Friedrich Kittler
Zur Theoriegeschichte von Information Warfare

Kai egeneto polemos en to ourano.

Apokalypse 12, 7

Selbstredend haben nicht erst die neunziger Jahre dieses Jahrhunderts entdeckt, daß Information im Krieg zählt. Seit jeher sind drei elementare Listen, die Krieger vermutlich sowohl von Händlern wie von Priestern unterscheiden, im Einsatz gewesen. A sucht erstens zu wissen, was B weiß, ohne daß B von As Wissen weiß. A sucht zweitens sein Wissen an A' (Untergebene oder Vorgesetzte oder Verbündete) zu übermitteln, ohne daß B von der Übermittlung, geschweige denn vom übermittelten Wissen weiß. Diese Logik der Intersubjektivität legt schon als solche eine dritte List nahe: Damit seine Pläne nicht von B durchkreuzt werden können, tut A gut daran, sich selber in A' und B' aufzuspalten und auf der Basis seines Wissens über B die möglichen Spielzüge beider Seiten durchzurechnen. Kriege, mit anderen Worten, implizieren schon seit langem Spionage, Nachrichtentechniken und Kriegsspiele. Unerhört an Information Warfare ist nur, daß Spionage, Nachrichtentechnik und Kriegsspiel allesamt in einem globalen Computernetz zusammenfallen.

Was Kriegsspiel in einer Vorgeschichte hieß, deren technische Modelle der Komplexität heutiger Computer unendlich unterlegen waren, ist schnell gesagt. Als ältestes Spielzeug, an dem die Stellungen zweier Feinde auf einem Schlachtfeld geometrisch simulierbar waren, rühmt sich noch im Zeitalter von Deep Blue das Schachspiel. Es gibt begründete Vermutungen, daß die große Schachregelreform der Frühneuzeit Offizieren wie Läufern und Türmen nur darum viel größere Bewegungsfreiheit einräumte, um auch im Kriegsspiel die militärische Innovationen der Zeit abzubilden. Aber mit dem Ende der Kabinettskriege ging das der Schachbrettgefechte einher. Clausewitz' revolutionäre Lehre bestimmte den Krieg als Zusammenstoß zweier Subjekte, die ihre Strategien nur mehr auf Wahrscheinlichkeitskalküle gründen konnten, weil sie mit dem unberechenbaren Willen des Gegners, den Zufällen des Geländes und der Unsicherheit des Nachrichtenwesens stets zu rechnen hatten. Dieser Lehre, die für die schwarzen und weißen Quadrate eines ideal flachen Schachbretts nur mehr Spott übrig hatte, trat mit dem Sandkasten, wie ihn Müffling 1825 in die Generalstabsarbeit einführte, das geographisch angemessene Kriegsspiel zur Seite. Am Sandkasten ließ sich zum ersten Mal realistisch simulieren, mit welcher Marschgeschwindigkeit Infanterien oder aber Artillerien in Geländen von bekannter Steigung überhaupt vorankamen.

Von solcher physikalischen Realität konnten Spionage und Nachrichtentechnik lange Zeit nur träumen. Es lag an ihrer wesentlich intersubjektiven Struktur selber, daß sie eher auf Subjekte als auf Waffen, eher auf Menschen als auf Maschinen zugriffen. Kriege der Vergangenheit züchteten also genau das, was die NATO in ihrer unnachahmlichen Akronym-Seligkeit zur HUMINT (human intelligence) degradiert hat. Spione, Agenten, Kundschafter und Geheimboten, seit 1800 schließlich auch Militärattachés in potentiell feindlichen Hauptstädten: So ungefähr sah das traditionelle Equipment von Information Warfare aus. Unser Wort "Engel" geht zurück auf das griechische angelos, angelos selber aber auf den persischen Namen jener berittenen Boten, die im Namen ihres Großkönigs das erste (und selbstredend militärische) Postsystem der Geschichte bedienten. Krieg entbrannte also, wie die Apokalypse so richtig schreibt,[1] am Himmel — aber eben darum war und blieb der InfoWar immateriell.

Technik oder Wissenschaft (falls man diese zwei Felder nach Heidegger überhaupt noch trennen darf) kam nur in einer einzigen Hinsicht ins Spiel: bei der Verschlüsselung eigener und der Entschlüsselung feindlicher Nachrichten. Noch heute heißt ein primitiver alphabetischer Schlüssel nicht umsonst nach Caesar, dem Feldherrn. Aber die Kriegsgeschichte der geheimen Information hat auch nach David Kahns bahnbrechenden Codebreakers noch Geheimnisse. Ungeklärt scheint zum Beispiel, ob es zwischen François Vietas Erfindung der algebraischen Anschreibbarkeit von Polynomen einerseits und seiner kryptoanalytischen Tätigkeit in den französischen Religionskriegen Zusammenhänge gab. (Im einen wie im anderen Fall läuft die Aufgabe schließlich darauf hinaus, Buchstaben und Ziffern einander zuzuordnen.)

