Gerfried Stocker
Information.Macht.Krieg

"Immer wenn ich eine Eisenbahn sehe, schaue ich mich nach einer Republik um."

Ralph Waldo Emerson

In keinem Bereich des zivilen Lebens gilt das Sprichwort vom "Krieg als Vater aller Dinge" so unangefochten wie in der digitalen Informationstechnologie, deren wichtigste Protagonisten — Computer und Internet — unmittelbar der Hexenküche des Militärs entsprungen sind. Kaum ein anderer Bereich hat sich in der Dynamik seiner Entwicklung aber auch dermaßen verselbständigt und ist in der strategischen Allianz von Militärforschung, Unterhaltungsindustrie und globalem Finanzmarkt zur eigentlichen Zivilisationsdynamik geworden. Eine Entwicklung, die darüber hinaus ein enormes Potential zur Organisation von Überwachung und Kontrolle vom militärischen in den zivilen Bereich, den sogenannten Consumer-Markt, überführt hat.

Unser Verständnis von Krieg als episodischer Ausbruch bilateraler Feindlichkeiten hat sich durch die unaufhörlichen Anstrengungen, das sogenannte Gleichgewicht der Abschreckung zu balancieren, geändert. Es wurde auf einen kalten Krieg als permanente Simulation projiziert; Krieg hatte sich zu einem logistischen Manöver oder, wie Paul Virilio es 1983 nannte, zu einem "reinen Krieg" gewandelt. Doch die infolge des Zerfalls des Ostblocks in Europa ausgebrochenen ganz realen Kriege nationalstaatlicher Prägung, die man für die westliche Welt schon so gerne zur Vergangenheit gezählt hätte, haben uns neu sensibilisiert und darauf aufmerksam gemacht, daß die Zukunft des Krieges seine Vergangenheit nicht auslöschen werde.

Von der Entwicklung militärischer Informatik im englischen Bletchley Park, wo man den Zweiten Weltkrieg durch das Knacken der deutschen Verschlüsselungs-Codes entschied, über die Forschungslabors des Kalten Krieges am MIT, wo im Auftrag der US Air Force mit SAGE (Semi-Automatic Ground Environment) das erste vernetzte Computersystem entwickelt wurde, bis zu Ronald Reagans SDI-Starwars-Programm, das allein durch seine vorgeblichen Ziele und Erfolge die Sowjetunion volkswirtschaftlich in die Knie zwang — das technowissenschaftliche Netz von Militär, Wissenschaft und Rüstungsindustrie hat dem Begriff von der Macht des Wissens in unserem Jahrhundert eine neue Dimension verliehen.

Von der politischen Rolle der Gazetten und Pamphlete in der Französischen Revolution über die Beschleunigung der Geopolitik durch die elektrische Telegraphie vor dem Ersten Weltkrieg[1] bis zum ersten Radio-Wahlkampf bei den US-Präsidentschaftswahlen 1920 zeichnet sich in der Parallelität massenmedialer und militärindustrieller Entwicklungslinien ein unübersehbares Charakteristikum der Moderne ab. Eine Koinzidenz, die in die historische Gemeinsamkeit der Entwicklung von Atombombe und Computer mündet und in der bedeutungsvollen Synergie von zerstörerischer Energie und Information den Grundstein für die strategische Macht der neuen Waffengattung Informatik legt.

Dem Fall des Eisernen Vorhangs, dem Golfkrieg von 1991 bzw. der medialen Verwirklichung seiner Ziele und der Entwicklung des Internet — vom militärisch-wissenschaftlichen Nachrichtensystem zur fashionablen Lieblingstechnologie eines neuen amerikanischen und mittlerweile auch europäischen Bildungsbürgertums —, ist ungeachtet der weitgehend ausständigen Analysen eine historische Ereignishaftigkeit zu bescheinigen, in deren Gefolge sich die Welt auch für die Militärstrategen grundlegend geändert hat: Im Juni 1995

graduierten die ersten 16 "InfoWar Officers" — speziell für die Verteidigung gegen Computerattacken, für den Einsatz von Virtual Reality in der Schlacht- und Manöverplanung und die Infiltration feindlicher Computeranlagen ausgebildet — an der National Defense University in Washington.

InfoWar als Konzept, das so weit über die Formen traditioneller Kriegsführung hinausgeht, daß diese heute noch als rein zivil identifiziert würden, wird natürlich auch weiterhin als militärische Option gehandelt, wobei die Erscheinungsformen der Kriegsführung sich allerdings radikal von den bekannten Manifestationen unterscheiden würden.

