SDI Considered Harmful -
Ansätze zum Umdenken in der Softwaretechnik

Reinhard Keil-Slawik

Technische Universität Berlin
Institut für Angewandte Informatik
Franklinstr. 28/29, Sekr. FR 5-6
D-1000 Berlin 10

Einleitung:

Es gehört zur bisherigen Geschichte der Informatik, daß fast alle großen Entwicklungsetappen durch staatliche bzw. öffentliche Maßnahmen eingeleitet worden sind. Oft sind die wesentlichen Impulse vom Militär ausgegangen. Beispiele dafür sind u.a.:

- der schnelle Wechsel von Analog- zu Digitalrechnern,
- die Ersetzung von Röhren durch Transistoren und diese später durch ICs,
- der Aufbau von Rechnernetzen,
- die Entwicklung und Standardisierung von Programmiersprachen,
- die Entwicklung von Computersystemen der 5. Generation (speziell in den USA).

Die enormen, für die jeweiligen Forschungs- und Entwicklungsprogramme bereitgestellten Mittel sowie die Geschwindigkeit mit der jeweils das nächste Vorhaben mit höheren Anforderungen und erweiterten Aufgabenbereichen in Angriff genommen wird, führen dazu, daß für die beteiligten Wissenschaftler weder das Verhältnis von Aufwand und Nutzen bei solchen Vorhaben im Vordergrund steht, noch die Überprüfung der Gültigkeit einzelner Forschungshypothesen.

Mit der Projektierung des größten und komplexesten Softwaresystems, das im Rahmen der strategischen Verteidigungsinitiative SDI (Strategic Defense Initiative) entwickelt werden soll, wird die Diskrepanz zwischen Anspruch und Wirklichkeit erstmals zum allgemeinen Diskussionsthema. Sowohl die technische Machbarkeit als auch die politische Wünschbarkeit werden zunehmend von DV-Fachleuten angezweifelt.

Da SDI in seiner Komplexität schwer faßbar ist skizziere ich zuerst wesentliche der mit SDI verbundenen Probleme anhand der bisher entwickelten großen militärischen Systeme. Dabei wird deutlich, daß die Entwicklung neuerer und größerer Systeme erfolgt, obwohl grundlegende Probleme noch ungelöst sind. Die Beschreibung des zentralen Schlachtenführungssystems für SDI und der damit verknüpften Anforderungen zeigt, daß mit SDI diese Tradition fortgesetzt wird. Zudem ist erkennbar, daß die heute in der Softwaretechnik bestehenden Probleme durch dieses Großprojekt nicht beseitigt, sondern angesichts der enormen Komplexität eher zunehmen werden. Diese Situation ist für viele Informatiker ein Anlaß zum Umdenken.

1. Probleme großer militärischer Softwaresysteme

Bedingt durch den Schock von Pearl Harbour werden vom amerikanischen Militär enorme finanzielle Mittel für die Entwicklung von computergestützten Frühwarnsystemen bereitgestellt. Angeregt durch die Leistungsfähigkeit des für ballistische Berechnungen entwickelten Rechners ENIAC (1946) beschließt die Projektgruppe "Whirlwind" am MIT unter der Leitung von Jay W. Forrester statt des projektierten Analogrechners einen Digitalrechner zu entwickeln, der aufgrund der aktuellen militärischen Erfordernisse nicht wie geplant als Flugsimulator, sondern als Kernstück eines Flugüberwachungssystems konzipiert wird. Über Telefonleitungen werden Daten übermittelt und aufgezeichnet, die die Flugüberwachungsoffiziere an Radargeräten mit einer Zeicheneingabe für die Positionsangabe eines identifizierten Flugobjektes eingeben. Das Whirlwind-Projekt bringt zwar viele hardwaretechnische Neuerungen wie 16 Bit-Prozessor, Magnetkernspeicher, Lichtgriffel etc., doch werden zugleich auch Grenzen sichtbar. Zehn Jahre nach der Fertigstellung wird der Betrieb von Whirlwind 1959 eingestellt. Das wichtigste Argument sind neben den Betriebskosten von 300.000 Dollar die hohen Wartungskosten für die Software.

