VEITH RISAK[1]

“Sicherheitspolitische Bedeutung der Informationstechnik”

Zusammenfassung

Es wird gezeigt, welche Schlüsselrolle die Informationstechnik (IT) in wirtschaftlichen und militärischen Konflikten spielt. Die IT bietet einerseits völlig neue Möglichkeiten durch Datenerfassung und Verknüpfung unter Echtzeitbedingungen einerseits für die Entscheidungsvorbereitung und andererseits für die operative Durchführung. Sie wurde damit mehr und mehr zur strategischen Waffe. Andererseits bildet die IT neue Angriffsziele, gerade weil die Koordination der Situationserkennung und der Operationen so wesentlich von ihr abhängt.

Dieser Artikel ist so strukturiert, daß er aus eher kompakten Thesen zu Chancen und Gefährdungspotential, sowie Vorschlägen zu möglichen Konsequenzen besteht. Weiterführende Informationen sind, aus Gründen der leichteren Lesbarkeit in zahlreichen Fußnoten zusammengefaßt.

Einleitung

Heutige politische, wirtschaftliche und militärische Strukturen sind sehr komplexe Systeme.

Ein komplexes System kann nur funktionieren, wenn Material- und Informationsfluß[2] koordiniert zusammenwirken.

Ein komplexes System, das Menschen dienen soll, muß von ihnen beherrschbar[3] sein. Dazu müssen die Komplexität, die der Nutzer sieht, und die von ihm geforderte Reaktionsgeschwindigkeit im Rahmen des von ihm mental und motorisch Beherrschbaren liegen.[4]

Je komplexer ein System ist, desto mehr neigt es zu Instabilität.[5]

Je komplexer ein System ist, und je mehr Zeitdruck besteht, desto leichter geht die Übersicht[6] und damit die Kontrolle verloren. [7]

---

[1] Univ. Doz. (praktische Informatik) an der Universität Salzburg, Leiter des Studienganges "Telekommunikationstechnik und -systeme" an der Techno-Z FH Salzburg. Adresse: 5020 Salzburg, Jakob-Haringer-Straße 5 0662-454 888/636, vrisak@tks.fh-sbg.ac.at

Der Artikel drückt ausschließlich die persönliche Meinung des Autors aus.

[2] Der Informationsfluß inkludiert hier auch den “Geldfluß”.

[3] Die "Beherrschbarkeit" setzt voraus, daß das dynamische System von dessen Nutzern in seinen wesentlichen Funktionen verstanden wird, daß die möglichen Handlungsalternativen erkennbar sind und ebenso die entsprechenden Konsequenzen bei Wahl dieser Alternative. Dieses "Verstehen" muß nicht bewußt sein; viele wichtige (komplexe und zeitkritische) Handlungsabläufe erfolgen – nach entsprechendem Training – weitgehend unbewußt (vgl. z.B. das Autofahren). Hier hat die Simulation als Trainingsinstrument ihren Platz; es muß nur sichergestellt sein, daß das der Simulation zugrundeliegende Modell hinreichend mit der Realität übereinstimmt. Dieses "hinreichend" ist alles andere als trivial. "Sandkastenspiele" und Realität weichen oft und gefährlich voneinander ab.

[4] Nähere Details vgl. [RIS94]

[5] Eine Konsequenz aus der Regelungstheorie.

[6] Eine interessante Fallstudie von Dörner, die in seinem Buch "Lohhausen", vgl. [DOE] enthalten ist, setzte Versuchspersonen in die Rolle eines Bürgermeisters der – simulierten – Kleinstadt "Lohhausen", die sie unter extremem Zeitdruck durch mehrere Jahre zu führen hatten. Zwei Personentypen stellten sich dabei heraus: Einer, der jeweils das aktuellste Symptom bekämpfte und einer, der zunächst versuchte, eine grobe Übersicht über die Lage von "Lohhausen" zu gewinnen. Während der erste Typ nur die Symptome bekämpfte und immer mehr die Übersicht verlor, was schließlich zu völlig irrationalen Befehlen führte, identifizierte der zweite Typ zunächst die wesentlichsten Probleme, wendete seine Arbeitskraft ihrer Lösung zu und kam damit aus dem Zeitdruck heraus.

