauf und kommuniziert diese situationsgerecht an interessierte Stellen. Er stellt der Bundeskanzlei die Grundlagen für die Information der Bevölkerung zur Verfügung.*

3. *Er kann im Sinne der operativen Krisenbewältigung für die Bundesverwaltung Massnahmen in Absprache mit den für die Informationssicherheit zuständigen Stellen anordnen.*

4. *Er koordiniert die Anstrengungen der Wirtschaft (kritische Sektoren), der Bundesverwaltung sowie der Kantone und Gemeinden zur Überwindung der Krise durch Bereitstellen einer gemeinsamen Plattform.*

14 Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz, vom 7. Juni 1999 (vgl. S. 56, 57).

15 Einsatzkonzept Information Assurance, Schlussbericht vom 30. November 2001, S. 1.

16 Einsatzkonzept Information Assurance, Schlussbericht vom 30. November 2001, S. 29.

Die jährlichen Kosten von SONIA wurden auf CHF 600'000 veranschlagt. Angesichts der enormen Folgekosten eines möglichen Krisenfalls im Bereich der Informationssicherheit scheint dieser Betrag verhältnismässig tief.

### 3.3 APF und Informationsregiment

Der Stab Bundesrat Abteilung Presse und Funkspruch (Stab BR APF) wurde mitten im Zweiten Weltkrieg als Antwort auf die damaligen Herausforderungen geschaffen. Dieses bemerkenswerte Instrument ist im Verlaufe der Jahre laufend auf die Erfordernisse der Zeit ausgerichtet worden, so dass der Stab BR APF und sein militärisches Element, das Informationsregiment 1 heute ein effektives multimediales (d.h. Print, Radio, TV und Internet umfassendes) Informationsorgan des Bundesrates in ausserordentlichen Lagen darstellt.[17] Allerdings bestehen im Rahmen jüngster Entwicklungen Bedenken bezüglich Aufrechterhaltung des multimedialen Auftrages und sind bis dato die zum Einsatz gelangenden Technologien nicht «gehärtet», d.h. gegen Attacken abgesichert.

Auftragserfüllung und Einsatzgrundsätze sind wie folgt definiert:

1. Eine ausserordentliche Lage ist für den Stab BR APF dann gegeben, wenn die zivilen Medien nicht mehr in der Lage sind, ihre Informationsaufgabe zu erfüllen. Eine solche extreme Situation kann bei bewaffneten Konflikten oder mit dem Eintreten von Naturkatastrophen entstehen; sie kann auch dadurch geprägt sein, dass sich die Bevölkerung über längere Zeit im Schutzraum aufhalten muss.

2. Der Einsatz des Stabes BR APF durch den Bundesrat erfolgt auf der Basis des restriktiv gehandhabten physischen Subsidiaritätsprinzips erst, wenn das zivile Mediensystem – ganz oder teilweise – nicht mehr in der Lage ist, die Informationsbedürfnisse der Bevölkerung zu befriedigen.

3. Der Stab BR APF stellt in ausserordentlichen Lagen die Information der Öffentlichkeit sicher. Dazu gehört in erster Linie die Information über Tatsachen und Massnahmen, welche für das Überleben der Bevölkerung wichtig sind, sowie die Orientierung über die Absichten und Handlungen der zivilen und militärischen Führung.

4. Die politisch-publizistische Leitung kann vom Bundesrat für die Beratung in medienpolitischen Fragen eingesetzt werden.

5. Als publizistische Leitlinie gilt der Grundsatz der Wahrhaftigkeit. Nur mit einer glaubwürdigen Informationspolitik kann das Vertrauen der Bevölkerung in die politische und militärische Führung aufrechterhalten werden. Die durch den Stab BR APF verbreiteten Informationen müssen darüber hinaus aktuell, sachgerecht und verständlich sein. Im Zweifelsfall oder wenn übergeordnete Interessen gefährdet werden könnten, wird auf eine Publikation verzichtet. Amtliche Texte und Verlautbarungen werden im Wortlaut wiedergegeben.

APF und Informationsregiment benötigen drei Voraussetzungen, um den Auftrag zu erfüllen:

1. **Strategische Positionierung:** Um den Zugang und die unmittelbar exekutiv wirksam werdende Funktion erfüllen zu können, ist eine dem umfassenden Auftrag entsprechende organisatorische Einordnung ins Sicherheitsdispositiv auf strategischer Stufe mit Immediatvortrag vorzusehen.

2. **Milizressourcen:** Um den Auftrag multimedial erfüllen zu können, sind Stab und Informationsregiment auf in der Verwaltung nicht angesiedeltes und im Rahmen der spezifischen Ausbildungen der Armee resp. anderer Sicherheitsinstrumente nicht bereitgestelltes Knowhow angewiesen. Primär die inhaltliche (d.h. journalistisch-redaktionelle) Kompetenz, sekundär auch die technologische Personalkomponente müssen aus finanziellen Gründen grossmehrheitlich aus der Miliz kommen. Outsourcing-Lösungen – etwa für einzelne Leistungskomponenten wie Television bei der SRG – berauben den Staat der Redundanz und sind nicht krisentauglich.