Das Projektteam entwirft, ausgehend von Whirlwind die neuen Computer für SAGE (Semi-Automatic Ground Environment air defense system). SAGE ist das zur damaligen Zeit ambitionierteste DV-Projekt des Militärs. Neben dem Bau von 24 Großrechnern für die Hauptquartiere der Air Defense Division (combat centers) müssen rund 2.000 Programmierer ausgebildet werden, damit das Projekt realisiert werden kann. Wiederum hardwaretechnisch erfolgreich ist SAGE jedoch nach einem Bericht des ehemaligen Beraters von Präsident Kennedy, James FALLOWS ein Fehlschlag: nachdem über 20 Milliarden Dollar investiert worden sind, scheitert 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 kreuzen. Doch noch ein anderes Problem offenbart SAGE. Bereits kleinere Störungen im Radarbild würden das System lahmlegen, wenn sich die Mannschaften an die festgelegten Regeln und Vorschriften halten würden. Die Operateure schafften es, so BRACKEN, irgendwie um das System herumzuarbeiten; doch niemals erschienen die mündlichen Übereinkünfte der Bediener in einem offiziellen Report.

SAGE ist nur eines von mehreren Ende der 50er Jahre für die Luftwaffe entwickelten Computersystemen, die aufgrund ihrer Code-Bezeichnung auch als große "L-Systeme" bezeichnet werden (vgl. Tabelle 1). Die Systeme sind miteinander verknüpft und bilden quasi ein einziges großes Frühwarn- und Entscheidungssystem.

117L	MIDAS	(Missile Defense Alarm System)
416L	SAGE	(Semi-Automatic Ground Environment Air Defense)
425L	NORAD	(North American Air Defense)

438L	AFIDHS	(Air Force Intelligence Data Handling System)
465L	SACCS	(Strategic Air Command (SAC) Control System)
474L	BMEWS	(Ballistic Missile Early Warning System)

Tabelle 1: In den 50er Jahren entwickelte Frühwarn- und Entscheidungssysteme (heute teilweise durch neuere Versionen abgelöst)

In den 60er und 70er Jahren werden diese Systeme erweitert, modifiziert und integriert. Im Kommandobunker von NORAD in den Cheyenne Mountains laufen alle Informationen zusammen. Hier werden sie ausgewertet und die entsprechenden Einsätze der Nuklearstreitkräfte ausgelöst. Wie sicher diese Systeme sind, zeigt die Tatsache, daß man es nach einem Bericht der Senatoren HART und GOLDWATER schaffte, allein im Jahre 1979 mit mehr als 1.500 Fehlalarmen umzugehen, ohne daß es zu einer Katastrophe gekommen ist.

Auch hier gilt, wie bei SAGE, daß die Sicherheit der Systeme, soweit man unter solchen Bedingungen überhaupt von Sicherheit reden darf, nicht in der Zuverlässigkeit der Technik liegt, sondern im flexiblen Umgang des Menschen mit dieser Technik. Die größte Sicherheit aber, liegt wohl in der Tatsache begründet, daß die Kommandeure in den Zeiten relativer Entspannung in ihrer Erwartungshaltung eher auf einen Fehlalarm vorbereitet sind, folglich die Zuverlässigkeit der Computersysteme einen anderen Stellenwert besitzt als in Krisen- und Konfliktzeiten.

