Computergeschichte und Militär

- Die Beeinflussung der Computerentwicklung durch den Militärapparat -

Ausarbeitung zum Seminar

„Gedankengeschichte der Informatik“

Martin Stromberg

Andreas Vangerow

SS 2001

Inhaltsverzeichnis

6. Das Militär und die Künstliche Intelligenz

7. Information Warfare

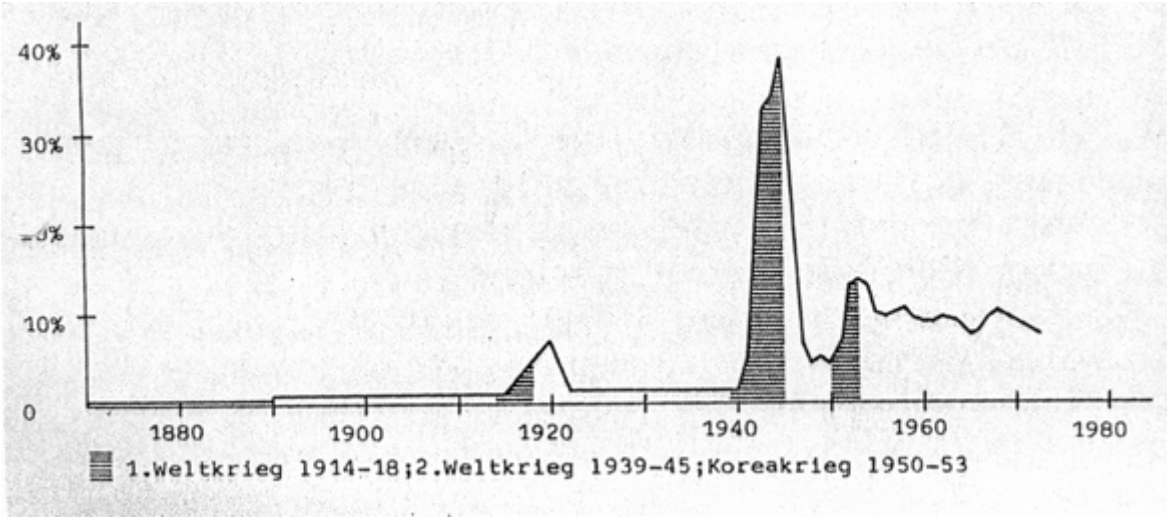
    7.1 Definition Krieg
    7.2 Definition Information Warfare
    7.3 Beispiel: Kosovo-Krieg
    7.4 Denial of Service Attacks
    7.5 Die Gegenmaßnahmen

8. Fazit

An dieser Stelle möchten wir uns bedanken für die freundliche Unterstützung der Historikerin Susa Schindler.

1. Einleitung

Die Ausarbeitung befaßt sich mit dem Thema der Beeinflussung der Computerentwicklung durch den Militärapparat. Sie soll darlegen, dass einige Militärs gerade mit Beginn des 2. Weltkriegs einen Grundstein der Computerentwicklung maßgeblich beeinflußt haben. Daher wird diese Ausarbeitung beim 2. Weltkrieg einsetzen und dann in erster Linie chronologisch auf militärische Großprojekte eingehen, die mit dem Bereich Informatik zu tun haben.
Die Entwicklung des 1. Weltkriegs, den Krieg immer mehr auf eine industrielle und wissenschaftliche Basis zu stellen, setzte sich im 2. Weltkrieg fort. Im 1. Weltkrieg wurden wissenschaftliche und industrielle Neuerungen verwendet, um den Gegner in die Knie zu zwingen. Es wurden zum ersten Mal Kampfflugzeuge, Giftgas und Flammenwerfer eingesetzt. Zur Zeit des 2. Weltkriegs profitierten in den USA zum Beispiel die Firmen, die mit dem Militär Geschäfte abschlossen. Sie erhielten staatliche Fördermaßnahmen, großzügige Budgets und einen krisensicheren Absatzmarkt.



[Darstellung der Ausgaben des US - Militärs im Verhältnis zum Bruttosozialprodukt, Quelle: Sörgel[2], 1999]

1945 gab das US-Militär ca. 82 Milliarden Dollar aus, was rund 40 % des Bruttosozialprodukts der amerikanischen Wirtschaft ausmachte.