Information Warfare bliebe ohne sicht- und definierbare Fronten, ohne geographisch lokalisierbare Kampfhandlungen, an deren Stelle würden überall gleichzeitig Duelle um die Informationskontrolle treten. Der Krieg würde nicht in martialischer Gestalt erscheinen, weil er aufgrund der Zersplitterung in viele kleine Einheiten und der Verteilung auf alle gesellschaftlichen Bereiche unsichtbar, un(be)greifbar wäre. Ebenso würde die Trennlinie zwischen Angriff und Verteidigung noch stärker verschwimmen, als dies bereits in der Nuklear-Ära des Kalten Krieg geschehen war.

In der InfoWar-Politik geht es nicht mehr nur um Sieg oder Niederlage. Oft wird es vorteilhafter sein, einfach nicht zu verlieren bzw. zu verhindern, daß der andere gewinnt. Es wird sogar zunehmend wichtiger werden, zu verhindern, daß der andere, der ja Geschäfts- und Handelspartner ist, komplett ausgeschaltet wird, da dessen billige, aber hochqualifizierte Arbeitskräfte — wie etwa im Falle Indiens als Major Player im Software-Business — weltweit Softwareentwicklung und Datenverarbeitung für Airlines, Banken und auch Regierungseinrichtungen erledigen.

Nicht-staatliche, sehr oft transnationale Organisationen und Wirtschaftskonglomerate werden eine wichtigere Rolle spielen als staatliche Regierungen; zu erkennen, welche Allianzen existieren — wer unterstützt wen? wer bedroht wen? — wird immer schwieriger. Außerdem müßte mit einer Vielzahl von kleinen, subtil penetrierenden Aktivitäten gerechnet werden, die infolge ihres heterogenen Auftretens, ihrer multiplen Morphologie nicht bestimmbar sein würden, womit auch auf erfolgreiche Weise alle Bestimmungen der UNO, alle völkerrechtlichen Konventionen und Ächtungen unterlaufen würden — eine eminente Herausforderung für die internationale Staatengemeinschaft.

Das Projekt InfoWar forciert jedoch nicht nur die diskreten Interventionen, es inspiriert unter demselben Titel auch die Hoffnungen der Waffenschmiede.

Where Do You Want to Fight Today …

Die Visionen von der posthumanen Menschmaschine erhalten in der Planung für die "Force 21" (die Armee des 21. Jahrhunderts) mit dem 21CLW (21th Century Land Warrior) — dessen Prototypen aussehen, als wären sie gerade einem Computer-Baller-Spiel entsprungen — neue Nahrung, und stehen ganz in der Tradition der SiFi-Stories aus den fünfziger Jahren, die suggerierten, daß die Kontamination mit geheimnisvollen Formen radioaktiver Strahlung zu unschlagbaren Mutanten führen könnte. (Eine kaum zufällige Analogie zu den Versuchen, die Militärs in Ost und West mit ihren Soldaten in der frühen Phase der Atomtests angestellt haben.)

Mittels "Augmented Reality" (einer Technologie zur computergestützten Verstärkung und Steigerung der Sinneswahrnehmung und physischer Fähigkeiten) wird der Soldat in eine

wandelnde Kommandozentrale verwandelt, bei deren Konzeption man sich allerdings noch uneins ist, ob sie sich selbst kontrollieren oder doch eher als ferngesteuerte Kampfmaschine funktionieren soll. Auf jeden Fall ist er mit Körpersensoren ausgestattet, die im Falle einer Verletzung den in sicherer Entfernung agierenden Kommandeuren genau darüber Bescheid geben, wie schwer die Verwundung ist und ob sich das Risiko einer Bergung noch lohnt.

Im "War after Next" (welchen haben wir denn inzwischen zu erwarten, möchte man ängstlich fragen) soll dieses moralische Dilemma gelöst sein. Er soll keine blutgetränkten Schlachtfelder mehr kennen und auch keine Irrtümer, in deren Folge eigene Soldaten die tragischerweise "definitely at the wrong place at the wrong time"[2] sind, von eigenen Raketen zerfetzt werden: Die Lösung verspricht man sich nicht nur von endgültig kybernetischen Robot-Soldiers, sondern mehr noch vom Einsatz künstlicher Intelligenz, also von Artificial-Live-Algorithmen, an den Schalthebeln der Kanonen und Raketen, die natürlich trotz aller Euphorie über "Smart and Non Lethal Weapons" nicht aus dem Repertoire der Kriegsplaner verschwinden.

Non Lethal Weapons — die laut John B. Alexander (Abteilungsleiter in Los Alamos) so genannt wurden, "weil kein anderer Begriff einen solch starken Eindruck machte" — gehören zu den großen Geheimnissen der US-Rüstungsforschung; sie sind "America's gift to warfare", so Admiral William Owens, Vice Chairman of the Joint Chiefs of Staff.[3]

Blendlaser, chemische und biologische Stoffe, die den Gegner und/oder sein Material kampfunfähig machen sollen, noch bevor er eigentlich weiß, daß er kämpfen sollte, elektromagnetische Bomben, die durch hochenergetische Ausstöße elektromagnetischer Strahlung jedes elektronische Gerät in weitem Umkreis zerstören und wie ein gigantischer Mikrowellenherd jedes Lebewesen, das sich in unmittelbarer Nähe aufhält, einfach grillen würde. Oder speziell gezüchtete Microben, die wahlweise elektrische Leiterbahnen oder deren Isoliermaterial ganz einfach auffressen würden.