Aber die Informationen, die so gewonnen oder verborgen wurden, waren selber noch keine Waffen. Deshalb sind in Alteuropa zwar einzelne Schlachten, aber (soweit ich sehen kann) keine Kriege durch Informationstechnik gewonnen oder verloren worden. In anderen Kulturen mag das anders ausgesehen haben, aber zumindest europäische Krieger waren eine ziemlich altmodische oder traditionsbewußte Kaste. Viel spricht daher für die Annahme, daß erst die Kopplung zwischen Generalstabsausbildung und Ingenieursausbildung, wie die Französische Revolution sie durch Gründung der École Polytechnique 1794 institutionalisiert hat, Informationssysteme als Waffensysteme begreifbar machte. 1809 jedenfalls hat Napoleon einen ganzen Feldzug — ausgerechnet gegen das Kaiserreich Österreich — durch Einsatz der damals revolutionären optischen Telegraphie entschieden.[2] Eine Zeitlang dienten auch Linzer Kirchtürme, gleichsam als Vorläufer aller Ars Electronica, zur Übermittlung von Napoleons militärischen Geheimbefehlen …

Der Feldzug von 1809 hat also — um es mit Jacques Lacan zu sagen — dem Krieg eine Funktion der Dringlichkeit oder Urgenz injiziert. Das ebenso höfliche wie selbstmörderische Warten der französischen Ritterschaft, bis 1415 auch der englische Feind zur Schlacht von Azincourt bereit war, nahm ein abruptes Ende. Von der optischen über die elektrische Telegraphie, von der Telegraphie über den (anfangs strikt militärischen) Funk bis zur Satellitenverbindung ist die Kriegsgeschichte der letzten zwei Jahrhunderte — nach Virilios These — reine Dromologie gewesen. Nicht umsonst heißen Verzögerungszeiten (delays) im technisch-militärischen Jargon auch "Totzeiten". Wer einige Sekunden zu spät weiß, den bestraft nicht das sogenannte Leben, sondern ein feindlicher Erstschlag.

Inzwischen dürfte es sich herumgesprochen haben, welche einschneidenden Folgen diese Kriegsgeschichte auch im zivilen Bereich gezeitigt hat. (Unbekannt ist bestenfalls geblieben, daß für solche Folgen die selbstarrogierte Zuständigkeit von Massenmedien-Soziologen nicht hinreicht.) Während die Waffensysteme aus Holz oder Bronze, Eisen oder Damaszenerstahl jahrtausendelang die Ausnahmeexistenz einer Kriegerkaste fristeten, hat die Waffe namens Nachrichtentechnik Kulturen, die vordem auf zivilen (um nicht zu sagen priesterlichen) Speichermedien wie Buch oder Buchdruck gründeten, zu Informationsgesellschaften umgeschaffen. Radio ist nur der um seine Wechselsprechmöglichkeit amputierte Heeresfunk des Ersten Weltkriegs, Fernsehen nur der zivile Zwilling der Radarschirme des Zweiten. Ganz zu schweigen von der Computertechnik, deren kryptoanalytische und damit militärische Herkunft im Fall Alan Turings immerhin seit 1974 kein britisches Staatsgeheimnis mehr ist, während etwa im Fall Claude E. Shannons[3] die National Security Agency noch immer Nachrichtensperre verhängt zu haben scheint. Die Intelligenz von Computern jedenfalls, wie Turing und Shannon sie entwickelten, ist aus der Modellierung nicht physikalischer Prozesse, sondern feindlicher Intelligenz entsprungen.[4] Was Wunder also, daß John von Neumann als Architekt der gleichnamigen Computerarchitektur auch das Kriegsspiel wieder ins

Symbolische überführt hat: Anstelle von Müfflings physikalistischem Sandkasten ist die Matrizenalgebra der Spieltheorie getreten.