2. Der 2. Weltkrieg – Ein Grundstein der Computerentwicklung

2.1. Bletchley Park – Die Arbeit des Alan Turing

2.1.1 Die polnische Vorarbeit – Marian Rejewski

Die polnische Regierung gehörte damals zu den ersten Regierungen, die die Bedeutung der Enigma für das deutsche Militär erkannten. Im 2. Weltkrieg wurden etwa 100.000 Exemplare der Rotor-Chiffriermaschine Enigma in der deutschen Armee eingesetzt. Die Enigma (griechisch für Geheimnis) war besonders berühmt. Den polnischen Kryptologen, zu denen auch der polnische Mathematiker Marian Rejewski zählte, gelang es dank Rejeweski bereits 1932, in das Enigma-System einzubrechen. Dazu schalteten sie sechs umgebaute Enigma-Maschinen, eine für jede Rotoranordnung derart hintereinander, dass sich der Stromkreis in dem Moment schloss, wenn eine der durch die Analytikergruppe herausgefundene Übereinstimmung auftraf [Lion 2000]. Eine solche Übereinkunft, wie zum Beispiel das in der 6er-Gruppe für die Rotorpositionen manchmal der 1. und der 4., der 2. und der 5. bzw. der 3. und der 6. Buchstabe gleich waren. Da der mechanische Teil dieser Konstruktion während der Arbeit tickte, bis das Endergebnis eintraf, nannte man sie „Bomba“, polnisch für Bombe. Die Suche nach einer Übereinstimmung konnte bis zu zwei Stunden andauern.

Dezember 1938 änderten die Deutschen die Anzahl der Rotoren von drei auf fünf. Aufgrund dessen war die Arbeit der polnischen Kryptologen hiermit beendet, es wären nun 60 modifizierte Enigma-Maschinen nötig gewesen, um die Dekodierung fortzuführen. Der Aufwand wurde als zu hoch abgelehnt [Lion 2000].

2.1.2 Turing Bomben

Der britische Mathematiker Alan Turing (1912 – 1954), der mit seiner „Turingmaschine“ bereits ein abstraktes, mathematisches Modell einer universellen Rechenmaschine aufgestellt hatte, arbeitete im 2. Weltkrieg als Entschlüsselungsspezialist in Bletchley Park für das britische Außenministerium. Bletchley Park ist ein ehemaliger Landsitz, auf dem im 2. Weltkrieg die Basis der Entschüsselungsabteilung der britischen Regierung war.

Turing entwickelte 1939 eine Maschine auf der Basis der polnischen Vorarbeit, die sogenannte „Turing Bombe“, die zur Dechiffrierung der deutschen Funksprüche diente. Bei den „Turing Bomben“ handelte es sich um Relaisrechenmaschinen, die für Nachrichten eingesetzt wurden, die mit der Enigma verschlüsselt waren [Netzwerk für Wissensweitergabe]. Sie waren vom Konzept den polnischen Bomben weit überlegen [Lion 2000]. Den Briten gelang es schließlich, die Enigma-Verschlüsselung, die ab 1938 geändert

worden war, zu dekodieren. Die Turing Bombe hatte den Nachteil, dass es, wenn sie angehalten hatte, keine hundertprozentige Wahrscheinlichkeit gab, dass die richtige Rotorposition erkannt worden war [Lion 2000]. Die Entschlüsselungsarbeit war dennoch sehr erfolgreich, so dass sich die britische Regierung gezwungen sah, die Bombardierung einiger ihrer Städte durch die deutsche Luftwaffe, ohne Gegenwehr hinzunehmen, damit jeglicher Verdacht auf eine Entschlüsselung der Enigma unbegründet war [Geschichte]. Die Bomben waren in großen Hallen aufgebaut, wo sie von Zivilistinnen betreut wurden. Sie hatten die Anweisung, den Analytikern sofort Bescheid zu geben, wenn eine der Maschinen angehalten hatte. Die Frauen waren nicht über die Vorgänge in Bletchley Park informiert, dennoch wurden sie streng überwacht. Dieser Entschlüsselungserfolg blieb den Deutschen bis zum Ende des Krieges unbekannt. Der Geheimschreiber T 52 von Siemens & Halske blieb jedoch unentschlüsselt [Beutelsbacher, 1996].