"Commando Solo" heißt eine schon 1995 vorgestellte Infowaffe des Pentagon für ein weiteres Hoffnungsfeld des Information Warfare, der psychologischen Kriegsführung und Propaganda (PsyOps): In der Umkehrung der Funktion von Spionageflugzeugen und -satelliten, die versuchen, Informationen zu gewinnen, geht es darum, gezielte Falschinformationen, also manipulierte Daten auszustreuen: Ein 70 Mio US$ teures Flugzeug mit einer elfköpfigen Besatzung und modernster Gerätschaft ist unterwegs, um Radio und TV eines Landes zu stören und beliebige Frequenzen mit eigenen Berichten zu besetzen.

Gerüchten zufolge, hatte man schon während des Golfkriegs mit dem Gedanken gespielt, Saddam Hussein im Computer nachzubauen und ihn mit Whiskyglas und Schinkensandwich essend auf irakischen TV-Frequenzen auszustrahlen. Vielleicht ein weiteres Indiz für die Verbindung zwischen Unterhaltungsindustrie und Militärtechnologie. Es scheint ohnedies, daß nach dem Ende des Kalten Kriegs Hollywood, Nintendo und Playstations der Rüstungsforschung (vor allem im Bereich von Computersimulation und Virtual Reality) den Rang als Leitindustrie des IT-Bereichs abgelaufen haben.

Die informatische Automatisierung des Krieges durch elektronisch erzeugte Blindheit und Lähmung wird den Schrecken des gesellschaftlich sanktionierten, kriegerischen Tötens nicht schmälern. Der Begriff vom "humanen Krieg" mag vielleicht "starken Eindruck machen", glaubwürdig ist er mit Sicherheit nicht.

Information and Business have no Front-Line

Im Unterschied zur militärischen Vergangenheit (der auch der Golfkrieg schon während seines Verlaufs angehörte), in der Technologie als kampfwertsteigerndes Werkzeug zum Einsatz kam, ist heute die moderne Informationsinfrastruktur als wichtigstes Rückgrat transnationaler Wirtschaftssysteme nicht nur das bevorzugte Ziel potentieller Aggression, sie ist durch die dem Computer immanente Fähigkeit, Intelligenz zu automatisieren, also Medium und Message zugleich zu sein, Waffe und Schlachtfeld in einem geworden.

Immer stärker kumuliert entscheidendes strategisches Wissen nicht mehr einfach in den Köpfen von Führungskräften, sondern wird — über enzyklopädische Datenbanken hinaus — vor allem als algorithmische Datenverarbeitung und -auswertung in Computersysteme implementiert und zu autonomen Entscheidungsstrukturen vernetzt. In weiterer Folge ist nicht mehr die Zerstörung und Eliminierung das strategische Ziel, sondern die Übernahme bzw. die Kontrolle des Wissens der anderen, da die Zerstörung angesichts des transnationalen Verflechtung der Wirtschaft nicht mehr länger verträglich wäre. Auch wenn bislang der Verzicht auf einen offensiven InfoWar noch in der Angst vor einem konventionellen Gegenschlag gründet — z. B. ist es Rußlands offizielle Position, eine Attacke gegen seine Informationsstrukturen thermonuklear beantworten zu wollen —, so ist doch schon abzusehen, daß vor allem die US-amerikanische Industrie, deren internationaler Erfolg zum überwiegenden Teil auf dem Software-Export beruht (Microsoft, Hollywood, aber auch Coca Cola und McDonalds, die ja eigentlich auch nur Software in Form patentierter Rezepte und geschützter Trademarks exportieren), absolut kein Interesse an der nachhaltigen Zerstörung globaler Informationsinfrastrukturen haben würde — von der Abhängigkeit des globalen Finanzmarktes vom Funktionieren seiner Netzwerke ganz zu schweigen. In diesem Zusammenhang wird auch verständlich, daß die wichtigste Basis für die Normalisierung der Beziehungen zwischen den USA und China nicht die Umsetzung internationaler Menschenrechts-Standards war, sondern das Zugeständnis Chinas, mit der industriellen Software-Piraterie Schluß zu machen.

InfoWar ist somit nicht nur eine Angelegenheit der Militärs im Cyberspace, sondern vielmehr eine immanente Erscheinung unserer Gesellschaft, deren Motor Technologien sind, die aus dem militärischen Zusammenhang entwickelt wurden. InfoWar ist eine Frage der zunehmenden Emanzipation des zivilen Bereichs — "vote with your modem …"; eine Frage des Wissens und der Wahrnehmung der Welt.

