Das kognitive Perpetuum mobile
Die Rolle von Computern mit künstlicher Intelligenz in der militärtechnologischen Entwicklung

Reinhard Keil-Slawik

Am 23. März 1983 verkündete Präsident Reagan seine Vision von einer ›Strategischen Verteidigungsinitiative‹ (SDI, Strategic Defense Initiative). Über ein zentrales computerisiertes Schlachtenführungssystem soll nicht nur die Abwehr feindlicher Atomraketen mit im Weltall stationierten Laserwaffen gesteuert werden, sondern auch die gesamte für einen atomaren Gegenschlag erforderliche Einsatzplanung erfolgen. Die vom Pentagon veröffentlichten technischen Anforderungen an dieses Schlachtenführungssystem übersteigen das technisch Machbare um eine Größenordnung, die nur unter Zuhilfenahme neuer »revolutionärer« Techniken überwindbar scheint.

Computer mit künstlicher Intelligenz (im weiteren kurz als KI-Systeme bezeichnet), insbesondere Expertensysteme, sollen diese revolutionäre Technologie verkörpern. Am 28. Oktober 1983 leitete die DARPA (Defense Advanced Research Projects Agency) – eine Institution, deren Aufgabe es ist, die Forschungsaktivitäten der drei Teilstreitkräfte Heer, Luftwaffe und Marine zu koordinieren – dem amerikanischen Kongress ein Forschungsprogramm mit dem Titel *Strategic Computing* zu. Dieses Vorhaben, das in Analogie zu SDI häufig auch als SCI (Stragetic Computing Initiative) bezeichnet wird, stellt im wesentlichen heraus, daß man nur mit Hilfe einer neuen Generation von »Maschinenintelligenz« in der Lage sein werde, die anstehenden Probleme im militärischen Bereich zu lösen:

»Ein äußerst zwingendes Beispiel für einen solchen Fall ist die projektierte Abwehr von strategischen Atomraketen, bei der das System so schnell reagieren muß, daß man sich vermutlich fast vollständig auf atomatisierte Systeme verlassen muß. Die Komplexität und Unvorhersagbarkeit der Faktoren, die die Entscheidungen beeinflussen, wird zu diesem Zeitpunkt sehr groß sein.« (DARPA 1985, S. 149)

Um aber Expertensysteme für die entsprechenden militärischen Anwendungen entwickeln zu können, muß ein ungeheuer hoher Aufwand ge-

trieben werden: »Es beinhaltet nicht mehr als ein volles, rationales Verständnis des menschlichen Verhaltens, das nachgebildet werden soll.« (Secretary of Defense 1984, S. 10)

Die Erwartungen an eine der menschlichen Intelligenz ebenbürtige oder gar überlegene künstliche Intelligenz sind jedoch unerfüllbar. Der Traum, daß der Mensch etwas hervorbringen könnte, was nicht nur in Teilbereichen, sondern im Ganzen besser ist als er selbst, entpuppt sich letztendlich als Wunsch nach einem kognitiven Perpetuum mobile; oder mit den Worten des Softwareexperten David L. Parnas (1986 b): »Menschen sind unzuverlässig genug, wie unzuverlässig müssen dann erst ihre Schöpfungen sein.«

Die Entwicklung komplexer DV-Systeme erfolgt grundsätzlich in Zyklen von Analyse, Entwurf, Einsatz und Auswertung. Aufgrund der im Einsatz gemachten Erfahrungen werden sie verbessert, restrukturiert oder durch neue Systeme ersetzt. Jeder Verbesserung bzw. bessere Anpassung an den Einsatzkontext gründet sich auf solche Zyklen. Die Fehlerbewertung wie auch die Bewertung der Angemessenheit eines Systems ist ein sozialer Prozeß, an dem viele Menschen beteiligt sind.

Wo solche Zyklen durch sogenannte intelligente Maschinen durchbrochen werden sollen, spreche ich von einem kognitiven Perpetuum mobile. Dies wäre eine Maschine, die ein Ergebnis produziert, das zuverlässiger wäre als die Konstruktion der Maschine selbst. Für Wärmekraftmaschinen wird das Prinzip des Perpetuum mobile heute als nicht realisierbar erachtet, doch im Bereich der datenverarbeitenden Maschinen erlebt dieser Traum eine Renaissance.

Am Beispiel der militärtechnologischen Entwicklung will ich dieses Phänomen deutlich machen; zum einen deshalb, weil in diesem Anwendungsbereich für uns alle ein beträchtliches Gefahrenpotenial steckt, zum anderen, weil der militärische Einsatzkontext aufgrund der enormen finanziellen Aufwendungen gewissermaßen die Technologiefront repräsentiert. Wie ich im nächsten Abschnitt am Beispiel großer DV-Systeme im militärischen Bereich zeigen werde, wird die Zuverlässigkeit im Systemverhalten nicht – wie landläufig häufig angenommen – durch die Technik sichergestellt, sondern durch die Vernunft und Einsicht autonom handelnder Menschen.

1 Der programmierte Irrtum

Ein kurzer Blick in die militärtechnologische Entwicklung seit dem Zweiten Weltkrieg (vgl. dazu Keil-Slawik 1985 u. 1989) zeigt uns, daß wir die Unzuverlässigkeit und Undurchschaubarkeit großer militärischer computergestützter Systeme nicht als Sonderfall oder Ausnahmeerscheinung betrachten können, sondern daß diese Phänomene untrennbar mit der zunehmenden Integration und Automatisierung militärischer Teilsysteme verknüpft sind. Fehler und Fehlalarme sind seit dem Aufbau der ersten Frühwarn- und Entscheidungssysteme ständige Begleiter dieser Entwicklung.

Anfang der 50er Jahre wurde beispielsweise ein Schwarm Kanada-Gänse von der DEW-Radarkette (Distant Early Warning) irrtümlich als ein Angriff sowjetischer Bomber interpretiert (Bracken 1983, S. 48) und Anfang der 60er Jahre wurde die Öffentlichkeit durch mehrere Fehlalarme auf das Frühwarnsystem zur Erkennung ballistischer Interkontinentalraketen BMEWS (Ballistic Missile Early Warning System) aufmerksam. Die nordamerikanische Luftverteidigungszentrale NORAD (North American Aerospace Defense Command) erhielt z.B. am 5. Oktober 1960 von der Radarstation in Thule auf Grönland eine Warnung höchster Dringlichkeitsstufe, die besagte, daß ein Raketenangriff auf die USA eingeleitet worden war. »Der kanadische kommandierende Luftwaffengeneral unternahm die notwendigen Maßnahmen, die Meldung zu überprüfen. Nach 15 bis 20 Minuten erwies sich der Alarm als Fehlalarm. Die Radarstationen hatten offensichtlich vom Mond reflektierte Signale empfangen.« (Thompson 1985, S. 122)

Das SAGE-System (Semi-Automatic Ground Environment Air Defense System), mit dessen Hilfe die Schlachtenführung bei einem Luftangriff erfolgen sollte, erwies sich vollends als Fehlschlag. Nachdem über 20 Milliarden Dollar investiert worden waren, scheiterte das System in den 60er Jahren nach vielfältigen Revisionen an der technischen Komplexität der korrekten Erfassung feindlicher und befreundeter Flugzeuge, insbesondere wenn deren Flugbahnen sich kreuzten (vgl. Fallows 1981, S. 59).