2.1.3 Colossus I +II

Während des 2. Weltkriegs entwickelten die Engländer elektronische und elektromechanische Maschinen, um die deutschen Nachrichten zu entschlüsseln. Die berühmteste dieser Maschinen ist die Colossus, eine Röhrenrechenanlage. Sie war 1943 betriebsbereit und besaß zunächst 1500 Elektronenröhren. Sie wird in Fachkreisen als der erste digitale Computer angesehen. Die Colossus konnte ein noch komplizierteres Chiffrierverfahren als das der Enigma dekodieren und zwar die Nachrichten der Lorenz SZ40.

Die Lorenz SZ40 wurde zur geheimen Kommunikation zwischen Hitler und seinen Generälen verwendet. Dieser Fernschreiber nutzte einen 5-Bit Code (Baudot-Murray) für die Übertragung von 32 Zeichen. „Diese Binärdarstellung eignet sich hervorragend für eine modulare Addition eines Schlüssels: Chiffre = (Klartext + Schlüssel) mod 2.“ [*Zitat,* Lion 2000]. Nachdem 1942 die ersten Verschlüsselungen dieser Chiffriermaschine aufgetaucht waren, kam man sehr schnell zu der Erkenntnis, dass dieser Code auf modularer Addition basierte und von der obersten Heeresleitung benutzt wurde. Die Analytiker fanden ein Muster, da die deutschen Ingenieure bei der zufälligen Verschlüsselung, auf ein Rauschverfahren zurückgriffen, dass auf der anscheinenden irregulären Bewegung von zehn Rädern in der Lorenz basierte. Die britischen Annalytiker fanden jedoch heraus, dass bei der Bewegung der Räder, Regelmäßigkeiten auftraten [Lion 2000]. Turing stellte statistische Theorien auf, die bereits einen kleinen Teil entschlüsseln konnten. Aus Zeitgründen wurde hier eine Maschine benötigt. „Zunächst wurde eine elektromechanische Maschine (Robinson) mit elektronischen Zusatzkomponenten entwickelt, die über zwei Lochbänder einerseits die Nachricht, zum anderen die Anweisungen zur Verarbeitung einlas.“ [*Zitat,* Lion 2000]. Jedoch führte die

Schnelligkeit dieser Maschine zu einem Problem. Bei einer bestimmten Geschwindigkeit konnten die Löcher der Bänder nicht mehr zuverlässig durch die Photozellen erfaßt werden. Das hatte zur Folge, dass die ermittelten Häufigkeiten wertlos wurden. Die Bänder konnten zudem schnell Feuer fangen oder blieben stecken. In diesen Problemen liegt der Ansatz der Colossus. Es wurde beschlossen, die Instruktionen zur Verarbeitung nicht mehr parallel vom Band zu lesen, sondern im Speicher der Maschine abzulegen [Lion 2000].

Max Newman arbeitete als Mathematiker im Bletchley Park und entwarf Colossus anhand von Turings Konzept der universellen Maschine. Im Forschungszentrum der Britischen Post in Dollis Hill in London wurde die Colossus innerhalb von 8 Monaten von dem Ingeniuer Tommy Flowers gebaut. Sie war schneller, als die von Relaisschaltern abhängigen „Turing Bomben“. Ihr großer Vorteil war jedoch, dass sie programmierbar war. Speicher bedeutete Röhren. Obwohl diese Röhren allgemein als unzuverlässig galten, besaß die Colossus 1.500, später sogar 2.500 Röhren. Sie konnte 5.000 Zeichen pro Sekunde verarbeiten, bei einem Stromverbrauch von 4,5 kW [Lion 2000]. „Der Speicher bestand aus fünf Zeichen von je fünf Bits in Schieberegistern.“ [*Zitat,* Lion 2000]. Innerhalb von nur zwei Stunden lieferte die Colossus die konkreten Einstellungen der Lorenz. „Colossus war fest an eine bestimmte Aufgabe angepaßt und nicht im heutigen Sinne frei programmierbar.“ [*Zitat,* Lion 2000]. Aufgrund der angeordneten Geheimhaltung wurden die Pläne der Colossus von ihrem Erbauer selbst vernichtet, wie alles andere in Bletchley Park. Ein Grund dafür war sehr wahrscheinlich, dass viele Enigmas und Lorenz SZ40 in Dritte-Welt-Länder verkauft wurden. Die Geheimhaltung hatte zur Folge, dass ENIAC später als der erste Computer bezeichnet wurde und den Erbauern John Presper und John W. Mauchly diese wissenschaftliche Leistung anerkannt wurde [Singh, 1999].