Kritisch wichtige Systeme[8] müssen robust[9] sein gegenüber zufälligen und gewollten Störeinflüssen von außen und innen, sowie gegenüber Fehlbedienungen. Solche Störeinflüsse sollen im Idealfall die Funktionalität gar nicht einschränken.[10] Wo dies nicht möglich ist, soll die Störung lokal oder regional begrenzt[11] sein, bzw. die Funktionalität nur unwesentlich einschränken.

Reine Sternnetze sind besonders gefährdet.[12]

Hier kann man Wesentliches aus der dezentralen Organisation der Nervennetze einfacher Tiere[13] lernen; höhere Tiere und besonders der Mensch mit seinem "Zentralnervensystem" sind an dieser Stelle besonders verletzlich.

Chancen und Gefahren der Informationstechnik

Einführende Bemerkungen

Die Informationstechnik bietet neuartige und in ihrer Bedeutung zunehmende Chancen aber auch Gefahren bei der Führung komplexer Systeme unter Zeitdruck und Informationsmangel. Es ist dabei entscheidend, das "rechte Maß"[14] zwischen der IT-Unterstützung des menschlichen

---

Beide Entscheidertypen sind nicht nur unter diesen Versuchspersonen sondern auch im realen Kontext zu finden ...

7 Dabei ist besonders der Störfall zu beachten, der gerade in militärischen Situationen oft eher der Normalfall ist. Im Normalfall ist z.B. in einer Prozeßleitwarte "fast nichts zu tun"; in einem größeren Störfall, z.B. drohender Netzzusammenbruch müssen dann ganz plötzlich und unter hohem Zeitdruck Probleme analysiert, Entscheidungen getroffen und realisiert werden. Ähnliches gilt bei ärztlichen Notfallsituationen.

8 Je nach Bereich verschieden: Bank: elektronischer Geldverkehr, Medizin: Intensivstation, Flugverkehr: Flugleitsysteme, ...

9 Robuste Systeme tolerieren – in gewissem Maß – Fehlhandlungen und erlauben die Rückkehr in den Ausgangszustand (in militärischen Systemen eher selten). Robuste Systeme verhindern aber oft schon durch "vorbeugende Maßnahmen" das Auftreten von Fehlern. Das ist z.B. bei der Gestaltung von Nutzeroberflächen, wie Radarschirmen, ... zu beachten. Graphische Darstellung (z.B. von Geschwindigkeit, Richtung, ... von Flugzeugen, Raketen, ...) sind wesentlich schneller und fehlerfreier vom Menschen interpretierbar als Zahlenkolonnen.

10 Das kann z.B. durch redundante Hard- und Software geschehen.

11 Die Sicherung des "Überlebens" eines militärischen Netzes – auch bei Ausfall von Verbindungen und Netzknoten – wurde zunächst im DARPA-Netz der USA realisiert. Dies führte im zivilen Bereich zum gleichartig strukturierten Internet. Bemerkung: Im Gorbatschow-Putsch gelang es den Putschisten, alle TV-, Radio-, Telefon-, Telex-Verbindungen mit dem Ausland zu blockieren. Eine – ganz langsame – Internet-Verbindung nach Finnland blieb bestehen. Über diese Verbindung gelangten per Email ganz entscheidende Informationen in den Westen und umgekehrt. (Ein Teil des Mail-Verkehrs wurde in der Zeitschrift CACM später dokumentiert.)