Doch noch ein weiteres Problem komplexer Frühwarnsysteme wurde an SAGE deutlich: Bereits kleinere Störungen im Radarbild hätten das System lahmgelegt, wenn sich die Bedienungsmannschaften an die für die Benutzung des Systems festgelegten Regeln und Vorschriften gehalten hätten. Die Operateure schafften es irgendwie, um das System herumzuarbeiten und es funktionsfähig zu halten. Die dazu nötigen mündlichen Absprachen sind jedoch in offiziellen Berichten nie erwähnt wor-

den. Ja, die Bediener sind noch nicht einmal in der Lage gewesen, den Ingenieuren zu erklären, welche Bedienungsprozeduren sie in bestimmten Situationen anwenden würden. Paul Bracken hat diese Erkenntnis verallgemeinert: »Sehr wenige komplexe Systeme würden jemals laufen, falls die Benutzungsregeln buchstabengetreu befolgt würden.« (1983, S. 12)

Trotz verbesserter Elektronik und leistungsstärkerer DV-Systeme verloren Systemingenieure wie Generale aufgrund der zunehmenden Komplexität durch die Erweiterung und Vernetzung der Einzelsysteme den Überblick, über das gesamte Verteidigungssystem. Überrascht wurde die amerikanische Regierung von der sowjetischen Intervention in der ČSSR, der Tet-Offensive in Vietnam und später dem Yom-Kippur-Krieg wie auch von der Übernahme der Falklandinseln durch Argentinien; und nach Paul Bracken (ebd. S. 34 u. 51) kann bis heute keine definitive Ursache für dieses Versagen angegeben werden.

All dies führte Anfang der 70er Jahre zu einer Untersuchung durch den amerikanischen Kongress und als Folge zum Aufbau des weltweiten militärischen Befehls- und Kommunikationssystem Wimex (WWMCCS, Worldwide Military Command and Control System), das bis heute im Einsatz ist. Die zentrale Schaltstelle für Wimex bildet das NORAD-System. Es besteht aus 84 Großcomputern, deren Programme über 10.000.000 Zeilen umfassen. Die Programme wie auch die Computer sind teilweise veraltet oder für die Aufgabe ungeeignet; sie müssen fortlaufend angepaßt, verbessert und erweitert werden. Die Positionierung und Konfiguration von Satelliten und Sensorsystemen führt ebenfalls zu Änderungen im Systemverhalten; umfangreiche Tests sind erforderlich. Um möglichen Fehlalarmen vorzubeugen, sind daher allein in den Jahren 1979 und 1980 mehr als 3700 routinemäßige Raketenerkennungskonferenzen einberufen worden. Trotz dieser Kontrollen hat es über 147 Fehlalarme gegeben, wobei viermal die zweite von drei möglichen Warnstufen erreicht worden ist, d.h. die mit Atombomben bestückten Langstreckenbomber (B-52) waren aufgestiegen und die Interkontinentalraketen startklar gemacht worden und warteten lediglich auf den »GO-Code«, um den Gegenschlag auszulösen (vgl. ausführlich Bläsius, Siekmann 1987; Borning 1987).

Solche Fehlalarme sind nicht zu vermeiden. Die Senatoren Gary Hart und Barry Goldwater, die im Auftrag des amerikanischen Kongresses die Fehlalarme bei NORAD untersucht haben, kommen zu dem Schluß, daß wir uns auf die gemeinschaftlich getroffene Bewertung der Menschen, die mit dem System arbeiten, verlassen müßten, um Fehlalarme korrekt erkennen und damit umgehen zu können (vgl. Hart, Goldwater 1980, S. 13).

Der militärische Nutzen von Wimex ist darüber hinaus äußerst fragwürdig. Als es im Jahr 1977 getestet wurde, war es 62 % der Zeit nicht einsatzbereit; Teile des Netzes sogar 85 % der Zeit. Die vollständige Einsatzbereitschaft, wie sie in der ursprünglichen Spezifikation des Systems festgeschrieben worden war, konnte nicht erreicht werden (vgl. Pringle, Arkin 1983, S. 145). Doch selbst wenn Wimex funktionieren würde, wäre es nach James Fallows (1981, S. 52) von zweifelhaftem Wert: Gemäß einer NATO-Studie müßten die Kommandeure des zentralen Kommandobunkers für Europa rund um die Uhr 790 Wörter pro Minute lesen, wollten sie mit dem Informationsstrom des Systems Schritt halten. Ein Systemtest am 6. November 1980 zeigte zudem, daß die Kommendeure während der angenommenen Krisenzeit über 12 Stunden keine wesentlichen Informationen über den Bereitschaftszustand ihrer Truppen erhielten (vgl. Pringle, Arkin 1983, S. 150 f.). Das heißt, das System liefert zu viele Daten, und diese sind großenteils für die anstehenden Entscheidungen nicht relevant.

Die bisher skizzierte Entwicklung hat gezeigt, daß bei komplexen technischen Systemen nicht die Maschine, sondern der Mensch der Garant für Sicherheit und Zuverlässigkeit ist. Der verhängnisvolle Irrtum besteht in der Annahme, daß durch den Einsatz von KI-Systemen im militärischen Bereich die bisher aufgezeigten Defizite ausgeglichen werden könnten und dadurch die in den Forschungsprogrammen SDI und SCI projektierte Leistungsfähikgkeit erreicht werden könnte.

Bevor ich auf diese Problematik näher eingehe, will ich im nächsten Abschnitt anhand einiger wesentlicher Merkmale geistiger Prozesse deutlich machen, daß die bisher angeführten empirischen Befunde aufgrund theoretischer Erkenntnisse verallgemeinert werden können.

2 Irren ist menschlich

Geistige Prozesse können mit denselben Merkmalen charakterisiert werden, die auch für die Evolution der Lebewesen gelten. Jede Idee und jeder Akt des bewußten menschlichen Denkens ist insgesamt mit einem mehrstufigen Evolutionsprozeß vergleichbar. Die Evolution als solche entspricht einem Lernvorgang, der auf reproduktiven Gedächtnisleistungen beruht: »Ohne Gedächtnis, ohne ständige Reproduktion und Bewertung der duplizierten Produkte gäbe es weder eine Evolution der Lebewesen noch eine solche der Ideen.« (Eigen, Winkler 1983, S. 332)

In lebenden Organismen ist der Bauplan in Form des genetischen Kodes ein Teil des Lebewesens. Im Gegensatz zu lebenden Systemen befindet sich der Konstruktionsplan einer Maschine außerhalb der Maschine selbst. Die Funktion der Maschine wird abhängig von den Wünschen und Erfahrungen des Konstrukteurs definiert und dann im Einsatz überprüft. Der Mensch baut die Maschinen und entwickelt Formalismen. Er setzt sie ein und sammelt mit ihnen Erfahrungen, die in die nächste ›Maschinengeneration‹ einfließen; er zerstört sie, paßt sie an oder verbessert ihre Konstruktion im Rahmen seiner kulturellen und sozialen Entwicklung (vgl. dazu Keil-Slawik 1989). Folglich gibt es keine Evolution der Maschinen. Was evolviert, ist das Wissen in den Köpfen der Menschen.