Turing spielte zwar eine entscheidende Rolle beim Dechiffrierteam, aber er war nicht an der Entwicklung der ersten Colossus beteiligt. Am 1. Juni 1944 wurde eine neue Maschine, die Colossus II in Betrieb genommen. Sie wurde von Turing konstruiert, die Baupläne wurden von der britischen Regierung jedoch erst im Jahr 2000, 55 Jahre nach Ende des 2. Weltkriegs, freigegeben. Eine Nachbildung der Colossus II ist in Bletchley Park zu sehen. Erst im Jahre 1967 wurde die Existenz von Bletchley Park der Öffentlichkeit bekannt gegeben.

Heute ist der Landsitz ein Museum [heise-online].

2.2. 1940 Die Luftschlacht um England

In den 30er Jahren entwickelten Russel Varian und Philo Farnsworth die Grundlagen der Elektronenröhre. Varian hatte an der Stanford Universität studiert und mit Diplom abgeschlossen. Farnsworth entwickelte nun eine Methode zur elektronischen Fokussierung und Ablenkung des Elektronenstrahls [McCormick[1]].

Als der 2. Weltkrieg ausbrach, benutzte Varian diese Arbeiten als Grundlage, um eine Klystron-Röhre zu entwickeln, die Radar und Mikrowellenstrahlung ermöglichte. Es wurde ein nur 3 kg schweres Radargerät entwickelt, das von der Royal Air Force, während der Luftschlacht um England 1940 eingesetzt wurde. Deutsche Bomberflugzeuge wurden damit weit vor der optischen Zielerkennung erfaßt. Aus diesem Grund verlor der damalige Reichsmarschall Hermann Göring den Luftkampf trotz anfänglicher Überlegenheit.

Die amerikanische Regierung stellte 1940, als Reaktion auf diese Technologie, über 40 Millionen Dollar frei, die zur Erforschung neuartiger Verteidigungstechnologien verwendet werden sollte.

2.3 Datenverarbeitung bei der Wehrmacht und der SS

Ab 1937 verwendete das Nazi-Regime effizient Lochkarten in erster Linie für militärische Zwecke. Es gab eine enge Zusammenarbeit zwischen der Lochkartenstelle des Wehrwirtschaftsstabes und der deutschen IBM Tochter Dehomag. Die Lochkarte diente unter anderem der Rekrutierung von Soldaten und Zwangsarbeitern, der Material- und Geräteplanung, der Rüstungsproduktion und der Logistik [Helms[1], 1999].

Die 1941 gegründete Abteilung „Maschinelle Berichtswesen“ im Reichsministerium für Rüstung und Kriegsproduktion unter Leitung Albert Speers stellte 1943 in Zusammenarbeit mit dem Generalbevollmächtigten für Arbeitseinsatz, Fritz Sauckel, Lochkarten für die Totalerfassung von rund 80.000 Betrieben mit 93 % aller Beschäftigten zur Verfügung. Diese Erfassung sollte dazu dienen, den jeweiligen Produktausstoß und den Belegschaftsstand des Betriebs aufzuzeigen. Für jeden Betrieb wurden auch die Fehltage der Arbeiter notiert. Diese Faktoren wirkten sich auf die Zuteilung von Zwangsarbeitern aus. Die Daten wurden auch dazu benutzt, Arbeiter, die nicht der nationalen Vorstellung entsprachen, in ein Konzentrationslager abzuführen.

Die Lochkarte diente auch dem Wirtschafts- und Verwaltungshauptamt der SS mit seinem Maschinellen Zentralinstitut für optimale Menschenerfassung und – auswertung zur

Registrierung aller KZ-Häftlinge. Die Lochkarten enthielten Angaben über das Geschlecht, Alter und fachliche Qualifikation. Anschließend wurde immer die Lochkartennummer den Häftlingen auf den Arm eintätowiert. Meldete ein Betrieb Bedarf an Zwangsarbeitern an, wurde „mit Hilfe von IBM-Maschinen“ [*Zitat*, Helms[1]] den Anforderungen entsprechend Häftlinge ausgewählt.