12 Bei Ausfall des Zentralknotens bricht die gesamte Struktur zusammen.

13 So hat z.B. ein fünfarmiger Seestern ein Ring-Nervennetz, das die Teilnetze der Arme verbindet und koordiniert. Beim Durchtrennen des Ringes an einer Stelle bleibt die Koordinierung erhalten, sie zerfällt in zwei Teile erst dann, wenn – stärkere Störeinwirkung – der Ring an zwei Stellen durchtrennt wird. Auch das Teilnetz eines isolierten Armes, das eine Leiterstruktur hat, kann die Tätigkeit dieses Armes autonom koordinieren. Als unterste Kontrollebene kann jedes isolierte Segment Grundfunktionen autonom ausführen.

Bei zunehmenden Störeinflüssen überleben das System oder Systemteile, wenn auch mit immer mehr eingeschränkter Funktionalität. Wenn man damit in einem zentralisierten System (z.B. der Mensch) die Wirkung eines Kopfschusses vergleicht, wird der Unterschied in der Robustheit zwischen zentralen und dezentralen Systemen drastisch klar.

14 Dieser Begriff stammt aus der Mönchsregel des hl. Benedikt, der im 6. Jh. lebte. Diese Regel ist neben ihrer religiösen Bedeutung als Leitlinie für das Zusammenleben in Klöstern ein auch heute aktuelles Managementhandbuch, das sich wesentlich mit Führungsaufgaben und Entscheidungsfindung beschäftigt. Vgl. [RIS91].

Entscheidens und Handelns einerseits und der Freiheit des verantworteten menschlichen Handelns andererseits zu finden.[15]

Die der Situation strategisch und taktisch angepaßte Nutzung der Informationstechnik zielt darauf ab, ein optimales Verhältnis zwischen Chancen und Risiken herzustellen, oder dieses nach Störeinwirkungen wieder herzustellen. Diese Forderung ist typisch für komplexe Systeme unter Echtzeitbedingungen.

Im folgenden Abschnitt wird mit Hilfe des "Managementzyklus" auf wesentliche Chancen und Risiken der IT näher eingegangen.

Managementzyklus

Der Managementzyklus besteht aus folgenden Phasen:

- Zielfindung
- Situationsbewertung
- Entscheidung
- Planabsicherung
- Durchführung
- Erfolgskontrolle

Diese Aktionsfolge wird wiederholt durchlaufen, um das Ziel immer besser zu treffen. Der Managementzyklus kann auf verschiedenen Ebenen und unter verschiedenen Zeithorizonten durchlaufen werden. Dementsprechend haben seine Anteile jeweils mehr oder weniger Gewicht; bzw. überwiegt bei der Zielfindung die strategisch langfristige oder operativ-taktische kurzfristige Sicht. Dadurch wird u.a. auch der mögliche Einsatz der IT beeinflußt.

Die einzelnen Komponenten bieten verschiedene Möglichkeiten des Einsatzes der IT, die im Folgenden kurz dargestellt werden sollen:

Zielfindung

Die Zielfindung muß, zumindest in der obersten Ebene, vom Menschen verantwortet und durchgeführt werden.[16] Aus den Zielen der obersten Ebene können schrittweise Subziele abgeleitet werden. Man spricht dabei von einem hierarchischen top-down Vorgehen.[17] Die Autonomie der Zielfindung der unteren Ebenen wird dabei durch die übergeordneten Ziele schrittweise eingeschränkt.

Der umgekehrte, in der Wirtschaft teilweise eingeschlagene Weg, durch bottom-up Planung aus Teilzielen übergeordnete Ziele abzuleiten, ist im militärischen Bereich kaum üblich.

Die Ziele und ihre Teilziele müssen einerseits vom Menschen klar verstanden werden ***können.*** Andererseits müssen sie so formalisiert werden, daß sie Computersimulationen als Zielfunktionen vorgegeben werden können.

---

[15] Diese Problematik wird derzeit intensiv am Beispiel der "intelligent agents", vgl. [NN94] diskutiert.