Der Anspruch vieler KI-Experten, es ließe sich eine Maschine bauen mit einer dem menschlichen intelligenten Verhalten entsprechenden Komplexität, die zuverlässiger und besser funktioniert als ihr Schöpfer, kann als kognitives Perpetuum mobile 1. Art bezeichnet werden. Ähnlich wie ihr energetisches Pendant, das ohne Energiezufuhr von außen ständig Energie erzeugt, wäre sie in der Lage, fortwährend neue Informationen zu verarbeiten, ohne daß ein menschlicher Konstrukteur korrigierend eingreifen müßte. Die Konstruktion müßte von Anfang an vollkommen und fehlerfrei sein. Darüber hinaus müßten alle sich verändernden Aspekte des Einsatzumfeldes von vornherein berücksichtigt worden sein, sodaß keine Fehler auftreten oder undefinierte Situationen entstehen könnten.

Jeder Versuch aber, Fehler von vornherein grundsätzlich auszuschließen, ist zum Scheitern verurteilt. »Ohne den Widerspruch zwischen verfügbarem Wissen und der vom Menschenkopf noch nicht verstandenen Wirklichkeit gibt es keine Erkenntnis«, stellt Peter Brödner (1986, S. 6) in seinen Thesen zur künstlichen Intelligenz fest. Bei allen Produkten des menschlichen Geistes gilt, daß wir zu keinem Zeitpunkt absolute Gewißheit darüber haben können, ob das entsprechende Produkt in all seinen Eigenschaften auch dem entspricht, was wir von ihm erwarten – ganz egal, ob es sich dabei um mathematische Beweise, Bauwerke, Maschinen oder auch Software handelt.

Wohl aber können wir Fehler in den Fällen vermeiden, in denen uns die Art der Fehler und die Umstände ihres Auftretens bereits bekannt sind. Dies setzt voraus, daß wir mit der Natur dieser Fehler vertraut sind. Wir haben gelernt, entweder mit Hilfe bestimmter Techniken diese Fehler zu erkennen, bevor sie auftreten, oder aber in den entsprechenden Situationen geeignet zu verfahren. Auf diese Weise können wir bis zu einem gewissen Grad auch mit defekten Geräten und fehlerhaften Maschinen zuverlässig arbeiten.

In der Regel betrachten wir Fehler als etwas Negatives und vergessen dabei, daß es häufig erst die Fehler und Mißerfolge sind, die uns vor Augen führen, was unter welchen Bedingungen funktioniert bzw. nicht funktioniert, und uns damit die Möglichkeit zur Verbesserung geben (vgl. Petroski 1985). Der Philosoph Gilbert Ryle betont, daß wir immer auch schon etwas wissen oder können müssen, um überhaupt Fehler machen zu können: »Fehler sind Übungen der Kompetenz« (1983, S. 58), denn man muß z.B. zumindest die Grundregeln des Rechnens beherrschen, um überhaupt Rechenfehler machen zu können.

Je komplexer die Systeme jedoch werden, desto weniger können wir Fehler eindeutig bestimmen. Die Suche nach Fehlerursachen unterliegt Kriterien der Ökonomie und der Bequemlichkeit. Wie Jens Rasmussen feststellt, wird die Fehlersuche in der Regel dann abgebrochen, wenn man Abweichungen vom Normalverlauf findet, die man kennt, die daher als Erklärungen akzeptabel sind und bei denen man folglich etwas zur Korrektur unternehmen kann. Das bedeutet, »daß die Zuschreibung von Ursachen zu Menschen oder zu technischen Teilen im System eine rein pragmatische Frage ist« (1985, S. 6). Die Beantwortung dieser Frage hänge davon ab, aufgrund welcher Kriterien die Suche nach den Ursachen für einen bestimmten Fehler abgebrochen werde. Rasmussen schlägt daher vor, nicht von Fehlern, sondern von Mensch-Maschine-Mißverhältnissen *(man-machine mismatch situations)* zu sprechen.

Hinzu kommt, daß die Analyse und Bewertung dieser Mensch-Maschine-Mißverhältnisse im Kontext kommunikativen Handelns erfolgt. Computer verfügen aber weder über kommunikative Kompetenz, noch über individuell geprägte Wertvorstellungen. Die Annahme, Computer könnten sich aufgrund spezieller Lernprogramme eine solche Kompetenz aneignen, entspräche einem kognitiven perpetuum mobile der 2. Art. Lernen wie auch Wärmeübertragung sind zeitlich gerichtete Prozesse. Ähnlich wie beim energetischen Vorbild, das der Aussage widerspricht, daß Wärme nie von einem Körper niederer Temperatur auf einen Körper höherer Temperatur übergehen kann, kann eine Maschine nicht aus Fehlern oder Regelverletzungen lernen, die in ihrer eigenen Konstruktionsvorschrift verankert sind, d.h. aus Fehlern in ihrem Lernprogram, das der Mensch entwickelt hat. Oder anders ausgedrückt, der Mensch müßte eine Konstruktionsvorschrift angeben können, aufgrund derer eine Maschine etwas ›verstehen‹ könnte, was er selbst noch nicht verstanden hat. Würde irgendetwas dergleichen passieren, wäre die Maschine nicht beherrschbar, weil ihre Funktion undefiniert wäre.

Ebensowenig wie die Unmöglichkeit eines Perpetuum mobile in der Physik nicht bewiesen werden kann, sondern aufgrund empirischer Tat-

bestände als Faktum betrachtet wird, kann auch die Unmöglichkeit eines kognitiven Perpetuum mobile nicht formal bewiesen werden. Schließlich könnte es prinzipiell eine Situation geben, in der die bisher angeführten Einschränkungen nicht zutreffen würden. In den nächsten beiden Abschnitten werde ich mich daher mit der Herstellung und dem Einsatz von KI-Systemen im militärischen Bereich beschäftigen und Belege dafür anführen, daß auch durch die Möglichkeiten der KI das bisher Gesagte nicht hinfällig wird; im Gegenteil: statt neue, bessere Lösungen zu erzeugen, werden die bestehenden Probleme noch verstärkt.

3 Softwareentwicklung und KI

In komplexen Systemen werden immer Fehler auftreten. Gerade bei Computern wird dieses Problem besonders deutlich: Es gibt kein Rechnersystem, bei dem die Grundsoftware (z.B. das Betriebssystem) fehlerfrei arbeitet. Man hat erkannt, daß es generell nicht möglich ist, große Softwaresysteme fehlerfrei zu entwickeln. In der Softwaretechnik rechnet man bei qualitativ hochwertigen Programmen mit etwa fünf Fehlern pro tausend Zeilen Programmkode (vgl. Hamlet 1987, S. 92). Zum Teil werden auch erkannte Fehler nicht verbessert, weil mit jeder Verbesserung nur neue Fehler ins Programm kommen. Die Systeme sind undurchschaubar, denn es ist nicht möglich, ein weiteres System zu entwikkeln, das genau dasselbe Ein-/Ausgabeverhalten aufweist.