2.4 Das V2 Raketenprogramm

2.4.1 Peenemünde

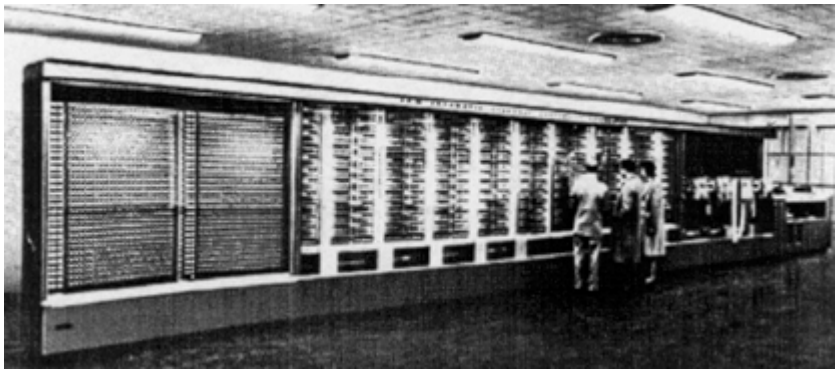
1937 wurde in Peenemünde eine Heeresversuchsanstalt gegründet, die sich mit der Raketenentwicklung befaßte. Der damalige technische Direktor Wernher von Braun (1912 – 1977) war der Konstrukteur der V1 (Vergeltungswaffe 1) und der V2 (Vergeltungswaffe 2), die aus der A4, eine Flüssigkeitsrakete, entwickelt wurden. Die V2 war die erste automatisch gesteuerte Flüssigkeitsrakete, die 1942 nach erfolgreichem Probeflug in Serienproduktion ging.

2.4.2 Die Auswirkungen der amerikanischen MARK I auf das Raketenprogramm

Ende September 1939 gab die Heeresversuchsanstalt Berechnungsaufträge an das Institut für Physikalische Meßtechnik (IPM) in Darmstadt weiter. Der Auftrag beinhaltete den Zusatz, dass die Lösung möglichst auf einen instrumentellen Weg erfolgen sollte. Seit Juni 1941 arbeitete das IPM offiziell an einer Differentialgleichungsmaschine, die für Bahnberechnungen der V2 eingesetzt werden sollte. Der damalige Leiter des Instituts Alwin Walther stellte am 18.8.1943 einen Antrag bei der Regierung für eine Forschungsbewilligung [*Zitat*, Netzwerk für Wissensweitergabe[1]] „zur allgemeinen Untersuchung und Weiterentwicklung des automatischen Ziffernrechnens.“ Der Antrag wurde mit der Begründung [*Zitat*, Netzwerk für Wissensweitergabe[1]] „völlig irreal und unnötig“ abgelehnt. Ein früherer Antrag auf Bewilligung von 150.000 RM wurde erst 1944, ein Jahr vor Kriegsende, genehmigt. In diesem Antrag war für 130.000 RM eine Integrieranlage aufgeführt, die im Rahmen des V2-Raketenprogramms entwickelt werden sollte. Zusätzlich wurden 20.000 RM für die Untersuchung über die Automatisierung von Rechenabläufen gefordert. Heute existiert auch die Vermutung, dass allierte Kräfte die Anträge verzögert haben. Dennoch entwickelte Walther, obwohl die Reichsführung sein Vorhaben ablehnte, illegal Schaltpläne für einen digitalen programmgesteuerten Rechner [Netzwerk für Wissensweitergabe[1]].

Im September 1944 wurde in den USA ein Großrechnenautomat fertiggestellt mit den Namen ASSC-MARK I. Das Projekt war ein Auftrag der US-Navy, an dem auch IBM mitwirkte. Entwicklungsbeginn war 1939 in der Harvard University in Cambridge, Massachusetts. Die Abkürzung ASSC steht für „Automatic Sequence Controlled Calculator“. Die Eingabe erfolgte über Lochstreifen. Der Mark I arbeitete noch ohne Röhren. Er konnte die vier Grundrechenarten bearbeiten und Zwischenergebnisse weiter verwenden. Er wog ca. 35 t, war 15 m lang und 2,5 m hoch. Der MARK I bestand aus insgesamt 700.000 Einzelteilen, davon waren 3000 Teile Kugellager. Zudem wurden ca. 80 km Leitung verbaut. Eine Addition erfolgte in 0,3 Sekunden, die Multiplikation erfolgte in 6 Sekunden. Sein Schöpfer war der Amerikaner Howard Aiken (1900 – 1973). Er hatte an der Universität von Wisconsin studiert und bekam 1939 einen Lehrstuhl in Havard, wo er mit drei Kollegen den MARK I entwickelte. Der MARK I wird vor allem in Amerika als der erste Computer angesehen. Somit gilt Aiken bei vielen amerikanischen Historikern als Erfinder des ersten Computers. Aiken entwickelte den MARK I noch weiter. 1947 stellte er einen vollständig elektronischen Rechner fertig, der die Bezeichnung MARK II trug [Revolution].

