Robert Adrian
Intelligente Maschinen

Jenseits der Information

Die meisten Unternehmen, die eine gewisse Größe erreicht haben, neigen dazu, schizoid zu werden, was bedeutet, daß sie über zwei komplementäre Identitäten verfügen: eine physische, aus Gebäuden, Anlagen, Angestellten usw. bestehende, und eine digitalisierte virtuelle Identität in Form vernetzter Computerdatenbanken. In der virtuellen Geschäftswelt der vernetzten Computer bewegen sich Informationen, Befehle und Geld mit Lichtgeschwindigkeit, während unten am Boden die Menschen und Maschinen — und sogar die Roboter — noch immer gegen Schwerkraft und Entfernungen ankämpfen.

Am Berührungspunkt zwischen dem virtuellen Unternehmen und seinem physischen Pendant — zwischen den Datenbanken und der Fabrikshalle — kontrollieren und verwalten immer komplexere Eingabe/Ausgabeschnittstellen den Informations-, Produkt- und Dienstleistungsfluß — und auch den Datenrückfluß in die Netzwerke —, so daß die verschiedenen Ströme für eine Computersimulation im Rahmen der Unternehmensplanung und -entwicklung quantifiziert und manipuliert werden können.

Wenn das virtuelle Unternehmen gut konstruiert ist und ordnungsgemäß funktioniert, ist jede Einzelheit über die physischen und finanziellen Operationen der Firma online in Echtzeit abfragbar — d. h. Information über den Standort jedes einzelnen LKW, jedes Angestellten, jedes Dokuments. Mit Hilfe verschiedener Softwareprogramme können künftige Entwicklungen durch eine Simulation der Auswirkungen von organisatorischen Veränderungen, des Geldflusses, der Einführung neuer Technologien, von Marketing/PR-Strategien und vielem mehr einfach durchgespielt werden. Die Verantwortlichen auf den jeweiligen Entscheidungsebenen können nach wie vor auf das Datenbanknetz zugreifen, um einen Überblick über das jeweils anstehende Element der Firmenpolitik zu bekommen. Infolge der Automatisierung der Datenaktualisierungs- und Bewertungsverfahren handeln die Manager aber zunehmend aufgrund von Entscheidungen, die die Maschinen getroffen haben, anstatt aufgrund der Daten, die die Maschinen liefern, selbst zu entscheiden. Dementsprechend ersetzt die Software in den Bürogebäuden der großen Konzerne nach und nach die Wetware.

Diese klassischen Feedbackschleifen, die sich im Falle eines wirklich großen multinationalen Konzerns auf globaler Ebene vollziehen, können wir in einer mikrokosmischen Version Tag für Tag im Supermarkt erleben, wo Strichcodeleser an den Kassen die Lagerbestandslisten aktualisieren und automatisch Daten über Verkaufs- und Vorratsmengen an die Hauptgeschäftsstelle des jeweiligen Unternehmens übermitteln. Die Menschen fahren natürlich immer noch die LKW, füllen die Regale auf und arbeiten an den Kassen, doch die Geschäftsführerin ist wie der Speditionsangestellte, der die Lieferungen für das Geschäft tätigt, lediglich ein Teil eines computergesteuerten Datenflusses, und ihr Zuständigkeitsbereich wird durch den Zentralcomputer stark eingeschränkt. Der Mikrokosmos des Supermarkts ist aber gleichzeitig mit dem Makrokosmos der nationalen — wenn nicht gar der globalen — Wirtschaft verbunden. Die jüngsten Entwicklungen bezüglich der Konsumautomation bestehen in einer Vernetzung von Finanzinstitutionen mit Einzelhandelsgeschäften. Die kleinen Kartenlesegeräte an den Supermarktkassen verbinden den Strichcodeleser, die Registrierkasse und Ihr persönliches Bankkonto mit dem Computernetzwerk der Supermarktkette und deren Verbindungen zur globalen Wirtschaft. In den meisten Teilen Europas erlaubt es das Girosystem bereits jedem Durchschnittsbürger,

zumindest theoretisch wochenlang ohne einen einzigen Groschen reales Geld in der Tasche zu leben. Der Computer des Arbeitgebers überweist die Lohnzahlung direkt auf das Bankkonto des Angestellten. Über die im Computer der Bank eingespeicherten Daueraufträge werden die regelmäßigen Zahlungen (Miete, Versicherung, Telefonrechnung etc.) des Kontoinhabers automatisch erledigt, und Direktkäufe werden ebenfalls über die Bank oder über Kreditkarten bezahlt. Bargeld wird — wie das Eingreifen des menschlichen Managers in die Entscheidungsfindungsprozesse des Unternehmens — zunehmend zu einer bloßen Rückversicherung, auf die lediglich im Notfall zurückgegriffen wird.