InfoWar steht für den Umgang mit Macht in einer Mediengesellschaft, in der Propaganda und Wahrnehmungsmanipulation technologische Perfektion erreicht haben, für " … die Entwicklungen von technischen und elektronischen Mitteln zur politischen Kontrolle, insbesondere Überwachungs- und Identifizierungstechnologien, Sammeln und Speichern von Daten, nicht-tödliche Waffen, Technologien für die Gefängnisse, zur Exekution und zur Folter" sowie für den "Trend einer zunehmenden Militarisierung der Polizeitechnologien und der Paramilitarisierung der Militärtechnologien, der weltweit auf eine Konvergenz der Technologien zur politischen Kontrolle zuläuft".[4]

Und während wir Zivilisten die apologetischen oder ängstlichen Kommentare über das Ausmaß der Änderungen und Neuerungen im zivilen oder, wie es zutreffender heißt, im Consumer-Bereich nur zu gut kennen, kann mit Staunen und auch ein wenig Schadenfreude beobachtet werden, wie die Militärs nicht mehr an sich halten können und in vollmundiger Euphorie von den neuen Kampfwertsteigerungen sprechen und sich gleichzeitig bis ins Mark vor der plötzlichen Verwundbarkeit der nationalen Sicherheit fürchten.

Die internationale Bande der Geheimdienste und Spionage-Organisationen, der Zauberlehrlinge aus allen Kreisen von Militär, Secret Services, Forschung und Wirtschaft, scheint von massiven Alpträumen geplagt zu sein, daß ihre gewaltigen Überwachungsnetze dem Feind in die Hände fallen könnten. Da der Feind seit dem Fall der Sowjetunion und der wirtschaftlichen Öffnung Chinas verschwunden ist, muß er natürlich neu erfunden werden. Was eignet sich da besser als das Internet?

Centralize Strategically, but Decentralize Tactically

Das Arpanet, konzipiert als Garantie für die Unverwundbarkeit der militärischen Kommando- und Kontrollfunktionen im Falle eines Atomschlags, hat sich durch die öffentliche zivile Nutzung als Internet in das für die Militärs alptraumhafte Gegenteil verwandelt. Auch wenn sich die ursprünglichen Visionen und Hoffnungen auf ein demokratisches Globales Dorf mittlerweile als illusorisch herausgestellt haben, zeichnet sich eine neue Kategorie von Öffentlichkeit, eine neue Dimension des Zivilen ab.

Die eigentliche Gefahr von Hackerattacken und Cyberterroristen in den USA liegt ja nicht in der ohnehin sehr unwahrscheinlichen Möglichkeit einer großflächigen Zerstörung oder Sabotage, sondern in den Auswirkungen einiger weniger, dafür spektakulärer Anschläge auf die amerikanische Medienöffentlichkeit mit Konsequenzen im Entscheidungs-Spielraum der amerikanischen Politik.

Welchen Hintergrund haben die beschworenen Bedrohungspotentiale? Wie real ist die Gefahr, daß einige Hacker im Auftrag der guten alten Feinde der USA (wen wundert es, daß die Liste der Länder, denen die US-Militär Experten großes Cyber-Zerstörungspotential zuordnen, von Lybien angeführt wird?) diese in ein öffentliches Chaos stürzen könnten? Oder wird lediglich Stimmungsmache betrieben? Eine naheliegende Vermutung angesichts plakativer Rückgriffe auf die US-Geschichte des Zweiten Weltkriegs, wenn die Bedrohung zum "Elektronischen Pearl Harbor" wird und angestrengte Forschungs- und Entwicklungsoffensiven "Manhattan Cyber Project"[5] heißen.

Die Hysterie um neue Feindbilder könnte unterschiedlich motiviert sein. Zum einen ist das Rennen zwischen den Lobbies der eher traditionellen Rüstungsindustrie und der immer mächtiger werdenden Computer- und Softwarebranche um die Zuteilungen der Mittel aus den Forschungs- und Verteidigungsetats durch den Kongreß voll im Gange. Im Vergleich zu den guten alten Zeiten des Cold War bzw. zu den Mitteln, die konventionelle Rüstungstechnologie nach wie vor verschlingt, sind die direkten Investitionen in die Entwicklung von Cyber- und Netwar verschwindend gering. Zwar entfallen in den US bereits seit einigen Jahren mehr als 50 Prozent der Baukosten von Rüstungsgütern auf elektronische Komponenten, doch handelt es sich dabei um primär konventionelle Waffensysteme, deren Effizienz durch den Einsatz elektronischer Systeme verbessert wird. So belaufen sich die Kosten zur Herstellung eines Tarnkappenbombers auf 1 Milliarde US$, wogegen für die Entwicklung des neuen Supercomputers (IBMs Nachfolger von Deep Blue) zur Kernwaffensimulation gerade einmal ein Budget von 500 Millionen US$ genehmigt wurde.