Im Anglo-Amerikanischen heißt intelligence ja nicht nur Intelligenz, sondern auch Geheimdienst, also Wissen des Wissens des Feindes. Das gute alte C3I stand für Command Control Communications Intelligence, das aktuelle C4I trägt — als Command Control Communications Computers Intelligence — auch noch der Hardware heutigen Wissens Rechnung. Es wäre eine lohnende, aber immer von der dreißigjährigen Sperrfrist sensitiver Dokumente bedrohte Aufgabe, die Technikgeschichte seit Ende des Zweiten Weltkriegs als schrittweise Verzahnung von COMINT, ELINT und Spieltheorie zu schreiben. COMINT oder Communication Intelligence stammt ersichtlich von Bletchley Parks ersten Computern, die ja kurz vor Kriegsende fast alle Geheimschreiber der Wehrmachtnachrichtenverbindungen knacken konnten. ELINT oder Electronical Intelligence dürfte von den Radarfrühwarnsystemen stammen, die seit den fünfziger Jahren neue Computergenerationen nicht nur von Kryptoanalyse auf Physik umprogrammierten, sondern dabei auch Joystick und Computerbildschirm in die Welt setzten.

Demgemäß spielte Electronic Warfare, das Paradigma des späten Kalten Krieges, noch in den menschenabgewandten, weil jeder Wahrnehmung entzogenen Gefilden der Physik. Als Konzept folgte Electronic Warfare aus dem Diktum von Admiral Moore, Joint Chief of Staffs, daß der Sieg in jedem Zukunftskrieg derjenigen Seite zufallen würde, die sich die Vorherrschaft über das gesamte elektromagnetische Spektrum (von den ultralangen U-Boot-Kommunikations-Wellen bis in den interstellaren Gigahertzbereich) gesichert hätte. Der zweite Golfkrieg machte sein Diktum wahr. Es ist heute beinahe wieder vergessen, daß die ersten US-Bombergeschwader die irakische Grenze kurz vor Mitternacht überflogen, während die unerklärte elektronische Kriegsführung, die ihnen den Himmel über Bagdad erst freischaltete, schon am frühen Nachmittag eingesetzt hatte.

Aber auch Electronic Warfare, diese Schattenseite der neuen medienwirksamen Waffensysteme, hat eine Schattenseite. Weltweite Systeme zur Frühwarnung, Aufklärung, Positionierung und Steuerung von Armeen setzen gleichermaßen weltweite Computernetze voraus. Nur in seiner ersten Planungsphase verschaltete das ARPANET, dieser vergessene Urahn all unserer kommunikativen Verzückungen, die systematisch über Amerikas Bundesstaaten verteilten Kommandobungalows lediglich mit ausgewählten Eliteuniversitäten. Aber schon mit den Glasfaserkabeln, die die NATO im Atlantik verlegte, um die Rohdatenmassen von ELINT und COMINT ihren US-Zentralen sofort rückkoppeln zu können, begann das Netz seine globalen Wucherungen. Ein elektronisches Abbild möglicher Feldzüge, das ihre Topologien und Operationen schon in Hardware oder Software vorwegnimmt, tendiert dazu, den Unterschied zwischen Krieg und Kriegsspiel aufzuheben. Spionage und Nachrichtentechnik einerseits, Computersimulationen andererseits fallen in ein und demselben Equipment zusammen.

Das Pentagon hat dieses neue Dispositiv auf den Namen "Information Warfare" getauft und in den letzten Jahren alles getan, um seine auch nach Ende des Kalten Krieges kaum verminderten Rüstungsgelder von Electronic Warfare auf Information Warfare umzulenken. Die Gründe liegen auf der Hand. Mit den globalen Netzen und Satellitenfunkstrecken, die in den letzten dreißig Jahren aufgebaut worden sind, fällt die Monroe-Doktrin. Achtzig Jahre lang genoß Amerika als einziger unter allen Erdteilen das Vorrecht, den Amerikanern zu gehören. (Nur am Halloween 1938 und nur in Orson Welles' grandioser Hörspielfiktion unterlagen die Staaten New Jersey und New York einen furchtbaren Tag lang Invasoren vom Mars, die insofern schon Blitzkrieg und/oder Information Warfare praktizierten, als sie nicht

Armeen, sondern nur Elektrizitätsnetze, Brücken und Eisenbahnlinien angriffen.[5] Das Internet als Schatten, den Electronic Warfare auf den Globus geworfen hat, beseitigt dagegen jedwedes "Sanktuarium", selbst wenn es Gottes eigenes Land heißt.

Information Warfare kann von jedem PC-bestückten Schreibtisch aus beginnen. Es ist leichter, billiger und damit auch proliferationsträchtiger, eine feindliche CPU als ein feindliches Phasenradar nachzubauen. Deshalb haben schließlich auch die Händler und Ingenieure (etwa bei Advanced Micro Devices) von den Kriegern gelernt, daß Wissen nur als Wissen des Wissens des Feindes (etwa bei Intel) zählt. Reverse engineering heißt schlicht und einfach, eigene Produktionstechniken auf Feindspionage zu gründen. Diese neue Intelligenz, weil sie die gute alte Ignoranzvermutung (bei Konkurrenten, Werbekunden und Käufern) ablöst, wird noch zu schaffen machen.