Als die Entwicklung des MARK I in Deutschland durch den Geheimdienst der Nazis bekannt wurde, mußte Alwin Walther Stellung nehmen, warum es in seinem Institut keine gleichartigen Entwicklungen gäbe. Das hatte zur Folge, dass Walthers Anträgen höchste Priorität eingeräumt wurde. [*Zitat,* Netzwerk für Wissensweitergabe[1]] „ ... die mangelnde Weitsicht der deutschen Führung ... zeigt sich, da der Rechenautomat der IPM auch zur Datenverarbeitungsanlage auszubauen gewesen wäre, wenn damals schon das geringste Bedürfnis danach bestanden hätte.“



[Abbildung der Mark I, Quelle: Revolution]

2.5 Manhattan-Projekt – Die Geburtsstunde der Kybernetik

Anfang der 40er Jahre gab der damalige Präsident Eisenhower dem Massachusetts Institute of Technology, kurz MIT, einen Auftrag für mehrere Forschungsvorhaben. Ein Auslöser für diesen Auftrag war die Angst vor einer nuklearen Rüstung der Nazis. Dieser Auftrag trug den Titel „Manhattan Project".

Das MIT-Labor unterteilte sich in mehrere Sektionen. Es gab nicht nur ein Labor für Strahlungsforschung, in dem die Wissenschaftler die Atombombe entwickelten, sondern auch ein Labor für Servomechanismen, in denen Regelkreise und Fernsteuerungen für Waffensysteme entwickelt wurden. Aus diesen Systemen wurden die heutigen Steuerungssysteme für Maschinen entwickelt, die in fast allen Produktionsanlagen zu finden sind [Helms[2], 1999].

In den damaligen Labor für Servomechanismen arbeitete auch Nobert Wiener, ein Mathematiker, der den Begriff der Kybernetik festlegte. Er definierte die Kybernetik, als die Wissenschaft vom Informationsfluß in offenen oder geschlossenen Regelkreisen. [*Zitat,* Helms[2], 1999] „Sie wurde die theoretische Grundlage für Computer, Mikroelektonik und die auf Mikroelektonik basierende und von Computern gesteuerte Automation."

Nach der Atombombardierung Hiroshimas und Nagasakis stellte sich Norbert Wiener die Frage, ob die von ihm begründete Kybernetik das technische Macht- und Vernichtungspotential vermehren könnte. Er kam zu der Einsicht, dass dies bereits geschehen war. Wiener schrieb einen offenen Brief an den Atlantic Monthly, der im Januarheft 1947 erschienen ist. In dem Brief forderte er seine Kollegen auf, ihre wissenschaftliche Arbeit der Gesellschaft zur Verfügung zu stellen. Er rief dazu auf, sich nicht an [*Zitat,* Helms[2], 1999] „die herrschende Macht" zu verkaufen. Er selbst wollte ein Zeichen setzen und schrieb, dass er bei seinen eigenen Forschungen entscheiden werde, ob er sie [*Zitat,* Helms[2], 1999] „ohne Gefahr für die Gesellschaft" veröffentlichen kann.

Es läßt sich nicht einschätzen, wieviel oder ob Wiener mit diesem Brief überhaupt etwas erreicht hat. Tatsache ist, dass in den 50er Jahren auf Veranlassung des Pentagons Elektrizitätswerke, Raffinerien und Chemiebetriebe im Namen der nationalen Sicherheit in eine vollautomatische Steuerung übergehen sollten [Helms[2], 1999].

2.6 1946 ENIAC

Das US-Militär förderte, ausgelöst durch den 2. Weltkrieg ein Projekt, genannt „Project PX“, dessen Ziel die Entwicklung einer vollelektronischen Rechenmaschine war. Sie sollte der automatischen Erstellung von Feuertabellen dienen, die für den Krieg gegen das Dritte Reich benötigt wurden. Diese Tabellen enthalten die ballistische Berechnung der Flugbahnen in Abhängigkeit zum verwendeten Geschoß [Korb, Siefkes, Törpel 1999].