Wenn ein derartiges Management- und Automationssystem eingeführt wird, können natürlich auch jede Menge Fehler passieren. Der plötzliche Zusammenbruch eines Computersystems kann ein Unternehmen zumindest zeitweise vollständig lähmen, wie dies kürzlich in Wien zu beobachten war, wo der wichtigste Milchversorgungsbetrieb seine Geschäftstätigkeit automatisiert und zentralisiert hat. Unglücklicherweise war die verwendete Software nicht fehlerfrei, so daß es während der ersten Woche zu wiederholten Systemabstürzen kam, weshalb die meisten Geschäfte der Stadt plötzlich keine Milch mehr geliefert bekamen. Trotz der peinlichen Situation und der Kosten (die sich auf zig Millionen Schilling beliefen) hat man eine Rückkehr zur alten, auf menschlichen Ressourcen beruhenden Methode niemals ernsthaft in Erwägung gezogen. Die digitale Automatisierungstechnologie gilt als unvermeidlich und irreversibel. Maschinen werden ungeachtet der sozialen Kosten ihres Einsatzes und der immer wieder auftretenden spektakulären Fehlschläge einfach als verläßlicher, effizienter und gewinnbringender betrachtet als menschliche Arbeitskräfte.

Darüber hinaus müssen die Einsparungen im Personalbereich und die schnellere Datenübertragungsgeschwindigkeit auch im Zusammenhang mit den Sicherheitsfragen gesehen werden, die für Unternehmen immer schon ein ernstes Problem waren, sich in einer Umgebung vernetzter Datenflüsse jedoch noch wesentlich komplexer präsentieren als bisher. Im Kampf gegen Hacker, Computerkriminalität und Industriespionage wird ein großer Teil der Forschungs- und Entwicklungsressourcen darauf verwendet, Maschinen zu entwickeln, die sich selbst gegen potentiell schädliche Eindringlinge schützen können. Damit ein solcher Schutz effizient funktioniert, muß die Maschine in der Lage sein, die immer schlaueren und einfallsreicheren Eindringlinge zu erkennen. Das bedeutet, die Maschine muß ein "Bewußtsein" für ihre territorialen Grenzen erhalten und in die Lage versetzt werden zu entscheiden, wer diese Grenzen überschreiten und auf ihre Speicher und Programme zugreifen darf.

Ähnlich wie der Wiener Milchversorgungsbetrieb bei seinem Softwaredebakel denkt auch ein Unternehmen, das Opfer eines Hackers geworden ist, nicht daran, zur herkömmlichen Datenverarbeitung und -übertragung durch menschliche Arbeitskräfte zurückzukehren — die gegenwärtige kulturelle Einstellung zur Computerautomation würde dies nicht erlauben —, sondern wird nach verbesserten Schutzmaßnahmen suchen. Dies geschieht normalerweise in der Form, daß heikle Daten aus den Kommunikationsnetzen isoliert werden (sogenannte "Firewalls"/"Intranets") und eine Software entwickelt und installiert wird, die in der Lage ist, unautorisierte Aktivitäten festzustellen. Die Situation wird jedoch komplizierter, wenn hinter dem unautorisierten Zugriff nicht bloß ein einzelner Hacker steckt, sondern Computerkriminalität oder Industriespionage vorliegt, da dahinter zumeist ausgefuchste Experten oder — noch schlimmer — Insider wie Firmenangestellte oder Programmierer stehen.

Die Schwachstellen der Sicherheitssysteme finden sich an den Schnittstellen zwischen dem virtuellen Unternehmen und dem physischen Unternehmen. Aufgrund des kulturellen und

ideologischen Glaubens an die Überlegenheit der Maschine genießt das virtuelle Unternehmen Priorität, was bedeutet, daß das virtuelle Unternehmen von den Menschen, denen es ursprünglich dienen sollte, isoliert werden muß. Die Maschine muß lernen, sich gegen Menschen zu verteidigen, was bedeutet, daß die Computerinstallation und das gesamte firmeninterne Netzwerk (das virtuelle Unternehmen) unter Einführung komplizierter Zugriffshierarchien, die den unautorisierten Zugriff bzw. kriminellen Mißbrauch verhindern oder zumindest minimieren, umstrukturiert werden. Die interessante und zumeist übersehene Auswirkung dieser Bevorzugung des virtuellen Unternehmens besteht darin, daß die menschlichen Arbeitskräfte einschließlich der Manager zunehmend als bloße Schnittstellen zwischen den verschiedenen Elementen der elektronischen Netzwerke betrachtet werden. Ungeeignetes Handeln seitens menschlicher Protagonisten kann das ordnungsgemäße Funktionieren der Maschinen beeinflussen, weshalb die Maschinen so konstruiert (oder trainiert) werden, daß sie immer mehr Managementfunktionen übernehmen. Das bedeutet, daß sie mehr Entscheidungsbefugnis — mehr Autonomie — erhalten.