[16] Bei der Automatisierung von (Teil-)Prozessen können jeweils – gut verstandene – Teiltätigkeiten automatisiert werden, um den Menschen von Routineaufgaben zu entlasten. Die Autonomie der Zielsetzung darf er aber nicht aus der Hand geben.

[17] Bei dieser Zielfindung und bei der Sicherstellung der Subziele mit den übergeordneten Zielen können IT-Werkzeuge, auch solche des CSCW (Computer Supported Cooperative Work), erfolgreich als Hilfsmittel eingesetzt werden.

Dieser Schritt ist kritisch, da eine fehlerhafte Übersetzung von Zielen in die erwähnten Zielfunktionen notwendig zu falschen Simulationsergebnissen führen muß.[18]

Situationsbewertung

Bei dieser Phase des Managementzyklus kann die IT vorwiegend zur Simulation (Was-Wäre-Wenn-Analyse herangezogen werden. Dazu ist eine Abbildung der realen Welt in ein hinreichend abstrahiertes Modell der erste Schritt. Die Angemessenheit dieser Abstraktion bei der Modellbildung und die Qualität der zugrundeliegenden Daten[19] sind entscheidend für die Qualität und Tragfähigkeit der abgeleiteten Schlußfolgerungen. Diese Daten sind daher ein kritischer Ansatzpunkt für Störversuche.

Das Sandkastenspiel vergangener Zeiten wird damit durch Computersimulation ersetzt.

Die Situationsbewertung kann global-überblicksweise oder schrittweise verfeinernd hierarchisch durchgeführt werden. Bei der Wahl der für notwendig gehaltenen Detaillierung müssen der Detaillierungsgrad und die Vollständigkeit der notwendigen Daten ebenso berücksichtigt werden, wie die verfügbaren Ressourcen an Rechnerkapazität und Kommunikationswegen. Sie muß in jedem Fall zu einer Bewertung nach Bedeutung und Dringlichkeit führen, aus der die Prioritäten[20] der zuallererst notwendigen Aktionen abgeleitet werden können.

Entscheidung

In der Entscheidungsphase werden aufgrund der vorgegebenen Ziele und nach Analyse und Bewertung der bestehenden Alternativen verbindliche, nicht mehr zu diskutierende, Entscheidungen durch Wahl einer Alternative getroffen.

Die Entscheidungen können mittels rationaler Methoden, vgl. [KEP] oder intuitiv getroffen werden. Eine gute vergleichende Übersicht über verschiedene Entscheidungstechniken findet sich in [DOE].

Bei der Bewertung der möglichen Alternativen spielt wieder die Simulation eine große Rolle.

Es ist zweckmäßig, getroffene Entscheidungen zu dokumentieren,[21] um aus den Ergebnissen der Phase “Erfolgskontrolle” für spätere Entscheidungen lernen zu können.

Planabsicherung

Getroffene Entscheidungen sollen vor der Durchführung abgesichert werden, soweit dies unter den gegebenen Bedingungen (insbesondere Echtzeitbedingungen) möglich ist.

Dazu ermittelt man zuerst die kritischesten Aktionen bei der Durchführung.[22] Für diese analy-

---

[18] Dieser Fehler ist, wenn er nicht erkannt wird, besonders kritisch, da oft Rechnerergebnisse kritiklos hingenommen werden. Es werden dann falsche Ziele optimiert, ohne daß die Entscheider dies wissen.

[19] In der Softwareentwicklung bezeichnet man diese Fehlerquelle mit “garbage in – garbage out”.

[20] Ein entscheidender Fehler von Managern ist es, die Prioritäten falsch einzuschätzen, bzw. sich wider besseres Wissen niederprioren Anforderungen zuzuwenden. Dies führt im Regelfall, wie Dörner, vgl. [DOE] so eindrucksvoll zeigte, zu steigendem Zeitdruck, Aufschieben (“Verdrängen”) wichtiger Entscheidungen, immer hektischeren Aktionen, bis hin zum völligen Verlust der Übersicht und zum Zusammenbruch des Systems.