Zum anderen hat man aus den Mißerfolgen bei den Versuchen, staatliche Kontroll- und Regulierungsmaßnahmen in den digitalen Kommunikationsnetzen zu setzen (Clipperchip, CDA), gelernt, daß nur durch eine massive Trendwende in der öffentlichen Meinung die Einführung eines "Key Escrow" — der "digitalen Hundemarke" für alle Staatsbürger, wie die erbitterten Gegner eines staatlich kontrollierten Kryptografiesystems dies nennen — durchzusetzen sein wird.

Die enormen wirtschaftlichen Potentiale des Internet, das Wissen darum, daß die Hegemonie der amerikanischen Wirtschaft und damit der amerikanischen Kultur auf lange Sicht nur durch eine Vormachtstellung im Internet gewährleistet werden kann, haben dieses Medium ins Zentrum des wirtschaftlichen, politischen und militärischen Interesses gerückt. Da Information zur wichtigsten Ressource des Wirtschaftswachstums geworden ist und Software zunehmend entscheidendere Profite als Hardware bringt, ist das Internet der primäre Austragungsort des globalen Wettbewerbs geworden und bedarf aus dieser Sicht dringend des ordnenden Eingriffs. Erst wenn Sicherheit und Ordnung hinlänglich etabliert sind, werden die großen Investoren den Pionieren des Digital Goldrush folgen und ihre Territorien besetzen.

Für diese Strategie findet man ein Vorbild in der jüngeren Geschichte: In den Fünfziger Jahren, als sich das gewinnbringende Export-Potential des US-Kinos, mit Hollywood als erstem gigantischen amerikanischen Software-Produzenten, abzeichnete, und als deutlich wurde, welchen Einfluß es auf die Öffentlichkeit, welches Potential es hinsichtlich kultureller Hegemonialansprüche zu entfalten vermag, begann mit dem Feindbild des Kommunismus als Rechtfertigung eine methodische Verfolgung vor allem des intellektuellen Umfelds von Hollywood. Diese Verfolgung hatte auf die künstlerische Entwicklung Hollywoods zweifellos bedauerlichen Einfluß gehabt, aber das zwar nicht mehr neue, doch als internationaler Wirtschaftsfaktor neu entstehende Medium Film für das große Business erst brauchbar gemacht. Egal welcher Weltanschauung folgend man diese Entwicklung bewertet, ob als kulturellen Imperialismus oder als wesentlichen Beitrag zu einer globalen Kultur, die Gewinner sind ganz klar auszumachen.

Ebenso klar ist die Analogie zu den Bestrebungen, mit den "Cyberterroristen im lybischen Auftrag" und dem Image des Hacker als verbrecherischer Outlaw ein neues Feindbild in die Öffentlichkeit zu projizieren, auf daß sie die einschneidenden Maßnahmen zur Kontrolle und Regulierung des Internet und damit zur Beschränkung der privaten, individuellen Rechte im digitalen Raum sanktioniere. Daß auch innerhalb der EU Maßnahmen zur Einführung von Public Key Encryption vorgesehen sind, um das digitale Geschäft (digital commerce) endlich in Schwung zu bringen, kommt keinesfalls überraschend. Denn eines ist gewiß, ohne nachvollziehbare Identifizierungsmöglichkeit für Käufer und Verkäufer werden im Internet keine großen Geschäfte gemacht werden. Das Konzept des Eigentums ist auch im virtuellen Raum mit dem Konzept der Idenfizierbarkeit des Eigentümers verknüpft.

Derzeit stoßen solche Bestrebungen noch auf Widerspruch. Das amerikanische Bürgerrechtsverständnis ist in Form von Vereinigungen wie EFF (Electronic Frontier Foundation), die für die neue Öffentlichkeit der virtuellen Räume plädieren, eine starke Vertretung, und seitens der Industrie hat sich vor allem außerhalb der USA massiver Widerstand gegen die Implementierung von Verschlüsselungssystemen formiert, die jederzeit z. B. von amerikanischen Regierungsdiensten geknackt werden können.

The Innocent have Nothing to Fear

In Europa ist das Problembewußtsein der Politik wie auch der Öffentlichkeit für diese Fragen der Informationsgesellschaft kaum ausgeprägt und kommt vor allem reichlich spät. So wurde die Ausarbeitung von Konzepten zur Regulierung des Internet bisher Experten der Industrie und der Staatssicherheit überlassen. Welche Auswirkungen dies auf die zivilen Bereiche unserer Gesellschaft, auf die Wahrung der Privatsphäre der Bürger haben wird, ist erst vor wenigen Monaten durch Medienberichte über die Speicherung und Auswertung der Logfiles von Mobil-Telefon-Betreibern sowie durch die endlich erfolgte Bestätigung der Existenz des Echelon-Systems (siehe) öffentlich geworden.