Generell gilt, daß Computer die meiste Zeit nicht rechnen, sondern damit beschäftigt sind, Daten hin und her zu schaufeln und zu analysieren. Die Regeln, nach denen dies geschieht, können nicht in Form mathematischer Funktionen oder Gleichungen beschrieben werden: »Stattdessen sind sie komplizierte Ansammlungen ziemlich ad hoc gebildeter Regeln, Algorithmen und Methoden, von denen die Designer hoffen, daß sie den Problembereich, mit dem es der Computer zu tun hat, korrekt modellieren.« (Ornstein 1986, S. 4) Das Problem der korrekten Modellierung wird umso gravierender, je größer das zu lösende Problem ist.

Beim Entwurf von Software kommt es also wesentlich darauf an, alle Sonderfälle und Ausnahmebedingungen vollständig zu erfassen und ordnungsgemäß zu verarbeiten. Dies ist kein mathematisches Problem, sondern es hängt davon ab, inwieweit die Systemingenieure das zu lösende Problem mit all seinen Randbedingungen durchschauen.

Software besteht aus einem einheitlichen und zudem abstrakten Baustoff. Das Verständnis ist nur über beschreibende Texte oder die Erpro-

bung eines bereits existierenden Produktes möglich. Programmieren muß nach Peter Naur deshalb nicht in erster Linie als Produktion von Programmen und zugehörigen Texten betrachtet werden, sondern als ein Prozeß, bei dem die Programmierer eine Theorie darüber entwickeln, wie die vorhandenen Probleme durch die Programmausführung gelöst werden können. Da nicht alle bei der Systementwicklung auftretenden Probleme und Entscheidungen mit all ihren Wechselbezügen dokumentiert werden können, ist diese Theorie nur in den Köpfen der Entwickler vorhanden: »Das Wiederherstellen der Theorie lediglich aufgrund der Dokumentation ist gänzlich unmöglich.« (Naur 1985, S. 258)

Die Folge ist, daß es in der Softwaretechnik keine handhabbaren mathematischen Methoden gibt, mit denen man wie in anderen ingenieurwissenschaftlichen Disziplinen die Zuverlässigkeit der Produkte ›garantieren‹ könnte. Dies wird besonders dann deutlich, wenn bereits geschriebene Programme erweitert oder an neue Einsatzbedingungen angepaßt werden müssen. Jede Änderung führt dazu, daß die Struktur des Programmes schlechter und damit der Einarbeitungsaufwand für die Programmierer größer wird. Schließlich ist es billiger, statt Änderungen vorzunehmen, ein neues Programm zu schreiben (vgl. Belady, Lehman 1976, S. 112).

Obwohl Programme im Prinzip leichter zu ändern sind als elektronische Bauteile, die jeweils neu gefertigt werden müssen, können große Softwaresysteme kaum noch geändert werden, weil die damit verbundenen Effekte nur schwer oder gar nicht zu durchschauen sind. »Der Aufwand für die Entwicklung und das Testen der Software für das Kampfflugzeug F-18 ist so umfassend gewesen, daß, wenn Änderungen erforderlich waren, das Flugzeug an die bestehende Software angepaßt wurde, anstatt die Software an das Flugzeug anzupasssen.« (Jacky 1985, S. 26) Nach Jonathan Jacky erwartet das amerikanische Verteidigungsministerium, daß es um 1990 herum etwa zehn Prozent der gesamten Verteidigungsausgaben, also etwa dreißig Milliarden Dollar, nur für Software ausgeben wird.

Diese Problematik gilt erst recht für KI-Software. Nach David Parnas sind heute allgemein zwei verschiedene Definitionen von künstlicher Intelligenz im Gebrauch und zwar:

»KI-1: Die Verwendung von Computern zur Lösung von Problemen, die bisher nur durch Anwendung der menschlichen Intelligenz zu lösen waren . . .

KI-2: Die Verwendung einer bestimmten Reihe von Programmiertechniken, die als heuristische bzw. regelbezogene Programmierung bezeichnet werden. Bei diesem Ansatz werden menschliche Experten einer Untersuchung unterzogen, um festzustellen, welche heuristischen Methoden bzw. Faustregeln sie bei der Problemlösung verwenden.« (Parnas 1986 a, S. 63 f.)

Die erste Definition charakterisiert künstliche Intelligenz als eine Sammlung von Problemen, während die zweite Definition sich auf eine Reihe von Techniken bezieht. KI-Programme können durchaus beiden Definitionen entsprechen.

Was bisher über die Zuverlässigkeit von Software gesagt wurde, gilt nun nicht nur für KI-1, wo Programme nach traditionellen, ingenieurswissenschaftlichen Methoden entwickelt werden, sondern in noch stärkerem Maße für KI-2: Die Regeln, die man durch Befragung menschlicher Experten erhält, sind meist inkonsequent, ungenau und unvollständig; und die Programme werden durch praktisches Herumprobieren entwickelt, wobei immer dann eine neue Regel eingebaut wird, wenn sich ein Fall ergibt, der mit den bisherigen Regeln nicht behandelt werden kann. Nach Parnas sind solche Programme noch weniger vertrauenswürdig als herkömmliche.

Das Problem besteht hierbei jedoch nicht darin, daß die Entwickler auf die Benutzung formaler Sprachen mit einem eingeschränkten Ausdrucksrepertoire angewiesen sind. Die häufig vertretene These, auf natürlicher Sprache basierende Techniken würden neue Möglichkeiten eröffnen, ist irreführend. Bezugnehmend auf seine Erfahrungen bei der Benutzung von KI-Techniken zur Entwicklung von militärischen Simulationsprogrammen *(war games)* kommt P. K. Davis (1986) von der RAND Corporation zu der Einschätzung, daß die unterstellte Transparenz von Regeln, die in einer natürlichsprachlichen Art kodiert werden, irreführend ist. Es sei schwierig, komplette Regelblöcke zu verstehen und zu überprüfen, zum Teil deswegen, weil es schwierig zu entscheiden sei, ob sie vollständig sind.

An dieser Stelle scheint ein kognitives Perpetuum mobile der einzige Ausweg zu sein. Eine wissenschaftliche Beratungskommission des amerikanischen Verteidigungsministeriums kommt zu dem Ergebnis, daß die Leistungsfähigkeit der zur Zeit in den Computerlaboratorien entwickelten Systeme etwa um das 1.000.000.000fache gesteigert werden müßte, um zu militärisch einsatzfähigen Systemen zu gelangen. Beispielsweise müßte die Antwortzeit von einer Stunde bei heutigen Systemen auf 1 Sekunde verkürzt werden. Dazu muß noch berücksichtigt werden, daß der Aufwand zur Aufstellung der zehn- oder gar hunderttausend Regeln, die ein Expertensystem verarbeiten soll, die Gesamtkosten der Hard- und Softwareentwicklung weit übersteigen könnte (vgl. Secretary of Defense 1984, S. 10).