3. **Finanzen:** Die «Härtung» und Sicherung unserer zentralen Informationstechnologien gegen Attacken ist unabdingbar. Ohne entsprechende Investitionen in diesem Bereich werden alle anderen Vorbereitungen Makulatur.

---

17 Der Auftrag der APF und des Informationsregiment 1 leiten sich aus dem Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz, vom 7. Juni 1999 ab (vgl. S. 56 ff).

## 4 Fazit: Sieben Thesen

In der Schweizer Sicherheitspolitik klaffen bezüglich Bedeutung der behördlichen Information und Kommunikation in ausserordentlichen Lagen Theorie und Praxis auseinander: Während die Gefährdungen weitgehend erkannt und auch die nötigen Gegenmassnahmen im Prinzip bekannt sind, ist nicht nur die Realität, sondern vor allem die Zukunftsperspektive ernüchternd.

So ist man einerseits daran, das Informationsinstrument des Bundesrates für ausserordentliche Lagen in Form des Informationsregimentes und des Stabes BR APF zu demontieren oder reduzieren. Kompetenzgerangel und bürokratische Eifersüchteleien spielen dabei eine ebenso grosse Rolle, wie – mangels richtiger Prioritätensetzung – als «vorgeschoben» zu wertende Finanzengpässe. Insgesamt fehlt es an der Fähigkeit zur Priorisierung unserer Mittel angesichts moderner Gefährdungen und ihrer Eintretenswahrscheinlichkeit.

Gänzlich ungenügend ist der Sektor der Informationssicherheit in Bezug auf den Stand der Umsetzung als richtig und wichtig erkannter konkreter Massnahmen. Während Analyse und Massnahmen bekannt sind, fehlt in der Umsetzung bisher ein sichtbarer Fortschritt.

Vor diesem Hintergrund rechtfertigt es sich deshalb, folgende 7 Thesen zu formulieren:

**These 1: Informationsfaktor wird Erfolgsschlüssel in künftigen Konflikten**
**Die Bedeutung des Faktors Information in den machtpolitischen Auseinandersetzungen nimmt in der Informationsgesellschaft zu und nicht ab. Gerade die offene demokratische Gesellschaft ist in besonderem Masse gefährdet.**

**These 2: Multimediale Bedrohung**
**Information Warfare geschieht heute grenzüberschreitend, vernetzt und multimedial (Print, Radio, TV, Internet etc.). Auch demokratische Staaten setzen seine Mittel umfassend ein.**

**These 3: Bedeutung der Bedrohung unterschätzt**
**Das Bewusstsein für die gewachsene Bedeutung des Faktors Information ist trotz guten Grundlagen unserer Sicherheitspolitik im Bereich der Behörden und der Verwaltung in abnehmendem Masse vorhanden. Für die Sicherheit der Schweiz ist ein adäquates Instrumentarium im Bereich Sicherstellung der Informationsführung in ausserordentlichen Lagen bedeutsamer, als eine Kampfbrigade mehr oder weniger.**

**These 4: Informationsführung in a.o. Lagen von strategischer Bedeutung**
**Als Mittel zur Informationsführung in ausserordentlichen Lagen ist Führungsupport von strategischer Bedeutung. Sie gehört in der Einsatzhierarchie auf Stufe Exekutive und nicht in ein Bundesamt. Zur Nutzung von Synergien optimal ist die Ansiedlung im VBS, das zunehmend als umfassendes Sicherheitsdepartement funktionieren muss.**

**These 5: Ohne Instrumente keine aktive Führung**
**Behörden und Militärführung müssen nicht nur über gute Einsichten, sondern auch über entsprechend ausgerüstete und alimentierte Instrumente und Infrastrukturen verfügen, wenn sie im modernen Geschehen eine Chance haben wollen, ihre Rolle aktiv spielen zu können.**

**These 6: Multimediale Bedrohung – multimediale Abwehr**
**Der heutigen Bedeutung von Information und Kommunikation in ausserordentlichen Lagen sind nur multimediale Instrumente (umfasst Print und elektronische Medien) angemessen. Der Einsatz der Info Op in allen modernen Konflikten zeigt die Nutzung aller Medien im Verbund.**

**These 7: Aufrechterhaltung von Milizkompetenz**
**Die Verfügbarkeit einer ausreichenden multimedialen Milizkompetenz ist zu erhalten. Ein Aufbau umfassender professioneller Strukturen ist aus publizistischer Sicht staatspolitisch fragwürdig und finanzpolitisch untragbar. Ein Zukauf von Kompetenz nur im Krisenfall ist unrealistisch und nicht krisenresistent.**