Bereits seit 1991 arbeiten europäische Sicherheitsbeamte — mehr oder weniger unter Ausschluß der Öffentlichkeit, beraten von Experten des FBI und der US Drug Enforcement Administration — an der Überwachung bestehender und zukünftiger Daten- und Kommunikationsnetze. In einem "Memorandum of Understanding concerning the lawful interception of telecommunications" (ENFOPOL 112, 10037/95), wurde die gemeinsame Vorgangsweise festgehalten.[6]

Beispielsweise geht es dabei um die Vernetzung der derzeit europaweit in Aufbau befindlichen sicherheitspolizeilichen Datenbanken, wobei "nicht so sehr der Nachweis der Schuld des Täters einer individuellen strafbaren Handlung, sondern die Vorsorge für die Verfolgung zukünftiger Straftaten, somit Strafverfolgung im weiteren Sinn (antizipierte Strafverfolgung)" im Zentrum der Absichten steht.

Im Hintergrund dieser Initiative steht die Einsicht, daß durch die Liberalisierung des Telekommunikations-Marktes die bisher geübten Kontroll- und Überwachunspraktiken wirkungslos bzw. verunmöglicht werden. Als unbedingt notwendig erachtet wird daher die Verankerung von Abhörmethoden und -techniken in den Grundgesetzen und die Verpflichtung für private Kommunikations- anbieter, ihre Systeme im Hinblick auf staatliche Abhörmaßnahmen zu adaptieren. Damit ist unter anderem die Installierung von Wordscannern und eigenen permanenten Leitungsanschlüssen gemeint, welche die Überwachung auch aus der Ferne gewährleisten. Allenthalben, auch in Österreich, erfolgt die Finanzierung der entsprechenden Einrichtungen auf Kosten der Telekom-Provider und damit zu Lasten der Nutzungsgebühren …

In Ländern, die sich diese Bedingungen zu akzeptieren weigern, kann die Überwachung gegen den Willen erfolgen, da die Abhörtechnik bereits in den ausgelieferten Kommunikationssystemen installiert ist. So etwa ermöglicht es die ISDN-Technologie, jedes Telefon unbemerkt durch Fernsteuerung zu aktivieren und somit zu einer Abhörwanze umzufunktionieren.[7]

Das britische Forschungsinstitut Statewatch berichtet über Vereinbarungen zwischen den EU-Staaten über die legistischen Voraussetzungen für den globalen Lauschangriff.[8]

In diesem Bericht wird darauf hingewiesen, daß nicht nur Telefon-Stammdaten und Gesprächsvermittlungs- und Inhaltsdaten aufgezeichnet werden sollen, sondern auch die Bewegungsdaten des Teilnehmers — auch wenn kein Telefongespräch geführt werden sollte.

[…] Daß "weder das Abhörziel noch eine andere Person Hinweise darauf erhält, daß an den Kommunikationssystemen Veränderungen vorgenommen wurden, um den Abhörauftrag vorzunehmen […] und darüber Stillschweigen zu bewahren ist, wer und wie öffentlich abgehört wurde sowie die Technik und Methode, mit welcher abgehört wurde" (Quelle lt. Statewatch: "Memorandum of Understanding concerning the lawful interception of telecommunications", Enfopol 112, 10037/95, Limite, Brussels, 25.11.95)

Dieses Memorandum wurde laut Statewatch am 23. November 1995 von allen 15 EU-Mitgliedsstaaten durch die jeweiligen Vertreter in Form der Justiz- und Innenminister unterschrieben — auch von den Vertretern Österreichs!

Weiters faßt der Bericht die rechtlichen Grundlagen zur Überwachung in den Mitgliedsländern zusammen: Deutschland, Österreich, Dänemark, Luxemburg, Spanien und Portugal können einfach ("can simply") durch Änderungen im Strafrecht die volle Überwachung realisieren, während Belgien, Frankreich, Großbritannien, Irland, Griechenland, Norwegen und Schweden gänzlich neue Gesetze bzw. eine Kombination aus beiden benötigen.

In den einzelnen Ländern seien bereits Diskussionen im Gange, welch "große Vorteile" die Polizei habe, wenn "sie bereits Personen überwachen könne, die unter Verdacht krimineller Aktivitäten stehen." Der Bericht verweist auch explizit auf Österreich, wo bereits ein einfacher Antrag auf Telefonabhörung die Eröffnung eines Untersuchungsverfahrens einleitet. (Quelle: "Report on the national laws regarding the questionaries on phone tapping", Enfopol 15, 4354/2/95 REV2, Restricted, 13.11.95)[9]

Some Numbers Beat No Numbers Anytime

Nun ist die Überwachung und Bespitzelung der Kommunikation nicht neu und wohl untrennbar mit deren technischer Entwicklung verbunden.