Aus diesem Grund soll auch der Wissensakquisitionsprozeß automatisiert werden. Als Konsequenz daraus schlägt die Beratungskommission in ihrer Studie vor, Expertensysteme zu entwickeln, die imstande sein

sollten, Texte zu lesen und zu verstehen, um so ohne einen menschlichen Experten Wissensstrukturen erzeugen und revidieren zu können. »Die Systeme sollten auch in der Lage sein, direkt mit einem menschlichen Experten zu interagieren, um ohne die Intervention eines Informatikers die Expertise zu erhalten. « (Ebd., S. XIII)

Abgesehen davon, daß eine solche technische Lösung lediglich eine Verlagerung des Problems darstellt, weil es auch solche Expertensyteme bisher nicht gibt, besteht die große Gefahr darin, daß damit die Fehlerquellen vergrößert statt vermindert werden. Sowohl der Experte als auch der Konstrukteur wären jetzt noch weniger in der Lage festzustellen, inwieweit tatsächlich alle Möglichkeiten vollständig und adäquat berücksichtigt worden sind.

Zwar wird viel darüber geredet und geschrieben, was man im Prinzip mit Expertensystemen alles machen könnte. »Aber wir sind sehr weit entfernt davon, hinreichend allgemeine und vor allem erprobte Techniken hierfür zu haben, die es rechtfertigen, ihre Anwendung als ›Engineering‹ zu bezeichnen.« (Struß 1986, S. 53) Wo aber die ingenieurmäßigen Voraussetzungen fehlen, können Maschinen nicht weiterhelfen.

4 Die reduzierte Wirklichkeit

Zu den Problemen einer ingenieurmäßigen Entwicklung von KI-Systemen kommen noch weit schwierigere Probleme hinzu, die sich aus dem spezifischen militärischen Einsatzkontext ergeben. Dabei geht es im wesentlichen um die korrekte Beschreibung und Modellierung dessen, was die Systeme eigentlich leisten sollen. Diese Schwierigkeit besteht nicht nur für die Entwickler von KI-Systemen, sondern vor allem auch für die Benutzer solcher Systeme. Beide benötigen Modelle, anhand derer sie ihr Verständnis von der Funktionsweise und den Wirkungen der Maschine überprüfen und verbessern.

Modelle unterliegen grundsätzlich zwei wesentlichen Einschränkungen: Erstens sind sie immer nur partiell, und zweitens werden sie um so unzuverlässiger, je größer der Zeitraum ist, in dem sie nicht an der ›harten‹ Wirklichkeit überprüft werden. In jedem Modell sind nur diejenigen Aspekte der Wirklichkeit erfaßt, die für den jeweiligen Zweck relevant sind. Was aber jeweils für ein bestimmtes Modell relevant ist, können wir nicht durch Modellieren herausfinden, sondern nur durch Erproben in der Wirklichkeit. Dies gilt erst recht für jede Art von Software. Wir haben keine Theorie, mit der wir das Verhältnis Modell/Wirklichkeit erfassen

können, stellt Brian Smith (1985) fest, wir haben nur Theorien, die sich auf das Verhältnis Modell/Software beziehen. Es bleibt also nur die Möglichkeit, die Systeme zu testen, indem man sie einsetzt und erprobt.

Von daher kann man sich auf Expertensysteme, wie auch allgemein auf Software, nur dann verlassen, wenn man möglicherweise eintretende Situationen ausführlich und unter realistischen Bedingungen anhand von Testfällen nachbilden kann. Aber die meisten Funktionen der in SCI und SDI angesprochenen Anwendungen können in Friedenszeiten gar nicht unter realistischen Bedingungen getestet werden. Weit schwierigere Probleme noch wirft die Frage auf, ob die Benutzer überhaupt in der Lage wären, die angestrebte Systemfunktionalität angemessen zu nutzen.

Politische wie auch ranghohe militärische Entscheidungsträger können schon heute die Konsequenzen und die Tragweite ihrer Entscheidungen nicht mehr abschätzen, weil ihnen nur minimale Entscheidungsmöglichkeiten verbleiben. Ein ehemaliger Direktor für Wehrforschung und -entwicklung erklärte bereits 1976 dazu: »Es hat keinen Sinn, ihm (dem Präsidenten) einen Raum voller Statusanzeigen zu geben und zu sagen: ›Hier ist es Chef, treffen Sie eine Entscheidung.‹ Es muß auf eine Skala vereinfacht werden – zum Beispiel grün, gelb und rot –, und er kann aufgrund des Zeigerausschlags entscheiden, was er tun sollte.« (Zit. n. Aldridge 1981, S. 64) Mit einer Farbskala lassen sich jedoch weder die Konsequenzen eines Einsatzes von Atomwaffen beschreiben noch geeignete Gegenmaßnahmen verdeutlichen. Das bedeutet aber, daß der wesentliche Entscheidungsspielraum eigentlich nur noch darin besteht, nicht den vom System vorgeschlagenen Entscheidungsmöglichkeiten zu folgen.

Auch hier glaubt man, mit Hilfe von Expertensystemen, die natürliche Sprache verstehen und verarbeiten zu können, das Problem lösen zu können. Zwar bietet die natürliche Sprache sehr viel reichhaltigere Strukturen als eine formale Interaktionstechnik, und obendrein muß sie von den Benutzern nicht zusätzlich erlernt werden, doch ist es zugleich auch ein Wesensmerkmal natürlicher Sprache, daß man sich unverständlich oder mißverständlich ausdrücken kann.

Ohnehin ist der Begriff ›Verarbeitung natürlicher Sprache‹ bei Computersystemen recht fragwürdig. Computer erfüllen keine der für den Erwerb der natürlichen Sprache notwendigen biologischen und sozialen Voraussetzungen. Menschen, die an einem System mit sogenannter natürlichsprachlicher Schnittstelle arbeiten, merken zweierlei:

»Erstens, sie benutzen die Strukturen ihrer natürlichen Sprache, um mit einem System zu interagieren, das diese Sprache nicht versteht, aber in der Lage ist, einige dieser Strukturen zu verarbeiten. Zweitens spiegeln die Antworten eine spezielle Dar-

stellung wider, die von einer Person oder einer Gruppe von Personen erzeugt wurde und die eine Blindheit verkörpert, der sich selbst die Entwickler nicht vollständig bewußt sein können.« (Winograd, Flores 1986, S. 124)

Für die Reichhaltigkeit und Vielfältigkeit der Strukturen gilt noch eine weitere Einschränkung: Da Computer weder über Lebenserfahrung verfügen noch über gesunden Menschenverstand, kann die Bedeutung von Sätzen immer nur vor dem Hintergrund der im Rechner vom Menschen angelegten Strukturen und Objekte erschlossen werden. Von daher wird es immer Sätze geben, die für den Menschen einen Sinn haben, bei denen der Computer aber eine Fehlermeldung generiert, die beispielsweise besagt, daß die gestellte Frage, bezogen auf den Inhalt der Datenbank, keinen Sinn ergibt. Je komplexer die Problemstellung, desto präziser und eindeutiger muß die Interaktion mit dem Computer sein, um sicherstellen zu können, daß auch tatsächlich genau die Anweisungen ausgeführt werden, die der Mensch beabsichtigt. Der Linguist Geoffrey K. Pullum bezeichnet daher die in SCI beschriebenen Anwendungen als prototypische Fälle, in denen natürlichsprachliche Ein-/Ausgabemöglichkeiten gerade nicht eingesetzt werden sollten.