Je mehr die Menschen aber durch die zunehmende Integration und Automatisierung aus den Entscheidungsprozessen gedrängt werden, desto unzuverlässiger wird das Gesamtsystem. So war das weltumspannende Frühwarn- und Entscheidungssystem WWMCCS (World Wide Military Command and Control System; gesprochen wimmex) als es 1977 gründlich getestet wurde 62% der Zeit nicht einsatzbereit, Teile des Netzes sogar 85% der Zeit. Doch selbst wenn es heute funktionieren würde, wäre es nach FALLOWS von zweifelhaftem Wert: nach einer NATO-Studie müßten die Kommandeure des zentralen Kommandobunkers für Europa rund um die Uhr 790 Worte pro Minute lesen, um mit dem Informationsstrom des Systems Schritt halten zu können. Ein Systemtest am 6. November 1980 zeigte zudem, daß die Kommandeure während der angenommenen Krisenzeit über 12 Stunden keine wesentlichen Informationen über den Bereitschaftszustand ihrer Truppen erhielten. Das heißt, das System liefert zu viele Daten und die sind großenteils für die anstehenden Entscheidungen nicht relevant.

Die Einsatzplanung für die amerikanischen Nuklearstreitkräfte basiert auf einem umfangreichen Plan mit über 6.000 strategischen Zielen in der Welt (SIOP, Single Integrated Operational Plan). Dieser Plan wird mit Hilfe von Computern verwaltet. Im Sinne einer Strategie der flexiblen Antwort sollen diese Zielpunkte nach unterschiedlichen Kriterien ausgesucht und zu Einheiten zusammengefaßt werden, denen dann verschiedene Waffensysteme mit unterschiedlichem Zerstörungsgrad zugeordnet werden. Eine solche "flexible" Einsatzplanung setzt aber voraus, daß sowohl die Aktionen des Gegners be-

kannt sein müssen als auch, daß eine Bewertung (assessment) über Truppenstand, Zerstörungsgrad von Angriffszielen, Umfang vorhandener Ressourcen etc. sowohl bei Freund' als auch Feind vorgenommen werden kann. Tatsächlich ist dies technologisch kaum realisierbar, weil beispielsweise weltraumgestützte Lichtsensoren lediglich Lichtstrahlen von Explosionen registrieren, nicht aber den Grad der Zerstörung und die Art der Explosion. Zerstörungen durch radioaktiven Fallout können beispielsweise nur unter Einbeziehung der globalen Wetterlage analysiert werden. Dies allein würde einen Großrechner vollauf auslasten.

Nach ausführlicher Analyse kommen ARKIN und PRINGLE zu dem Schluß, daß die Optionen für diesen Einsatzplan (SIOP) sinnlos sind, weil sie lediglich auf theoretischen Angriffsmustern eines angenommenen Gegners unter Einbeziehung angenommener Gegenschläge basieren und lediglich eines sicher sei, nämlich daß ein Atomkrieg nicht gemäß eines vorher gefaßten Planes verlaufen würde.

Die Gesamtintegration all der bisher angesprochenen Komponenten und Teilsysteme wird durch den Begriff des C^3I-Systems charakterisiert (Command, Control, Communications and Intelligence). Für das Militär ist C^3I die Zauberformel für die elektronische Kriegführung, für deren Verbesserung das amerikanische Verteidigungsministerium allein im Haushaltsjahr 1985 etwa eine Milliarde Dollar zur Verfügung gestellt hat. Ein solches C^3I-System oder auch Schlachtenführungssystem soll auch das elektronische Herz für SDI werden. Präsident Reagan hatte am 23. März 1983 in einer Rede an die amerikanische Nation seine Vision vorgestellt, mit Hilfe von SDI Atomwaffen unwirksam und obsolet zu machen.

PARNAS stellt angesichts dieser Pläne klar, daß wir als Informatiker über keinen technologischen Zauber verfügen, Atomwaffen überflüssig zu machen. Wie die Vergangenheit zeigt, sind die mit solchen Systemen verbundenen Probleme bisher weder technologisch noch politisch gelöst, noch haben wir Anhaltspunkte dafür, wie sie gelöst werden könnten.