1786 hatte eine geheime Instruktion Kaiser Joseph II die Statthalter der österreichischen Erblande darauf hingewiesen, daß es dienlich sei, den Betrieb von sogenannten Kleinen Posten und ihren Briefkästen solchen Personen in die Hände zu spielen, von deren Rechtschaffenheit und Abhänglicheit die Polizei versichert wäre. […] und auch in Paris warb 1759 der Chef des Pariser Rechnungshofes für die Vorteile der "petite poste" mit dem Argument, daß die Polizei mit der Kleinen Post erstmals ein Mittel besäße, um all die Adressen von den Leuten zu ermitteln.[10]

Doch während Einrichtungen der Staatssicherheit und des Militärs seit jeher danach trachteten, zu wissen, was der andere weiß, und das Gegenteil zu verhindern, ist in Industrie und Wirtschaft das Konzept von Spionage und Gegenspionage erst im Zuge des Zweiten Weltkriegs und der anschließenden Rückkehr der Experten aus der Kriegs-Intelligence in die Wirtschaft entstanden. (Die Schwerindustrie des 19. Jahrhunderts hatte noch kaum ein Bewußtsein über die strategische Bedeutung von Information über das Wissen der Kokurrenz entwickelt.)

Die Übernahme von Generalstabs- und Spionagetechniken in die Unternehmensführung hat diese gewissermaßen militarisiert und so das Konzept des "Reverse Engineering" als industrielles Korrelat der militärischen Feindspionage in die Informationstechnologie eingeführt.

In besonderer Weise wurde Reverse Engineering zu einem Element des kalten Krieges, als man in der UdSSR, aber vor allem in Bulgarien begonnen hatte, Computerchips aus dem Westen nachzubauen. Ganze Hochschulen wurden gegründet, um ein Heer von Wissenschaftern und Technikern auszubilden, die ins Land geschmuggelte US-PCs zerlegten und analysierten, um daraus das Wissen für eine eigene Computerindustrie zu gewinnen. Mit beachtlichem Erfolg, wie man mittlerweile weiß. In China kam noch vor nicht allzulanger Zeit der von der Volksarmee organisierten Softwarepiraterie eine primäre Versorgungsfunktion zu.

Der Begriff der "Competitive Intelligence" gehört mittlerweile zum Standardvokabular avancierter Unternehmensstrategie. Die sehr bezeichnend "WarRoom Research" genannte US-Beratungsfirma, die ihre Intelligence-Dienstleistungen für "Corporate Espionage" wie auch "Counter Espionage" der Privatwirtschaft, militärischen und politischen Einrichtungen, Großbanken und Versicherungen, aber auch der Telekom-Industrie und HighTech-Forschungseinrichtungen anbietet und als Initiator des sogenannten "Manhatten Cyber Project"[11] gilt, hat 1996 in Zusammenarbeit mit dem US-Senat eine Studie zur Sicherheit der Informationssysteme unter den Fortune-1000-Unternehmen durchgeführt und recherchierte dabei eine hohe Anzahl erfolgreicher Attacken quer durch alle Industrien mit relativ hohen finanziellen Schäden pro Vorfall. Die Eindringlinge kamen sowohl von außen als auch von innen, und sehr oft standen Mitbewerber/Konkurrenten dahinter. Der überwiegende Teil dieser Vorfälle wurde allerdings nie angezeigt oder veröffentlicht, aus der verständlichen Angst vor dem Verlust von Image und öffentlichem Vertrauen. Und — was wohl für die USA

typisch ist — sehr oft wurde auch grundsätzliches Mißtrauen gegenüber "Governmental Investigations" als Motiv angegeben.[12]

Is it a War Crime to Crash Another Country's Stock Market?

Im Sinne der von Paul Virilio propagierten Verschiebung vom Exo- zum Endo-Kolonialismus verortet das Militär die neuen Feinde der Informationsgesellschaft vor allem im Inneren, im eigenen Land, und identifiziert sie als Hacker und Cyberguerilleros, die der nationalen Sicherheit an den Kragen wollen und willfährig den Interessen feindlicher Nationen dienen könnten.

Allerdings ist es auch nicht so sehr die Angst vor dem Eindringen in militärische Computeranlagen, obwohl veröffentlichte Statistiken auch hier eine enorme Verwundbarkeit dokumentieren. (Von mehr als 1000 täglichen Hackerattacken gegen Pentagonrechner ist die Rede, wobei nur etwa 50 davon bemerkt bzw. gemeldet werden. Schwierig beim Hacken ist in der Regel nur die Überwindung des ersten Computers eines Systems, innherhalb einer Firewall halten fast alle Computer auch einen Eindringling für einen legitmen User.) Es sind vor allem die vielen kaum abgesicherten, auf relativ instabilen Betriebssystemen laufenden Computernetze der zivilen Verwaltung, der Industrie, von Banken, Versicherungen, Strom- und Gasgesellschaften etc., die den von solchen Computersystemen längst abhängig gewordenen Staaten Sorgen bereiten.