Reverse engineering heißt aber auch, daß Subjekte alias Untertanen — im Unterschied zu denen von Holz und Bronze, Eisen und Damaszenerstahl — vielleicht wieder eine Chance haben. Wenn die US-Army ihrem alten Traum, stets über das beste proprietäre Computerequipment zu verfügen, eine Absage erteilt und sich statt dessen — wie der Rest der Welt auch — auf dem freien Markt bedient, entsteht wieder so etwas wie waffentechnische Chancengleichheit. Das aber hat welthistorische Folgen. Den Szenarios von Information Warfare zufolge gibt es, leider, keine nationalstaatlichen Gewaltmonopole mehr. Mit Mafias und Kartellen, NGOs und Terrorbanden geht das Ende Hobbes'scher Bürgerkriege selber zu Ende. Wenn Machtsysteme mit Betriebssystemen und Computernetzen nachgerade zusammenfallen, werden sie auf einer Ebene anfällig, die prinzipiell intelligibel ist: auf der Ebene des Codes.

Am Horizont von Information Warfare taucht deshalb nicht nur der — seit Etatisierung der Nachrichtentruppen ebenso vertraute wie langweilige — Appell auf, Zukunftskriege gefälligst nach Maßgaben und Budgetträumen der neuesten Waffengattung zu führen. Es taucht auch eine Figur wieder auf, die mit der Gründung stehender — und das hieß nationalstaatlicher — Heere gründlich vertrieben schien: der Künstler-Ingenieur. Heute weiß nur noch die Kunstgeschichte, daß die gefeierten Genies der Renaissancekunst nicht bloß Gemälde oder Gebäude schufen, sondern Festungen durchrechneten und Kriegsmaschinen konstruierten.[6] Wenn das Phantasma aller Information Warfare, den Krieg auf Software und seine Todesarten auf Betriebssystemabstürze zu reduzieren, wahr werden könnte, würden einsame Hacker den Platz des geschichtsmächtigen Künstler-Ingenieurs einnehmen.

Nicht umsonst imaginiert ein famoses InfoWar-Szenario der RAND Corporation den Fall, daß im Jahr 2002 die USA ihren militärischen Bestand für ein einstürzendes saudisches Herrscherhaus einfach darum zurückziehen, weil Airbusse voll amerikanischer Touristen wie Steine vom Himmel über Chicago fallen. Der Airbus ist bekanntlich das erste zivile Flugzeug gewesen, das wie seine militärischen Vorgänger nur mit Bordcomputerunterstützung überhaupt in der Luft bleiben kann. Im Kriegsspiel der RAND Corporation aber gelingt es iranischen Mullahs, die auf Saudi-Arabien immer schon ölige Augen geworfen haben, mit hohen Bestechungsgeldern den indischen Programmierer der Airbus-Software zum Hacker seines eigenen Programms umzudrehen. Ein einziger Künstler-Ingenieur aus jenem unzufälligen Halbkontinent, der einst mit Erfindung der Null die Basis alles Digitalen schuf, reicht also hin, um über den Transmissionsriemen amerikanischer Mediendemokratie die letzte verbliebene Supermacht strategisch zu paralysieren.[7]

Solche Szenarien setzen aber nicht nur voraus, daß alle Mächte dieser Erde vor medienwirksamen Todesarten ihrer Einwohner gleichermaßen zittern wie Gottes eigenes

Land. Sie stilisieren auch das Schreiben von Software zum künstlerischen Akt eines Individuums, das es in großen Softwareschmieden längst nicht mehr gibt. Deshalb steht — wie schon bei Alvin Tofflers ideologielastigem Cyberspace Manifesto — sehr zu befürchten, daß das freie Individuum in seiner Macht, den Geist selber zum Sieg über die Materialismen des 19. und die militärisch-industriellen Komplexe des 20. Jahrhunderts zu führen, ein Feigenblatt ist und bleibt.