2. Das Schlachtenführungssystem für SDI

Nach dem FLETCHER-Report ist das Kernstück von SDI ein zentrales Schlachtenführungssystem. Es besteht aus mehreren teilautonomen Subsystemen (Schichten) für die Ausführung der jeweils spezifischen Aktivitäten, die den jeweiligen Flugphasen einer Interkontinentalrakete zugeordnet werden (vgl. Abbildung 1). Lokale Funktionen für jedes Subsystem sind die Flugbahnerkennung und -verfolgung (track), die Bewertung von Objekten (classify), z.B. die Unterscheidung zwischen Sprengköpfen und Täuschungsobjekten oder die Bestimmung der Wahrscheinlichkeit, daß ein Ziel vernichtet worden ist, und

die Zuordnung von Ressourcen (allocate), also von Waffen und Sensoren zu Zielen. Die Subsysteme sind untereinander verbunden indem die in den Flugphasen gewonnenen Daten jeweils weitergegeben werden. Darüberhinaus gibt es die Komponente "Wissen über die aktuelle Situation". Das ist eine logische Aggregation aller Informationen, die für die Funktionen der Schlachtenführung relevant sind.

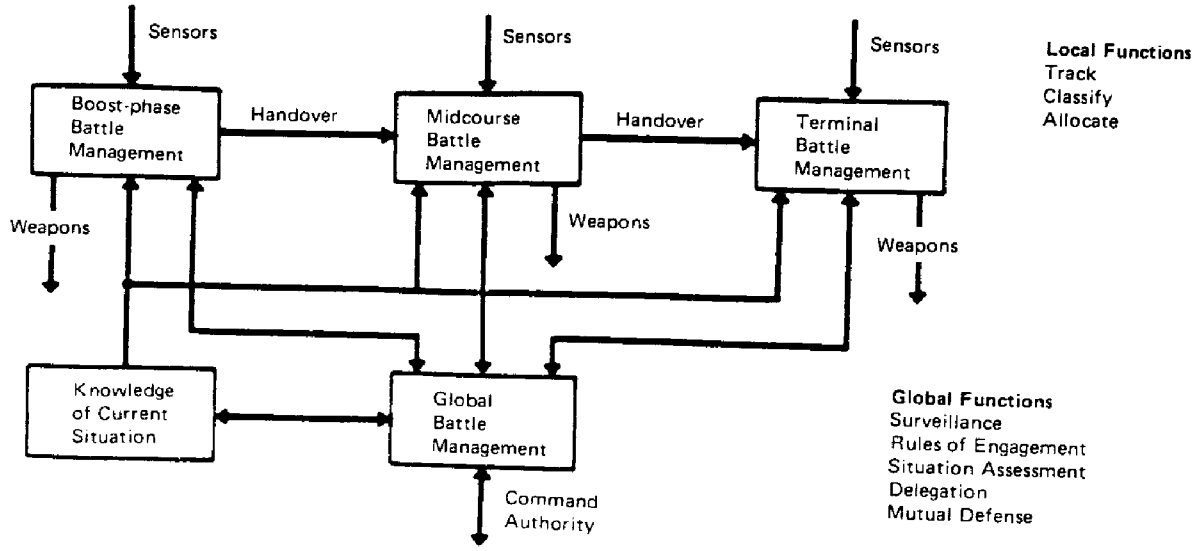

Abbildung 1: Schichtenmodell eines Schlachtenführungssystems

Die globalen Funktionen des Systems sind diejenigen, die sich auf die Verbindung der Subsysteme beziehen oder aber mehrere Phasen der Schlachtenführung umfassen. Nach FLETCHER beinhalten sie:

- Überwachung (surveillance): "Diese Funktion übernimmt die Ausgabe des Erkennungssystems, bestätigt, daß ein Angriff initiiert worden ist, und stellt eine Einschätzung über die Art des Angriffs zur Verfügung."
- Regeln des Eingriffs (rules of engagement): "Diese Funktion enthält die Doktrin für die Schlachtenführung. Basierend auf der empfangenen Einschätzung über die Art des Angriffs würde diese Funktion die entsprechende Reaktion auswählen ... Die Möglichkeit, Nuklearwaffen einzusetzen, ist in dieser Funktion enthalten."
- Einschätzung der Situation (situation assessment): "Diese Funktion erstellt eine gegenwärtige Einschätzung über den Zustand der Feindseligkeiten und den Status der verschiedenen Verteidigungsressourcen. Dies ist eine kontinuierliche Funktion, die in Friedenszeiten ebenso wie in einer Schlacht ausgeführt wird."
- Übermittlung (delegation): "Diese Funktion beinhaltet den Wechsel der Steuerung von einer Operation zur nächsten und die Koordination zwischen den verschiedenen Schichten. Daten aus der Flugbahndatei werden zusammen mit Steuerinformationen an die nächste Operation oder die nächste Schicht der Verteidigung übertragen."

- Wechselseitige Verteidigung (mutual defense): "Diese Funktion koordiniert und verwaltet die Ressourcen im Verteidigungssystem, damit das System überlebt ... Wechselseitige Verteidigung muß die Verteidigung des gesamten Systems betrachten und sicherstellen, daß es keine angreifbaren Bindeglieder gibt."

An die Software von SDI werden Anforderungen in einer bisher nicht gekannten Größenordnung gestellt. Der Umfang beträgt ca. 10 Millionen Code-Zeilen. Jede weltraumgestützte Sensor- und Waffenplattform enthält eine vollständige, exakte Kopie der Datenbasis des Schlachtenführungssystems, der Computer und der Software; damit können sie "autonom reagieren". Aufgrund der räumlichen Verteilung des Systems werden Entfernungen in Millilichtsekunden gemessen. Ohne zusätzliche Techniken der Zwischenspeicherung oder der Zeitettiketierung werden die getrennten Datenbasen durch Intervalle aus der Synchronisation geraten, die mehrere tausend Rechenzyklen umfassen können. Während einer Schlacht wird es eine Überfütterung an Informationen geben, daher müssen menschliche Entscheidungen, speziell in der Startphase von Raketen, weitgehend durch automatisierte Entscheidungsprozesse ersetzt werden, Daten müssen aggregiert werden und Entscheidungen über den Einsatz von Waffen - auch von Atomwaffen - auf einfache Menues zum Auswählen reduziert werden. Handlungsalternativen, die den Kommandeuren zur Verfügung stehen, müssen entsprechend in ihrer Anzahl und ihrer Komplexität begrenzt sein. Neue Bewertungsalgorithmen mit einer bisher nicht gekannten Komplexität müssen entwickelt werden, die auf eine veränderliche Schlachtensituation reagieren, unterschiedliche Waffensysteme steuern, teilweise Zerstörungen überstehen können und Objekte behandeln, die nicht eindeutig identifiziert werden können, sowie komplizierte Eingriffsregeln auslösen. Das System kann nie unter realistischen Bedingungen getestet werden. Die Entwicklung des Systems wird mehrere Jahre dauern und so komplex sein, daß kein Individuum jemals das System vollständig durchschauen wird.

All dies sind Anforderungen, die in der FLETCHER-Studie benannt werden. Sie werden als Herausforderung (challenge) an die Informatik verstanden.