InfoWar bedeutet seinem eigentlichen Konzept zufolge die Perfektionierung eines Trends in der Kriegsführung dieses Jahrhunderts, nämlich deren Ausrichtung auf zivile Ziele: Von den Bomben auf London, Dresden und Hiroshima zu den ethnischen Säuberungen in Bosnien. Die zivile Flugüberwachung zu stören, die Datenbanken von Versicherungen und Bankinstituten zu löschen und die Währung eines feindlichen Landes zu ruinieren, das alles könnte sehr sauber und unblutig mit dem Computer geschehen, stellt aber in jedem Fall einen gewaltsamen und folgenschweren Angriff auf die zivile Bevölkerung dar.

Die Administration Bush hat mehrfach die Option geprüft, die Computeranlagen der irakischen Finanzbehörden zu zerstören, aber angeblich war es die CIA, die dagegen opponierte. Im Times Magazin vom August 1995 wird ein hochrangiger früherer CIA-Beamter zitiert: "Every time screwing around with financial systems has been discussed as a covert action, people have walked away from it […] Messing with a country's money represents a fundamental attack. No CIA-Director has ever recommended it."

Daß man im globalen Finanzbusiness weniger zimperlich ist (oder zu sein vorgibt), haben nicht zuletzt die Ereignisse rund um die Asienkrise gezeigt, ausgelöst durch die gezielten Spekulationen gegen die malayische Währung, in deren Folge die gesamte Region in die direkte Abhängigkeit des Internationalen Währungsfonds und seiner Vorgaben zur Neuordnung der Wirtschaftssysteme und -praktiken gezwungen wurde. Ein Lehrspiel des InfoWar.

Software code — more than law — defines the true parameters of freedom in cyberspace, the question of what the architecture of cyberspace should be is not a neutral question. We need to think about it in political terms.

Lawrence Lessing, special master in the antitrust case of US vs Microsoft

Fußnoten:

[1] "So groß aber auch die Schlachtfelder sein mögen, so wenig werden sie dem Auge bieten. […] Kein Napoleon […] hält auf einer Anhöhe […] Der Feldherr befindet sich weiter zurück […] in einem Hause mit geräumigen Schreibstuben, wo Draht- und Funktelegraph, Fernsprech- und Signalapparate zu Hause sind. Von dort telephoniert der moderne Alexander zündende Worte […], dort empfängt er die Meldungen […]." Vgl. Von Schlieffen, Graf Alfred, 1909 zitiert nach R. Genth, J. Hoppe: Telephon! Der Draht, an dem wir hängen. Berlin 1986, 60

[2] US-General in einer TV-Erklärung zu einem Zwischenfall im Golfkrieg, bei dem ein US-Militär-LKW von eigenen Waffen in die Luft gejagt wurde.

[3] Time Magazine vom 21.8. 1995, Vol 146, No 8

[4] An Appraisal of Technologies of Political Control. Scientific and Technological Options Assessment/STOA. Working Document (Consultation version), PE 166 499, Luxembourg, 06. Januar 1998. Siehe auch <http://jya.com/stoa-atpc.htm>.

[5] http://www.warroomresearch.com

[6] http://www.poptel.org.uk/statewatch

[7] "The message switching system used on digital exchanges like System X in the UK supports an Integrated Services Digital Network (ISDN) Protocol. This allows digital devices, e.g. fax to share the system with existing lines. The ISDN subset is defined in their documents as "Signalling CCITT1-series interface for ISDN access. What is not widely known is that built in to the international CCITT protocol is the ability to take phones ‚off hook' and listen into conversations occurring near the phone, without the user being aware that it is happening. This effectively means that a national dial up telephone tapping capacity is built into these systems from the start. (System X has been exported to Russia and China)." In: An Appraisal of Technologies of Political Control. Scientific and Technological Options Assessment/STOA, Working Document (Consultation version), PE 166 499, Luxembourg, 06. Januar 1998

[8] "Memorandum of Understanding concerning the lawful interception of telecommunications", ENFOPOL 112, 10037/95. http://www.poptel.org.uk/statewatch/

[9] Zitiert nach: Lindau, Edmund E., pressetext.austria, 22. Februar 98

[10] Zitiert nach Siegert, Bernhardt. In: Helga Konrad (Hg.): Online. Graz 1993, 131, 132

[11] http://www.warroomreseach.com/mcp/

[12] http://www.warroomreseach.com/WRR/SurveysStudies/1996ISS_Survey_SummaryResults.htm