»Die Computern innewohnenden und unüberwindbaren Beschränkungen machen sie nur unzuverlässiger, wenn auf ihnen KI-Programme laufen, und dies um so mehr, wenn sie natürlichsprachliche Ein-/Ausgabemöglichkeiten besitzen. Ihre Reaktionen auf unerwartete, mehrdeutige Äußerungen, vor denen man sich bei linguistisch ungeschulten Benutzern nicht schützen kann, werden immer unvorhersehbar sein.« (Pullum 1987, S. 56)

Doch als Benutzer dieser Systeme wären auch linguistisch geschulte Offiziere für Europa – und speziell für die Bundesrepublik – im wahrsten Sinne des Wortes vernichtend, sollten sie ihre erlernten Fähigkeiten anwenden. Der Nukleare Einsatzplan der Nato (NOP) wurde zusammen mit der Doktrin der flexiblen Antwort bereits 1968 in einem Dokument mit der Bezeichnung MC 14/3 festgelegt. Flexible Antwort heißt hier, daß man zuerst versucht, den Gegner auf der Ebene zu bekämpfen, die er selbst gewählt hat (direct defense). Mißlingt dies, geht man zur Strategie der begrenzten Eskalation über (deliberate escalation), die, im Falle ihres Scheiterns, als dritte Stufe den umfassenden Einsatz von Atomwaffen nach sich zieht (general nuclear response). »Aber die Dichte von atomaren Einheiten in der Bundesrepublik bedeutet, daß selbst begrenzte Angriffe massiv sein müßten.« (Pringle, Arkin 1985, S. 97) Durch die Behandlung unserer militärischen Sicherheit als technische Frage wird die Problemstellung so umdefiniert, daß sie mit den wirklichen Problemen nichts mehr zu tun hat (vgl. Bracken 1983, S. 129–178).

5 Das Verschwinden der Wirklichkeit

Den gegenwärtigen militärtechnologischen Überlegungen kommt nur dann eine Stimmigkeit zu, wenn man stillschweigend die Existenz eines kognitiven Perpetuum mobile der 3. Art voraussetzt. Bei dieser Art von Perpetuum mobile geht es darum, daß die Technologie wie auch die Problemstellung so komplex geworden sind, daß nur noch computergestützte Simulationsmodelle und nicht die Wirklichkeit zur Grundlage für die Analyse und Auswertung der technischen Systeme erklärt werden können.

Bereits jetzt gilt, daß in vielen militärischen Bereichen oftmals rechnergestütze Gefechtsmodelle die einzige Möglichkeit bieten,

»die Effizienz von Waffen-, Führungsinformations- und Aufklärungssystemen, Streitkräftestrukturen und taktisch/operativen Konzepten in reproduzierbarer Weise und unter realitätsnahen Einsatzbedingungen zu untersuchen. Eine empirische Überprüfung anhand historischer Gefechte scheidet mangels hinreichender Aufzeichnung meist aus. Angesichts der rasanten waffentechnischen Entwicklung wäre sie auch wenig relevant. Auch Truppenversuche und Gefechtsübungen unterliegen notwendigerweise verfemdenden Sicherheitsauflagen. Es verbleibt mithin allein die formale Simulation.« (Hofman 1986, S. 15)

Dieses gilt erst recht bei den neu zu entwickelnden Systemen, da sie ja speziell in Bereichen eingesetzt werden sollen, in denen der Mensch nicht in der Lage ist, schnell genug zu reagieren und zu entscheiden.

In der seit August 1982 vorliegenden Militärdoktrin ›Airland Battle 2000‹ wird das Konzept des ›intergrierten und erweiterten Schlachtfeldes‹ begründet und die Rolle der Computertechnik betont. Dazu heißt es u.a.:

»Der Einfluß, den die Technologie auf das Gefechtsfeld haben wird, ist gekennzeichnet durch größere Mobilität, höhere Feuerkraft, umfangreiche Manövrierkräfte, die unabhängig operieren können, sowie weitreichende Kampfpläne, die zwar kompliziert sein werden, jedoch mit Hilfe Künstlicher Intelligenz ohne weiteres synchronisiert und aufeinander abgestimmt werden können.« (Zit. n. Crumley 1985, S. 134)

Welche Folgen das hat, wird am Beispiel des integrierten amerikanischen Gesamteinsatzplanes für die Nuklearstreitkräfte deutlich. Die weitgehende Verschmelzung von Frühwarn- und Aufklärungsdaten sowie der kurze Zeitraum, in dem im Konfliktfall entsprechende Maßnahmen ergriffen werden müssen, erfordert, daß auch die Einsatzplanung automatisiert wird. Diese basiert auf einem umfangreichen Plan mit über 40.000 strategischen Zielen weltweit (SIOP, Single Integrated Operational Plan; vgl. Arkin, Fieldhouse 1985, S. 89, 93 u. 96). Die Verwaltung dieser Ziele ist nur mit Computern möglich; sie umfaßt die kontinuierlich notwen-

dige Aktualisierung und Erweiterung von Zielen sowie deren Zusammenfassung nach Prioritätsklassen gemäß entsprechender Einsatzstrategien. Nur so ist es möglich, im Sinne einer Strategie der flexiblen Antwort diese Zielpunkte geeignet auszuwählen und zu Einheiten zusammenzufassen, denen dann verschiedene Waffensysteme mit unterschiedlichem Zerstörungsgrad zugeordnet werden können.

Eine so detaillierte Einsatzplanung gründet notwendigerweise auf Annahmen, deren Richtigkeit nicht überprüfbar ist. Kriegsspiele *(war games)*, die auf einem Computer ablaufen, dienen dazu, SIOP regelmäßig auszuwerten und aufgrund der Interpretationen sowjetischer Kriegspläne zu akutalisieren. Diese Aktualisierung ist folglich rein hypothetisch. »Einer der Gründe dafür, daß der Prozeß weiter geht, die Daten verfeintert werden und die Annahmen eher wie Fakten aussehen, liegt in der Benutzung von Computersimulationen für den Planungsprozeß. Das System ist schon vor langer Zeit zu komplex geworden, um noch von Menschen gehandhabt werden zu können.« (Arkin, Fieldhouse 1985, S. 99)

Nach ausführlicher Analyse der technischen und militärpolitischen Aspekte kommen Peter Pringle und William Arkin (1983, S. 251) daher zu dem Schluß, daß die Optionen für diese Einsatzpläne sinnlos seien, weil sie lediglich auf theoretischen Angriffsmustern eines angenommenen Gegners unter Einbeziehung angenommener Gegenschläge basierten. Es sei nur eines sicher: daß ein Atomkrieg nicht gemäß eines vorher gefaßten Planes verlaufen werde.