3. Die Herausforderung an die Softwaretechnik

Im zweiten Abschnitt wurde skizziert, welche Probleme mit großen militärischen Systemen verbunden sind und daß diese Probleme bis heute nicht gelöst sind. Weder die Beherrschbarkeit noch die Zuverlässigkeit dieser Systeme konnte bis jetzt glaubhaft demonstriert werden. Bezüglich der Anforderungen an die SDI-Software läßt sich feststellen, daß der Problemdruck ungeheuer verstärkt wird. Statt die Probleme zu verkleinern bzw. partiell zu isolieren, um zu handhabbaren Lösungen zu gelangen, sollen bisher nicht gelöste Probleme im Rahmen eines noch komplexeren Gesamtsystems angegangen werden. Dies beinhaltet zusätzliche und teilweise noch nicht bekannte Probleme. Mit SDI

kann folglich eine forschungsstrategische Perspektive für die Softwaretechnik kaum geltend gemacht werden.

Aber auch ein relevanter Fortschritt in Einzelbereichen scheint mit SDI nicht erreichbar. Der Softwaretechnikexperte Prof. PARNAS, der bisher u.a. auch Forschung für militärische Einrichtungen durchgeführt hat und als Fachmann in die wissenschaftliche Projektkommission für SDI berufen werden sollte, lehnte eine Teilnahme an SDI trotz der damit verbundenen finanziellen und wissenschaftlichen Anreize ab. In seinem Rücktrittsschreiben an den Leiter der SDI-Kommission, begründet PARNAS seine Entscheidung, indem er, unter Hinweis auf die Besonderheiten softwaretechnischer Systeme, aufzeigt, warum die mit SDI gestellten Anforderungen nicht erfüllbar sind bzw. daß die geforderte Software unzuverlässig sein wird. Er setzt sich mit den herkömmlichen und mit neuen, von der Fletcher-Kommission geforderten Methoden der Softwareentwicklung auseinander und zeigt anhand seiner Erfahrungen, daß die von der Kommission vorgeschlagenen Methoden zur Programmierung und Programmverifikation ebensowenig wie künstliche Intelligenz und Expertensysteme zur Lösung der Probleme geeignet sind.

Da es sich bei der SDI-Software überwiegend um Größenordnungen handelt, mit denen selbst die meisten Softwaretechniker nicht vertraut sind, soll hier zur Illustration ein kurzes Beispiel gegeben werden. Das größte bisher für das Militär entwickelte Einzelsystem ist SAFEGUARD. Es hat mit zwei Millionen Programmzeilen nur ein fünftel des Umfangs der projektierten SDI-Software. Die Entwicklungszeit betrug sechs Jahre, wobei in Spitzenzeiten bis zu 1.200 Entwickler an der Erstellung des Systems beteiligt waren. Bezüglich der SDI-Software kommt LIN bei seiner Aufwandsabschätzung auf 13.400 Menschjahre bei optimistischer und 81.700 Menschjahre bei pessimistischer Prognose. Bei einer Entwicklungszeit von 20 Jahren wären das im ungünstigsten Fall rund 4.000 Entwickler, die am Projekt ununterbrochen beteiligt wären.

Aufgrund des für SDI veranschlagten Gesamt-Budgets - nach HORNING handelt es sich dabei um ein Billion-Dollar-Projekt (10^{12} $) - wären die Kosten vergleichsweise problemlos. Jedoch weist die Zahl der beteiligten Entwickler auf ein grundlegenderes Problem hin: Software mit einem größeren Umfang ist nicht einfach nur größer, sondern ist in jeder Hinsicht auch mit qualitativ anderen Problemen behaftet. Eine Gruppe von 15 Programmierern kann ein gutes Team bilden; 4.000 Programmierer benötigen jedoch eine bürokratische Organisation. Geht es bei herkömmlichen technischen Systemen meistens darum, für eine bereits bekannte Funktion eine verbesserte technische Realisierung zu finden, so beinhaltet die Entwicklung von Software die Schaffung neuer, bisher noch nicht bekannter Funktionen.