Dabei zeigte sich, daß sich die Selbsteinschätzung der Versuchspersonen häufig nicht mit ihrem Aktionsmustern deckte.

[21] Diese Dokumentation führt andererseits zur Gefahr der Ausspähung.

[22] D.h. jene, deren Störung mit den schwerwiegendsten Konsequenzen einhergeht. Man sollte dabei sehr selektiv vorgehen, da für die Planabsicherung meist nur begrenzte Ressourcen verfügbar sind. Auch die Planabsicherung ist ein kritischer Ansatzpunkt für gegnerische Ausspähung.

siert man zunächst mögliche Störungsursachen und sucht vorbeugende Maßnahmen zur Ausschaltung dieser Ursachen. In einem zweiten Schritt überlegt man die möglichen Störungsfolgen und sucht Eventualmaßnahmen, um deren Auswirkung zu verringern.

Für den Extremfall[23] sind entsprechende Notmaßnahmen (meist verbunden mit extremer Dezentralisierung) vorzusehen.

Durchführung

Die plangemäße Durchführung von Aktionen setzt eine klare und eindeutige, sowie rechtzeitige Information der ausführenden Akteure[24] voraus. Die dazu nötige Kommunikation und deren Absicherung[25] ist eine kritische Stelle der Informationsübertragung.

Erfolgskontrolle

Die Erfolgskontrolle stellt fest, ob und wieweit die geplanten Ziele erreicht wurden. Bei militärischen Systemen ist ja mit wesentlich größeren Störeinwirkungen zu rechnen, als z.B. in automatisierten Industrieanlagen.

Aufgrund des festgestellten Erfolges, bzw. eventueller Planabweichungen wird nun der Managementzyklus erneut durchlaufen. Dies erfolgt so oft, bis das angestrebte Ziel hinreichend gut erreicht ist, oder bis sich eine neue Situation26 mit neuen Anforderungen und Zielen ergibt.

Chancen und Notwendigkeiten

Der Managementzyklus macht Ansatzpunkte für die Optimierung der Zielerreichung, aber auch Ansatzpunkte für zufällige oder gewollte Störeinflüsse deutlich.

Heutige komplexe Echtzeitsysteme erfordern den koordinierten Einsatz von Menschen, Informationsstrukturen und Organisationsabläufen. Computer- und Netz-basierte Informationssysteme sind wegen der extrem hohen Datenmengen und wegen der oft extrem engen Zeitbedingungen heute in militärischen, aber auch in wirtschaftlichen Systemen unverzichtbar geworden.

Als Chancen bieten sie vor allem:

- Filtern, Verifizieren und Integration von Daten
- Menschengerechte Darstellung der Situation
- Analyse- und Entscheidungsunterstützung
- Automatische Aktionsdurchführung
- Erfolgskontrolle

Regionale und mehr noch globale Konfliktsituationen können nur mit Hilfe komplexer Datennetze überwacht und überblickt werden. Diese Netze müssen extrem robust gegen Störeinwirkungen und insbesondere gegen den Ausfall von Teilnetzen sein. Dies ist nur mit einer stark vermaschten Struktur, nicht mit Sternnetzen möglich.

---

[23] Insbesondere für den Totalausfall der Kommunikationssysteme.

[24] Akteure können Menschen, sowie computergestützte oder vollautomatische Waffensysteme sein.

[25] Gegen Abhören oder Verfälschung.

[26] Dies kann auch eine Erschöpfung der verfügbaren Ressourcen sein, die keine Alternativen mehr offenläßt. Gerade bei Subzielen kann eine weiträumige Situationsänderung eine völlige Neuorientierung erfordern.

Für ein kleines Land wie Österreich ohne eigene Verfügung über globale Stützpunkte, Satelliten, ... ergeben sich hier relativ enge Grenzen selbständigen Agierens, bzw. die Notwendigkeit der Kooperation mit starken Partnern wie der NATO.