Im August 1943 begannen John W. Mauchly und John Presper Eckert an der Universität Pennsylvania mit der Entwicklung des Röhrenrechners ENIAC. 1944 unterbreiteten sie dem Militär das Angebot, ENIAC für ballistische Berechnungen zu bauen. Das Angebot wurde angenommen und somit wurde ENIAC von dem Militär finanziert. Die Rüstungsindustrie benötigte für ihre neuen Geschütze Abschußtabellen. Ziel war es, eine analoge und mechanische Rechenmaschine zu konstruieren, die universell eingesetzt werden konnte. Die bis zu diesen Zeitpunkt verfügbaren Maschinen konnten diese Anforderungen nicht erfüllen. Sie waren zu langsam und ein kontinuierlicher, menschlicher Eingriff war vonnöten. Das Militär war bereit Millionen Dollar in dieses Projekt zu investieren. Wie groß die Schwierigkeiten bei ENIAC waren, läßt sich dadurch erkennen, dass er erst nach dem Krieg fertiggestellt wurde.

ENIAC war die erste vollelektronische Großrechenanlage der Welt, die Abkürzung steht für „Electronic Numerial Integrator And Calculator“. Er basierte auf Elektronenröhren. Der Vorteil der Elektronenröhre war es, ein trägerfreies Schaltelement zu sein, d.h. im Gegensatz zu einem Relais, in dem eine metallene Zunge bei jedem Schaltvorgang bewegt werden mußte, tauschen Röhren lediglich Elektronen zwischen zwei Polen aus. Somit lag der Vorteil der Elektronenröhre in der Geschwindigkeit. ENIAC war um den Faktor 1000 bis 2000 schneller als ein Relaisrechner. Jede Röhre repräsentierte eine Ja / Nein Entscheidung, bzw. eine Null oder eine Eins, also ein Bit. Auf diesem System (Binärsystem) aufbauend, war es möglich, dass komplexe mathematische Berechnungen durchgeführt werden konnten [McCormick[2]]. Doch wie wurde ENIAC programmiert? Er wurde mit 6000 Schaltern, bzw. Kabelsteckverbindungen programmiert, durch deren Verbindungen wurde ENIAC in die nötigen Zustände versetzt. Zuständig für diesen Vorgang war eine Gruppe von Mathematikerinnen, die den Spitznamen „ENIAC-Girls“ trugen. Ein Programm wurde zunächst auf einer Schalttafel zusammengestellt, die die Leitungen und Drähte zeigte. Dieser Vorgang war natürlich zu einem zeitaufwendig und äußerst kompliziert. Die Dateneingabe erfolgte über dekadische Drehschalter, auf denen die Ziffern 0 – 9 eingegeben wurden. Ein Nachteil war schon damals, dass Programme nicht gespeichert werden konnten. Als Speicher dienten nur 20 Akkumulatoren. Insgesamt umfaßte der Rechner an die 70.000 Widerstände,

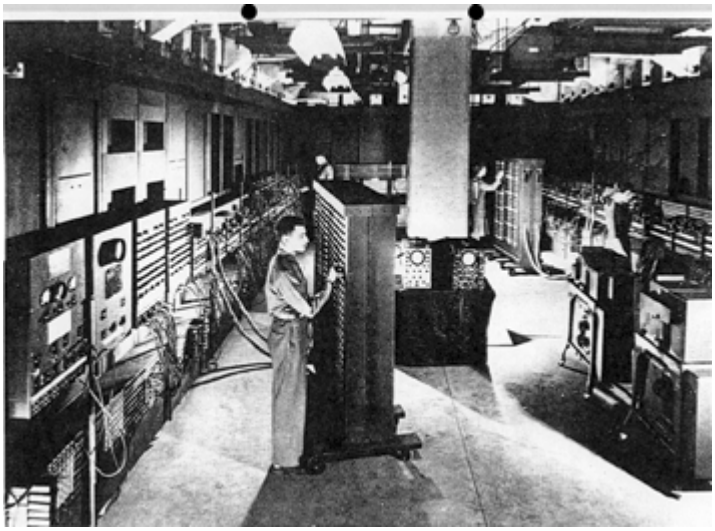
18.000 Elektronenröhren und 10.000 Kondensatoren. Sein Gewicht betrug 30 t und benötigte 140 qm. Daher war er in einer Halle untergebracht, die vom Militär strengstens bewacht wurde. Die Elektronenröhren wurden aufgrund der kurzen Lebensdauer mit _ ihrer Leistung betrieben. Zu seinen Eigenschaften zählte ein enormer Stromverbrauch, der sich mit dem Verbrauch einer mittleren Kleinstadt vergleichen ließ. Er erzeugte eine große Menge an Abwärme, die eine Kühlung erforderlich machte. Während ENIAC in Betrieb war, war eine Gruppe von Technikern beauftragt, defekte Lötstellen, es gab ca. 500.000 Lötstellen, und durchgebrannte Röhren zu finden und auszuwechseln, was ständig der Fall war [Sörgel[2], 1999].