Wenn die Zunahme der Autonomie der Maschinen weiterhin so schnell voranschreitet wie in den vergangenen 15 Jahren, ist leicht absehbar, daß das im globalen Netzwerk existiertende virtuelle Unternehmen das aus Fabriken und Büros bestehende "reale" bis zum Ende des ersten Jahrzehnts des nächsten Jahrtausends ersetzt haben wird. Die menschlichen Arbeitskräfte werden dann das tun, was Menschen am besten können: in der Gegend herumgehen und Dinge für die Maschinen holen und transportieren. Dies wird für die meisten von uns keinen großen Unterschied machen, denn wir haben uns ohnehin bereits an den Gedanken gewöhnt, daß die "Dienstleistungsindustrien" die Hauptarbeitgeber der Zukunft sein werden.

Mit dem sehr groben Bild, das ich eben gezeichnet habe, wollte ich einige der verborgenen Elemente des unaufhaltsamen Fortschritts in der Automatisierung der "privaten" Industrie und Wirtschaft aufzeigen. Normalerweise konzentriert man sich allerdings mehr auf die Bereiche Militär und Überwachung, weil diese oft die Öffentlichkeit und die Regierung beschäftigen und deshalb automatisch zum Gegenstand von Besorgnis und Kritik werden. Vielleicht aber käme hier ein militärisches Beispiel ganz gelegen, und worum sonst könnte es dabei gehen als um den "Golfkrieg".

Die virtuelle Realität ist ein Produkt der Flugsimulationssysteme, die seinerzeit für die Luftstreitkräfte der Vereinigten Staaten entwickelt wurden. Der Pilot wird in einen aerodynamischen Anzug gesteckt, mit Sensoren ausgestattet und in ein realistisch gestaltetes Cockpit gesetzt, das an einen leistungsstarken Computer angeschlossen ist. Auf diese Weise können simulierte Flug- und Kampfsituationen trainiert werden, ohne den Piloten oder das viele Millionen teure Fluggerät in Gefahr zu bringen. Dieses Flugtraining ist so realistisch, daß "Trainingsstunden" teilweise als tatsächliche Flugstunden angerechnet werden.

Als der Golfkrieg ausbrach, waren die Piloten bereit. Die Trainingssysteme wurden umprogrammiert, um die Geographie von Kuwait und jene des Irak zu simulieren, und die Piloten flogen ihre "Kampfeinsätze" in den Simulatoren. Es wird berichtet, daß einige der Piloten angaben, sie könnten, sobald sie im Cockpit säßen, keinen Unterschied zwischen dem Training und realen Flugeinsätzen mehr feststellen.

Das aufschlußreichste Element ist jedoch die elektronische Befehlsstruktur, die die tatsächliche Kontrolle über das Flugzeug ausübt. Ein integriertes Überwachungssystem, in dem die Informationen von AWACS-Überwachungsflugzeugen und geostationären Satelliten kombiniert werden, wird an die Bordcomputer der Bomber angeschlossen. Die Mission und

das Ziel werden in die Computer einprogrammiert, und die Rolle des Piloten besteht darin, die verschiedenen Systeme zu kontrollieren und im Falle eines Angriffs oder Systemversagens für Start-, Lande- und Notmanöver zur Stelle zu sein. Die meisten modernen Angriffsflugzeuge können jedoch kaum ohne Computer geflogen werden, so daß ein totaler Systemabsturz in den meisten Fällen einem tatsächlichen Flugzeugabsturz gleichkommt — was uns wieder an das Problem des Wiener Milchversorgungsbetriebs erinnert, wo auch mit dem Zusammenbruch des virtuellen Unternehmens die ganze Milchversorgung zusammenbrach.

Die Bilder, die uns im Fernsehen gezeigt wurden, stammten von den Monitoren der Angriffsflugzeuge. Ob die Piloten diese Bilder bei realen oder bei simulierten Kampfeinsätzen gesehen haben, ist unwichtig. Wichtig ist, daß wir erkennen, daß dies unwichtig ist. In diesem Sinne hatte Baudrillard zumindest teilweise recht, als er sagte, der Golfkrieg sei niemals passiert. Der Krieg, den wir im Fernsehen gesehen haben, und auch der Krieg, den die US-Piloten auf ihren Monitoren gesehen haben, ist niemals passiert. Der Krieg, den die Menschen in Bagdad und die irakischen Soldaten in der Wüste erlebt haben, war hingegen real.

Die Regierung der Vereinigten Staaten hat erfolgreich demonstriert, daß in einer ernsten Kriegssituation eine Armee von Männern und Maschinen auf dem Boden völlig hilflos gegen die integrierten Schaltkreise einer virtuellen Armee in der Luft ist. Sie hat aber noch etwas anderes demonstriert, das wesentlich interessanter ist: Der reale Oberbefehlshaber ist jetzt eine integrierte Befehlsstruktur aus in Echtzeit vernetzten Computern. So wie der Pilot in seinem Cockpit sitzt, während sein Flugzeug vom Computer gesteuert seine Mission ausführt, so sitzen auch die Generäle in ihren Kommandoposten, wo sie Ausdrucke lesen und Monitore überwachen. Mit Ausnahme der regelmäßig wiederkehrenden altmodischen Scharmützel ist der Krieg heute automatisiert. Die virtuelle Armee hat die reale Armee ersetzt.