An nicht-staatlichen Organisationen, die das dreihundertjährige Gewaltmonopol der Nationalstaaten unter heutigen Computerbedingungen Schritt um Schritt zersetzen würden, nennen die nationalstaatlich finanzierten Strategen des Informationskrieges immer nur umweltverseuchte Ökologen, friedensverseuchte Linke und islamverseuchte Terrorbanden. Was sie unterschlagen, ist die Computerbranche selber — nicht als mythische Letzte Grenze freier Hacker, sondern als ebenso empirische wie kriegerische Bande globaler Konzerne. Diese Bande hat es immerhin schon geschafft, die Staatsmonopole für Post, Funk und Telekommunikation aufzurollen. Auch setzt die US-Army seit etwa acht Jahren der Computerindustrie keine hochgesteckten Ziele wie etwa Very High Speed Computing mehr, sondern deckt ihren Bedarf, bescheiden wie der Rest der Welt, auf dem freien Markt. Also geht die Bande gegenwärtig dazu über, die Unterhaltungsmedien und Fernsehanstalten ihren Chips und Netzen einzuverleiben. Wenn dann auch Andy Groves "Krieg um den Augapfel" gewonnen sein sollte, bleiben kaum lohnende Feinde oder Unfriendly Take-overs mehr übrig — außer den Nationalstaaten selber. Die lauten Warnungen vor dem Machtverlust des Nationalstaats, gegen den Strich gelesen, könnten daher besagen, daß Computerkriege am besten der Computerindustrie selber übertragen würden. Bill Gates und Scott McNealy als Condottieri ihrer Privatarmen aus Servern and Clients, Betriebssystemen und proprietären Netzen … Alle Prognosen, ob finster oder neoliberal, setzen allerdings eines voraus: daß die Universale Turing-Maschine, faktisch und theoretisch, das Ende jeder Geschichte ist. Information Warfare heißt ja bloß, mit Digitaltechniken um Digitaltechniken zu kämpfen. Physiker von heute gehen dagegen davon aus, daß die Turing-Church-Hypothese in ihrer allgemeinsten, nämlich physikalischen Auslegung ein Trugschluß war, dem die Informationskrieger womöglich aufsitzen: Von der Natur, was immer dieser Unbegriff sonst noch heißen mag, steht zumindest fest, daß sie keine Turing-Maschine ist. Da es sie aber gibt, ist auch nicht ausgeschlossen, daß es andere programmierbare Maschinen geben kann. Dann wäre die Weltgeschichte nicht schon am notwendig digitalen Ende angelangt und die Pax Americana, sofern sie noch immer auf John von Neumanns Zusammenschaltung englischer Computer, deutscher Raketen und amerikanischer Nuklearbomben beruht, ein Zwischenspiel gewesen. Der Krieg, der am Himmel entbrannte, geht im Himmel der Mathematik weiter.

Fußnoten:

[1] und Luther so schwach übersetzt

[2] Vgl. Oberliesen, Rolf: Information, Daten und Signale. Geschichte technischer Informationsverarbeitung. Reinbek 1982, 59—62

[3] Vgl. Shannon, Claude E.: "Communication Theory of Secrecy Systems". In: The Bell System Technical Journal, 28, 1949, 656—715

[4] Vgl. etwa Turing, Alan M.: "Intelligente Maschinen". In: Dotzler, Bernhard; Kittler, Friedrich (Hg.); A.M.T. Intelligence Service. Ausgewählte Schriften, S. 98: "Die Kryptographie wäre vielleicht der lohnendste Anwendungsbereich [von Computern]. Es gibt eine bemerkenswerte Parallele zwischen den Problemen eines Physikers und eines Kryptographen. Das System, nach dem eine Botschaft entziffert wird, entspricht den Gesetzen des Universums, die abgefangenen Nachrichten der erreichbaren Evidenz, der für einen Tag oder eine Botschaft konstante Schlüssel wichtigen Konstanten, die bestimmt werden müssen. Die Übereinstimmung ist

sehr streng, während aber die Kryptographie sich sehr leicht auf diskreten Maschinen durchführen läßt, ist das mit der Physik nicht so einfach."

[5] Vgl. Koch, Howard; Welles, Orson: "The War of the Worlds". In: Faulstich, Werner (Hg.): The War of the Worlds/Der Krieg der Welten. Vier Hörspiele. Tübingen 1981, 23: "They seem to be making a conscious effort to avoid destruction of cities and countryside. However, they stop to uproot power lines, bridges, and railroad tracks. Their apparent objective is to crush resistance, paralyze communication, and disorganize human society." Als Parallelstelle vgl. auch Deighton, Len: Blitzkrieg. Von Hitlers Triumphen bis zum Fall von Dünkirchen. 2. Aufl. München 1980, 225

[6] Vgl. etwa Edgerton, Samuel Y., Jr.: The Heritage of Giotto's Geometry: art and science in the eve of the scientific revolution. Ithaca 1991

[7] Vgl. Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. (Hg.): Strategic Information Warfare. A new face of war. National Defense Research Institute, RAND Corporation. Santa Monica 1996