Angesichts der qualitativen Andersartigkeit und der Neuheit der zu realisierenden Funktionen, verlieren Vorschläge, Expertensysteme oder Programmgeneratoren einzuset-

zen, an Bedeutung. Beides setzt voraus, daß der Problembereich von Menschen hinreichend gut durchdrungen ist, d.h. daß die Aktivitäten eines Experten fast standardisiert bzw. routinehaft ablaufen, denn nur dann kann das Verfahren durch Regeln beschrieben werden. Große militärische Systeme erfüllen diese Voraussetzungen nicht und qualitativ neue Software per definitionem auch nicht.

Erstmals werden mit SDI Erwartungen an die Leistungsfähigkeit von DV-Systemen formuliert, die aufgrund der vorhandenen Erfahrungen nicht erfüllt werden können. Damit erhält die Herausforderung an die Softwaretechnik einen neuen Sinn: SDI wird zum Anlaß für viele Informatiker, umzudenken, nicht mehr die technologischen Größenordnungen bzw. die Leistungsfähigkeit von DV-Systemen als alleiniges Bewertungskriterium für ihre Arbeit gelten zu lassen, sondern auch Werte und Wertvorstellungen einzubeziehen, die sich an politischen, sozialen und humanen Gegebenheiten orientieren.

4. Umdenken in der Softwaretechnik

Während einer internationalen Tagung mit dem Thema "Theory and Practice of Software Development (TAFSOFT)", die im März 1985 in Berlin durchgeführt wurde, gab es eine vom FIFF-Berlin (Forum Informatiker für Frieden und gesellschaftliche Verantwortung) durchgeführte Podiumsdiskussion zur Verantwortung der Informatiker, die sich einer überaus hohen Teilnehmerzahl erfreute.

Neben vielen anderen international angesehenen Wissenschaftlern beteiligte sich auch Prof. Parnas engagiert an der Diskussion. In einem Schreiben an die Initiatorin der Diskussion betonte Parnas einige Monate später, daß ihm diese Diskussion bezüglich seiner Entscheidung, sich nicht an der SDI-Kommission zu beteiligen, sehr geholfen habe.

So wie Parnas haben sich weltweit viele Informatiker in den letzten zwei bis drei Jahren mit ihrer Verantwortung als Informatiker beschäftigt. Speziell die Softwaretechniker erkennen zunehmend, daß sie sich umso mehr mit außerwissenschaftlichen Fragen beschäftigen müssen, je mehr ihre Arbeit durch von außen gesetzten Zielen bestimmt und beeinflußt wird. Beispiele insbesondere für die militärische Durchdringung der Forschung und Entwicklung sowie für erste Ansätze des Umdenkens finden sich in BICKENBACH, ET AL unter dem Titel "Militarisierte Informatik".

Doch nicht nur bezüglich außerwissenschaftlicher Fragen findet ein Umdenken statt, sondern auch bezüglich unserer Techniken und Methoden. Haben sich Softwaretechniker bisher nur auf die technologischen Leistungsmerkmale bezogen, so wird heutzutage die Notwendigkeit einer stärkeren Orientierung auf den Menschen hervorgehoben. Was für

die großen militärischen Systeme im besonderen geltend gemacht wird, hat auch für kleinere zivile Systeme seine Gültigkeit, nämlich

- daß Angemessenheit von Software bedeutet, auch den Zweck zu bewerten, für den die Software entwickelt werden soll
- daß die Qualität von Software wesentlich vom Verständnis der an der Entwicklung beteiligten Personen abhängt
- daß die Benutzung von Software umso besser ist, je mehr dem Benutzer Handlungs- und Entscheidungsmöglichkeiten eröffnet werden
- daß wesentliche Voraussetzung für qualitativ gute Software die Initiierung von Lernprozessen sowohl bei Entwicklern und Benutzern ist.

Auch wir Informatiker müssen uns klar darüber sein, daß wir bei all unseren technischen Möglichkeiten versagen, wenn es uns nicht gelingt, Technik auf die Bedürfnisse und Erfordernisse des Menschen abzustimmen.