Risiken

Der Managementzyklus zeigt aber auch Schwachstellen, an denen ein Gegner störend eingreifen kann. Dies sind insbesondere:

- Beeinflussung der Zielfindung durch Desinformation[27]
- Beeinflussung der Situationsbewertung durch verfälschte[28] Information
- Beeinflussung der Entscheidungsfindung, der Was-Wäre-Wenn-Analyse[29]
- Störung der Aktionen[30]
- Störung der Ergebniskontrolle

Alle diese Störeinflüsse zielen peripher darauf, notwendige einlaufende ("sensorische") Informationen, bzw. auslaufende ("aktorische") Kommandos zu behindern oder zu blockieren. Zusätzlich kann die zentrale oder dezentrale Verarbeitung gestört werden.[31]

Konsequenzen

Funktionierende Informationsflüsse[32] (lokal und global) sind für das Funktionieren von komplexen Systemen strategisch und taktisch lebenswichtig; sie sind daher aber auch bevorzugt Angriffspunkte und oft Schwachstellen.

Die in der Einleitung genannte "Beherrschbarkeit" komplexer Systeme setzt der Automatisierung wichtige Grenzen. Zum einen muß die Beherrschbarkeit einerseits unter kritischen Echtzeitbedingungen[33] bestehen, und andererseits muß sie auch unter – nahezu beliebigen – Störeinwirkungen[34] bestehen bleiben.[35]

---

[27] Z.B. Hinweise auf einen anderswo geplanten Angriff, der den wahren Ort des geplanten Angriffs verfälscht.

[28] Verfälschte Informationen sind weit gefährlicher als gelöschte. Gelöschte, also fehlende Informationen fallen auf, z.B. wenn ein Teilnetz zerstört wurde. Geschickt verfälschte Informationen (Anzapfen aus einem und Einspeisen in ein vermeintlich sicheres Netz) sind viel unauffälliger.

[29] Hier sind Einflüsse auf die verwendeten Programmsysteme, Datenbanken, ... durch Viren, Trojanische Pferde, ... möglich.

[30] Z.B. Störung der automatischen Zielsuche und Zielverfolgung von Flugkörpern durch Beeinflussung der Navigations- und Kommunikationssysteme, Selbstzerstörungskommandos, ...

[31] Bei Lebewesen würden diese Störeinflüsse z.B. zu Blindheit, Lähmung oder psychotischem Verhalten führen. In jedem Fall wäre die Gesamtfunktion des Systems und seine Fähigkeit zur Zielerreichung schwer gestört.

[32] Ich spreche hier von "modernen Krisen und Kriegen", nicht von nach archaischen Mustern ablaufenden Konflikten. Letztere werden stark individualisiert und extrem emotionell ausgetragen. In diesen Fällen spielt die IT gegenüber den Verhaltensmustern von "Blutrache" ... eine eher unbedeutende Rolle. Dies kann zu schweren Problemen führen, wenn Militärs beider Verhaltensmuster aufeinandertreffen. (Die jüngere Geschichte lieferte Beispiele ...) Diese Situationen zeigen aber neue Grenzen einer IT-gestützten Krisenbewältigung auf. Hier könnte – vielleicht – die Spieltheorie neue Ansätze zeigen. Doch geht auch sie von der Annahme aus, daß sich der Gegner rational verhält und die für ihn günstigste Strategie wählt. Jede andere ist für ihn ungünstiger, doch kann das Wählen suboptimaler Strategien einen rational denkenden Gegner verwirren.