Allerdings basieren nicht nur die Einsatzpläne auf computergestützten Simulationsmodellen, sondern auch für die Ausbildung der Offziere werden Simulationsprogramme benutzt. Gegenwärtige ›Kriegssimulationen‹ gehen von einem 60 Tage dauernden Atomkrieg aus. Da kein Mensch über Erfahrungen mit dieser Art von Krieg und Schlachtfeld verfügt, wird die menschliche Erfahrung durch das Training an solchen Simulatoren ersetzt. Dabei geht es nicht um »die Simulation von Krieg als einem analytischen Modell, sondern um Simulation als Erfahrung von Krieg für die Teilnehmer« (Cushman 1984, S. C1). Tatsächlich ist dieser Wirklichkeitsverlust vom Militär zumindest teilweise gewollt, denn ohne ihn könnten keine ›realistischen‹ Planspiele durchgeführt werden, bei denen der Einsatz von Atomwaffen vorgesehen ist. Nach Meinung von Carl Builder von der Universität Santa Barbara braucht man diese Kriegssimulationen, weil Menschen unter der Annahme, daß es sich um einen wirklichen Krieg handele, sich weigerten, Atomwaffen einzusetzen.

Was aber Offiziere in einer simulierten Wirklichkeit tun, widerspricht dem was bisher unsere Sicherheit ausmachte. Die Kommandeure kön-

nen die Wirkung ihrer Aktionen nicht mehr sinnlich erfahren und sich somit auch die Konsequenzen nicht vor Augen führen. »Sogar altgediente Hausdegen greifen relativ wahllos auf die Atombombe zurück«, sagt der Ausbildungsleiter vom Zentrum für Konfliktforschung am Lawrence Livermore Laboratorium (in den ZDF-Nachrichten am 27. 1. 1983), wo die Soldaten am Schlachtensimulator ›Janus‹ trainiert werden, der mit seinen 2.000.000 Befehlen pro Sekunde z.B. Angriffe mit Panzerdivisionen und deren Abwehr simuliert.

Je weniger der Mensch mit den unmittelbaren Konsequenzen seines Handelns konfroniert wird, und je weniger er beispielsweise durch den Einsatz ›autonomer Waffen‹ mit einem Verlust von Menschenleben rechnet, desto eher wird er in Konflikten auch Atomwaffen einsetzen (vgl. Beusmans, Wieckert 1987, S. 160). Mit künstlicher Intelligenz wird hier keine neue Qualität in der Entwicklung geschaffen, sondern die Ablösung von der Realität wird auf eine technisch elegantere Art und Weise vollzogen.

6 Fazit

In der Umgangssprache wird meist keine klare Unterscheidung zwischen Sicherheit und Zuverlässigkeit gemacht; auch Techniker neigen schnell zu dieser Gleichsetzung. Der Begriff Sicherheit ist aber weiter gefaßt als der Begriff Zuverlässigkeit. Gewöhnlich bezeichnet man ein System als zuverlässig, wenn es eine bestimmte Funktion über einen gewissen Zeitraum und unter festgelegten Umgebungsbedingungen so ausführt, wie es beabsichtigt ist. Sicherheit dagegen bezieht sich darauf, daß bestimmte Bedingungen, die zu Katastrophen oder Unfällen führen können, nicht eintreten, egal ob die beabsichtigte Funktion korrekt ausgeführt wird oder nicht (vgl. Leveson 1986, S. 135). Wesentlich für beide Begriffe ist, daß sie keine absoluten Werte verkörpern können, sondern lediglich Wahrscheinlichkeiten.

Wir befinden uns in einer Situation, in der sich Militärdoktrin und technische Entwicklung zu verselbständigen scheinen. Weltweite Aufklärung und flexible Einsatzplanung auf allen Konfliktebenen machen automatisierte Systeme zwingend erforderlich. Unter der Annahme, daß auch der Gegner über solche Systeme verfügt bzw. bald verfügen wird, ist es notwendig, eine neue Art von Technologie zu entwickeln, mit der man noch schneller, noch umfassender und noch flexibler reagieren kann. Neu ist dabei nicht die Entwicklung neuer Waffen mit einer höhe-

ren Vernichtungskraft, sondern deren zunehmende Integration und Automatisierung sowie die damit einhergehende Zentralisierung im militärischen Bereich.

Die Darstellung der militärtechnologischen Entwicklung hat gezeigt, daß eine neue Technologie nur dann unsere Sicherheit erhöhen kann, wenn wir bezüglich unserer Entscheidungsmöglichkeiten insgesamt weniger abhängig von der Technik werden. Dies gilt insbesondere unter der Voraussetzung, daß ein ›Hochtechnologiekrieg‹ im Schatten der Atombombe geführt werden wird. Die Verantwortung für die möglichen Folgen muß beim Menschen verbleiben. Ein Mensch kann aber nur verantwortlich handeln, wenn er auch Wahlmöglichkeit hat.

Maschinen gleich welcher Art verkörpern immer den Kenntnisstand ihrer menschlichen Schöpfer. Es gibt keine Maschinenevolution; Maschinen leben nicht, sie irren sich nicht und lernen nicht aus Fehlern. Eine Maschine wird von Menschen für einen bestimmten Zweck entworfen, gebaut und benutzt. Ihr Wert besteht darin, daß sie sich auf eine wohldefinierte und voraussagbare Art und Weise gemäß des gesetzten Zweckes verhält. Tritt ein Fehler auf, setzen sich Entwickler und Konstrukteure hin und analysieren den Fehler, um ihn zu beheben, eine verbesserte Konstruktion zu entwickeln, oder auch eine ganz neue Maschine. Sie können aber auch nach ganz anderen Wegen und Möglichkeiten suchen, um den gewollten Effekt zu erreichen.

Gegenwärtig sind KI-Systeme noch unzuverlässiger als traditionelle Softwaresysteme. Der Versuch, mithilfe dieser Systeme die Probleme der traditionellen Systementwicklung zu lösen, um noch komplexere Systeme entwickeln zu können, erweist sich als die Suche nach einem kognitiven Perpetuum mobile. Bezüglich des Einsatzes und der Benutzung von KI-Systemen werden die Probleme der Realitätsablösung nicht überwunden, sondern eher verstärkt. Selbst wenn es gelänge, die in SDI und SCI geforderte Leistungsfähigkeit von KI-Systemen mit der erforderlichen technischen Zuverlässigkeit zu entwickeln, würde dadurch unsere militärische Sicherheit nicht wachsen. Der Mensch würde aus den wesentlichen Entscheidungsabläufen gedrängt und sein Handlungs- und Entscheidungsspielraum würde sich verringern.

Nicht der Glaube an die Zuverlässigkeit von KI-Systemen kann uns daher Sicherheit geben. Unsere Sicherheit besteht darin, daß der Mensch sich seiner Unzuverlässigkeit bewußt ist und damit auch der Unzuverlässigkeit seiner Produkte. Das Mißtrauen gegenüber komplexen technischen Großsystemen, die Angst vor Katastrophen schafft ein kreatives Potential für die Suche nach anderen, auch nicht-technischen Lösungen. Ängste, Wünsche, Hoffnungen und Ideale sind ein

wesentlicher Bestandteil unserer natürlichen Intelligenz; ohne sie wäre sie sinnlos.