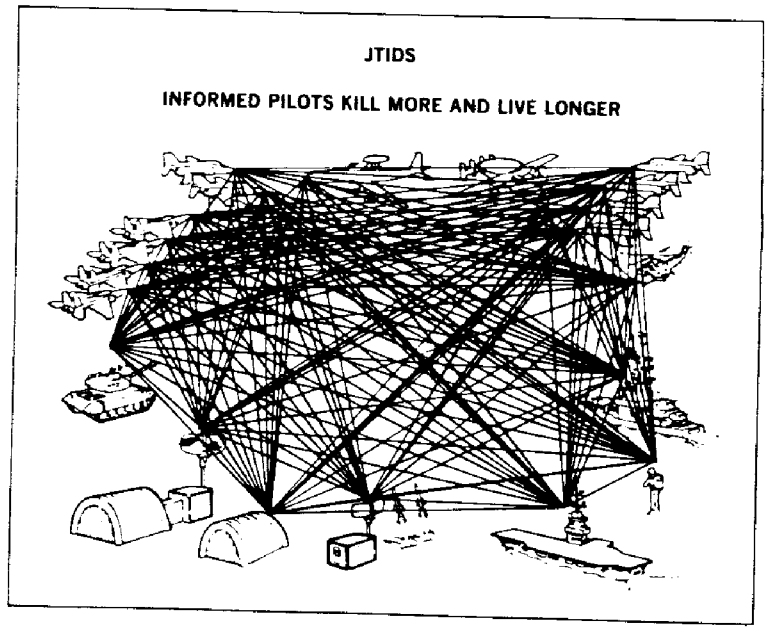

Abbildung 2: Komplexität militärischer Systeme (aus FALLOWS, S. 53)

Mehr Informationen zu besitzen ist nicht, wie dies in Abbildung 2 nahegelegt wird, grundsätzlich ein Fortschritt.

Auch wenn SDI technisch machbar wäre, ist meines Erachtens die Grenze des Vertretbaren erreicht.

Literatur

BICKENBACH, J., KEIL-SLAWIK, R., LÖWE, M., WILHELM, R. (Hg.): Militarisierte Informatik; Schriftenreihe Wissenschaft und Frieden, Nr.4, Juni 1985. Zu beziehen bei FIFF-Berlin, c/o Rudolf Wilhelm, Württembergische Str. 31, 1000 Berlin 15 (Einzelpreis 13,- DM)

BRACKEN, P.: The Command and Control of Nuclear Forces; Yale University Press; New Haven London 1983

FALLOWS, J.: National Defense; Random House; New York 1981

FLETCHER, J.C. (Study Chairman): Report of the Study on Eliminating the Threat Posed by Nuclear Ballistic Missiles; Vol.V, Battle Management, Communications, and Data Processing; Februar 1984

HART, G., GOLDWATER, B.: Recent False Alerts from the Nation's Missile Attack Warning System; Report to the Committee on Armed Services United States Senate; U.S. Government Printing Office; Washington 1980

HORNING, J.J.: Trip Report: Computing in Support of Battle Management; 20.8.1985; Eine deutsche Übersetzung ist in KURSBUCH 83 erschienen; S. 71-76; Berlin 1986

KURSBUCH 83: Krieg und Frieden - Streit um SDI; Kursbuch / Rotbuch Verlag; Berlin; März 1986

PARNAS, D.: Letter To Mr. James H. Offut, Assistant Director, BM/C3, Strategic Defense Initiative Organization; 28.6.85. Auf Deutsch veröffentlicht in mehreren Rundbriefen des FIFF sowie auszugsweise in KURSBUCH 83; S. 49-69; Berlin 1986

PRINGLE, P., Arkin, W.: S.I.O.P. The Secret U.S. Plan for Nuclear War; W.W. Norton & Company; New York, London 1983

LIN, H.: Software für Raketenabwehr im Weltraum; Spektrum der Wissenschaft; Nr.2, Februar 1986; S. 30-38