[33] Die begrenzte Kapazität des Menschen zur Informationsverarbeitung wird gerade von Systemen, die zugleich komplex sind und höchste Reaktionsfähigkeit erfordern, leicht überschritten. Militärische Kampfsituationen sind dafür ein Musterbeispiel. Unter diesen Bedingungen kann es durch diese Informationsüberlastung bei gleichzeitigem Entscheidungsdruck zu folgenschweren Fehlentscheidungen kommen. Ein Musterbeispiel ist der – irrtümliche – Abschuß einer Passagiermaschine im persischen Golf, die durch unübersichtliche Nutzeroberflächen des

Künftige Konflikte werden daher zunehmend versuchen, die IT-Infrastruktur[36] des Gegners zu stören.[37] Während Zerstörungen schnell auffallen, sind Verfälschungen sehr unauffällig. Sie setzen das Eindringen in die IT-Infrastruktur des Gegners voraus. Ist dies gelungen, kann dieser Zugriff einerseits zum Gewinnen strategischer Information (Datenspionage), als auch zur gezielten Verfälschung[38] genutzt werden.

Daher ist die Haltung der USA verständlich, einerseits Codierungsverfahren als strategische Waffe anzusehen[39] und andererseits bei genehmigten Codierungsverfahren eine Hinterlegung von "Generalschlüsseln" zu verlangen.[40]

Komplexe Netze müssen dezentral organisiert werden, um beim Ausfall des Zentralknotens nicht zusammenzubrechen. Dezentrale statt zentraler Intelligenz (ein wesentliches Softwareproblem) kann das "Überleben" regionaler Kommandostrukturen ermöglichen.

Gegen Ausfall einzelner Verbindungen muß technische Redundanz[41] vorgesehen werden. Simulationen können die Reichweite dieser Sicherungsmaßnahmen, z.B. gegenüber verschiedenen Terrorszenarios prüfen ("Was-Wäre-Wenn-Analyse")

Radarsystems und den Streß der Kampfsituation (das Schiff wurde zur gleichen Zeit von Schnellbooten angegriffen) mitverursacht wurde. Eine detaillierte Analyse erfolgte in den "ACM Software-Engineering-Notes" (@@@ Heft/Seite ...) in der ständigen Rubrik "Risks to the Public" von P. Neumann.

[34] Mit solchen Störeinwirkungen müssen wir im militärischen Krisen- und Konfliktfall weit stärker rechnen als in "zivilen" Systemen. Im zivilen Bereich ist die ungestörte Systemstruktur der Normalfall, der Störfall eine seltene Ausnahme. Im militärischen IT-Systemen wird ein Gegner besonders daran interessiert sein, die IT-Infrastruktur seines Gegners zu (zer)stören. Der "Störfall" ist hier die Regel.

[35] Solche Störfälle können einerseits die Datenerfassung betreffen; im Störfall ist der Entscheider "blind" oder "im Nebel". Dieser Fall der notwendigen "Entscheidung unter Informationsmangel und Zeitdruck" ist auch für viele Managementsituationen typisch. Wieweit das – auf Erfahrung, Assoziationsfähigkeit und Training beruhende – "Gespür" hier richtig zu leiten imstande ist, muß für mich offenbleiben, wird aber von mir auch nicht bestritten.

In einem weiteren Fall ist die operative Ausführung gestört; Entscheidungen und Befehle einer zentralen Stelle ("Führungsbunker") gelangen nicht (mehr) zu den operativ Ausführenden. Die Entscheider sind "gelähmt".

Beide Störeinflüsse finden sich auch in industriellen Anwendungen, wenn z.B. die "Leitwarte" räumlich weit vom Prozeß getrennt ist (vgl. Leitwarten der Energieverteilung), so daß dieser nicht mehr direkt beobachtet werden kann. Doch stehen im "zivilen Störfall" meist noch weitere Informationskanäle wie Fernschreiber, Mobiltelephon, Melder, ... zur Verfügung. Jedoch ist es in schwersten Störfällen (vgl. die Reaktorkatastrophe von Tschernobyl) denkbar, daß die Verbindung zwischen Leitstelle und Prozeß völlig abreißt. Das zu erreichen, ist im militärischen Fall sicher eines der Hauptziele des Gegners.