Wir leben jedoch in einer kulturellen Umgebung, in der uns die Perfektion unserer technischen Produkte häufig mehr wert ist als der Mensch mit seinen Fähigkeiten. Der Philosoph Günther Anders hat dies als »Prometheische Scham« bezeichnet. Darunter versteht er die »Scham vor der ›beschämend‹ hohen Qualität der selbstgemachten Dinge« (1981, Bd. 1, S. 23; vgl. insbes. S. 59–64). Selbst einige Wissenschaftler, die die militärtechnologische Entwicklung kritisieren und die damit verbundenen Gefahren aufzeigen, setzen mehr Vertrauen in die künstliche Intelligenz als in den Menschen (vgl. Bläsius, Siekmann 1987, S. 38).

Doch Krieg »ist nicht in erster Linie ein kognitives Ereignis« (Edwards 1986, S. 39). Wir dürfen uns nicht durch die Träume von regelbasierten, simulierten, formalen Lösungen hinters Licht führen lassen, sagt Paul Edwards, sondern was wir benötigten, wäre das volle Spektrum der menschlichen Fähigkeiten, um nach Alternativen zum Krieg zu suchen. Wir werden dazu viel Fantasie und Vertrauen brauchen. Vertrauen aber müssen wir in erster Linie unseren potentiellen Gegnern entgegenbringen und nicht einer Technik, deren alleiniges Ziel es ist, das Töten effektiver zu machen. KI-Systeme können nicht vertrauen. Sie kennen weder Angst noch Liebe; sie sind bestenfalls berechnend.

Literatur

Anders, G.: Die Antiquiertheit des Menschen, 2 Bde., München 1981

Aldridge, R. C.: The Counterforce Syndrome: A Guide to U.S. Nuclear Weapons and Strategic Doctrine, New York/Amsterdam, 1981

Arkin, W. M., Fieldhouse R. W.: Nuclear Battlefields. Global Links in the Arms Race, Cambridge, Ma., 1985

Belady, L. A., Lehman, M. M.: Characteristics of Large Systems, in: Wegner (1979)

Beusmans, J., Wieckert, K.: Computing, Research, and War: If »Knowledge is Power«, Where is Responsibility. Proc. Directions and Implications of Advanced Computing; Seattle, Wa.: July, 12, 1987

Bickenbach, J., Keil-Slawik, R., Löwe, M., Wilhelm, R. (Hg.):Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden, Nr. 4, FIFF Berlin; Marburg/Berlin/Münster, 1985

Bläsius, K. H., Siekmann J. H.:Computergestützte Frühwarn- und Entscheidungssysteme. Informatik-Spektrum; Band 10, Heft 1; 1987

Borning, A.: Computer System Reliability and Nuclear War. Communications of the ACM; Vol. 30, No. 2; 1987

Bracken, P.: The Command and Control of Nuclear Forces, New Haven/London, 1983

Brödner, P.: Thesen über Menschliche Kreativität und Künstliche Intelligenz. Vorgelegt zur Anhörung der Enquete-Kommission »Technologiefolgen-Abschätzung« des Deutschen Bundestages; 12. Mai 1986
Crumley, D. V.: Konzepte für den Einsatz von Robotern mit Künstlicher Intelligenz durch das Heer im 21. Jahrhundert. In: Bickenbach, Keil-Slawik, Löwe, Wilhelm (1985)
Cushman, J. H.: Warfare Simulation. Appendix C, in: Secretary of Defense (1984)
DARPA: The DARPA Program. A Proposed Strategic Plan for the Development und Application of Next-Generation Technology for the Military, in: Torrero, E. A. (ed.): Next-Generation Computer. Spektrum Series, New York, 1985
Davis, P. K.: Applying Aritficial Intelligence Techniques to Strategic-Level Gaming and Simulation, in: Ören, E. T. I., Ziegler, B. P. (eds).: Modelling and Simulation Methodology in the Artificial Intelligence Era, Amsterdam/New York/Oxford, 1986
Edwards, P. N.: Artificial Intelligence and High Technology War. The Perspective of the Formal Machine. Silicon Valley Research Group; Working Paper No. 6; Universitiy of California, Santa Cruz, 1986
Eigen, M., Winkler, R.: Das Spiel. Naturgesetze steuern den Zufall, München/Zürich 1983
Fallows, J.: National Defense, New York, 1981
Hamlet, R.: Testing for Trustworthiness. Proc. Directions and Implications of Advanced Computing; Seattle, Wa., July, 12, 1987
Hart, G., Goldwater, B.: Recent False Alerts from the Nation's Missile Attack Warning System. U.S. Government Printing Office; Washington D.C., October, 9, 1980
Hofman, H. W.: Einsatz moderner Informationstechnik im militärischen Bereich: Für den Verteidiger notwendig und verantwortbar. Informatik-Spektrum; Band 10, Heft 1; 1987
Jacky, J.: The »Star Wars« Defense Won't Compute. The Atlantic, Vol. 225, No. 6; June 1985
Keil-Slawik, R.: Von der Feuertafel zum Kampfroboter – Die Entwicklungsgeschichte des Computers. In: Bickenbach, Keil-Slawik, Löwe, Wilhelm (1985)
–: Von der Ökologie des Geistes zur Mechanisierung des Kopfes, in: Stöhr, M., Wendt, H. (Hg.): Menschliche und künstliche Intelligenz, Band 1, Frankfurt 1989a
–: Fehlerquellen in der militärischen Nutzung künstlicher Intelligenz, in: ebd., Band 2, 1989b
Leveson, N. G.: Software Safety: Why, What, and How. Computing Surveys; Vol. 18, No. 2; June 1986
Naur, P.: Programming as Theory Building. Microprocessing and Microprogramming 15; North Holland Publ. Comp.; 1985
Ornstein, S. M.: Deadly Bloopers. Manuscript; Computer Professionals for Social Responsibility (CPSR); Palo Alto, Ca., June, 16, 1986
Parnas, D. L.: Software Wars, in: Kursbuch 83, Berlin, 1986 a
–: Interview mit Ina Hönicke, in: Die Grünen; Dezember 1986 b
Petroski, H.: To Engineer is Human: The Role of Failure in Succesful Design, New York, 1985
Pringle, P., Arkin, W.: S.I.O.P. The Secret U.S. Plan for Nuclear War, New York/London, 1983
Pullum, G. K.: Natural Language Interfaces and Strategic Computing. AI & Society; Vol. 1, No. 1, 1987

Rasmussen, J.: Human Error Data. Facts and Fiction. Risø National Laboratory; Report Risø-M-2499; Roskilde, March 1985
Ryle, G.: The Concept of Mind, Harmondsworth, 1983
Secretary of Defense: Report of the Defense Science Board Task Force on Military Applications of New-Generation Computing Technologies. Office of the Under Secretary of Defense for Research and Engineering; Washington, D.C., December 1984
Smith, B. C.: Limits of Correctness in Computers. Stanford University; Center for the Study of Language and Information; Report No. CLSI-85-36; Palo Alto, Ca., October 1985
Struß, P.: Gibt es Expertensysteme? computer magazin; Jahrg. 15, Nr. 5, 1986
Thompson, H.: Und immer wieder geht der Mond auf – Computertechnik und Atomwaffen, in: Bickenbach, Keil-Slawik, Löwe, Wilhelm (1985); S. 121–125
Winograd, T., Flores, F.: Understanding Computers and Cognition. A new Foundation for Design, Norwood, N.J., 1986