Ein weiterer Störfall besteht in der Verfälschung der Informationsverarbeitung. In diesem Fall werden aus an sich richtigen Daten, (bewußt) fehlerhafte Ergebnisse und Handlungsvorschläge abgeleitet, oder die Rückmeldungen über befohlene Operationen erfolgen fehlerhaft. (NB: Hierzu gehören Fehlinformationen über das Vorhandensein von kampfbereiten Divisionen in der Endphase des Zweiten Weltkrieges ebenso, wie Informationsbarrieren zwischen Army und Navy und dem Präsidenten (Carter) während der Kuba-Krise.)

Das (vom Gegner beabsichtigte) Zusammentreffen mehrerer dieser Szenarios verschärft die Situation und führt zu Realitätsverlust.

[36] Hardware, Software und Orgware

[37] Zerstörung z.B. durch nukleare elektromagnetische Impulse, Störung durch Löschung, bzw. Verfälschung von Informationen.

[38] Z.B. von Operationsplänen, Zielkoordinaten, ...

[39] Und daher mit entsprechenden legistischen und sonstigen Maßnahmen zu sichern.

[40] Daß dieses Monopol aus Codierungsverfahren auch eine wesentliche "wirtschaftliche Waffe" ist, sei angemerkt.

[41] Das führt zu Maschen- statt Stern-Netzen. So läuft z.B. um Wien eine Ringleitung, die die Energieversorgung von mindestens zwei Seiten sicherstellt.

Literatur

Dem Ziel dieses Artikels entsprechend, eine eher thesenhafte Übersicht zu bieten, wurde auf ein ausführliches Literaturverzeichnis verzichtet. Die im Folgenden angegebenen Quellen sollen aber Ansatzpunkte zur Vertiefung bieten:

Dörner D., Kreuzig H.W., et. al. [DOE], Lohhausen, vom Umgang mit Unbestimmtheit und Komplexität Verlag Hans Huber Bern-Stuttgart-Wien 1983
Dieses Buch beschreibt zunächst vergleichend verschiedene Entscheidungsstrategien. Anschließend wird eine große Fallstudie beschrieben, in der Versuchspersonen unter Informationsmangel und Zeitdruck als "Bürgermeister" eine simulierte Kleinstadt "Lohhausen" über mehrere Jahre führen mußten. Das Buch gibt sehr ausführliche Analysen über verschiedene Persönlichkeitstypen und deren Führungsverhalten.

Kepner Ch.H., Tregoe B.B. [KEP], Entscheidungen vorbereiten und richtig treffen, rationelles Management Verlag moderne Industrie 1982

Neumann P. [NEU99], Risks to the Public Regelmäßige Kolumne in der vierteljährlichen Zeitschrift SEN (Software Engineering Notes) der ACM-Verlag New York
In dieser Kolumne werden jeweils aktuell bekanntgewordene Störfälle, die irgendwie im Zusammenhang mit der IT stehen, analysiert und kommentiert. Eine sehr umfangreiche Sammlung mit vielen hundert Einträgen aus dem zivilen, behördlichen und militärischen Bereich. P. Neumann führt zu diesem Thema auch eine umfangreiche Datenbank.

N.N. [NN94], Intelligent Agents, CACM 1994, H. 7
Sonderheft über als Software realisierte "intelligente Agenten", die dem Nutzer Routineaufgaben abnehmen sollen, ihn aber in seiner Freiheit einschränken können. Dieses Sonderheft führte zu einer monatelangen kontroversiellen Diskussion.

Risak V. [RIS91], Benedikt, Menschenführer und Gottsucher Böhlau-Verlag Wien 1991
Eine Mönchsregel aus dem 6. Jh. als Managementhandbuch gedeutet.

Risak V. [RIS94], Limits on Complexity and Velocity Demands ...Proc. ICCHP'94 Springer Lecture Notes 1994