In der Öffentlichkeit fand ENIAC durch die Medien einen großen Nachhall. In verschiedenen Artikeln wurde er unter anderem als „elektronisches Genie“ oder als „Supergehirn“ bezeichnet.

ENIACs Verwendung endete jedoch nicht mit dem Ende des 2. Weltkriegs. ENIAC spielte im Atombombenprogramm der USA eine wichtige Rolle [Bayrischer Rundfunk, 1998]. Mit ihm wurden entscheidende Berechnungen durchgeführt. Im Kalten Krieg diente er Wissenschaftlern als Rechner.

An der Entwicklung des ersten vollelektronischen Rechners waren auch John von Neumann und Herman Heine Goldstine beteiligt, die später das erste Programmierhilfsmittel, das „flow diagramm“ (Flußdiagramme) entwickelten. Von Neumann war fasziniert vom Rechnerbau und begann 1944 die Konzeption des speicherorientierten Rechenautomaten, genannt EDVAC. Der von ihm entwickelte logische Aufbau der Maschine wird heute verkürzt als Von-Neumann-Architektur bezeichnet [Korb, Siefkes, Törpel 1999].

Es läßt sich nicht abstreiten, dass der ENIAC einen technologischen Durchbruch darstellte und große Auswirkungen auf die Computerentwicklung hatte. Dies war jedoch erst durch die finanzielle Unterstützung des Militärs möglich.



[Personal beim Programmieren des ENIACS durch Verdrahtung, Quelle: Sörgel[2], 1999]

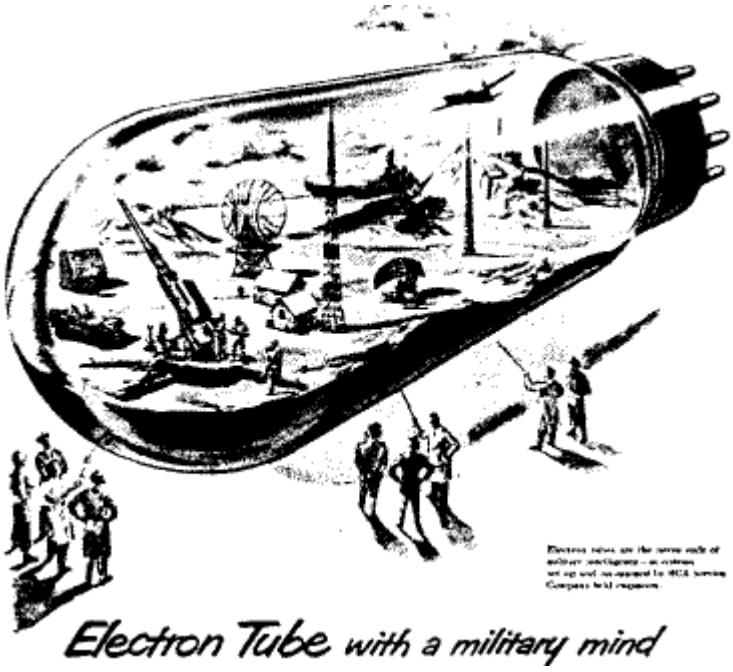
2.7 Gegendarstellungen

Nicht immer hat der 2. Weltkrieg die Entwicklung der Technik „positiv“ gefördert.
Die Arbeiten des Ingenieurs Konrad Zuse an seinen Rechenautomaten wurden durch den Krieg unterbrochen, da er zum Militärdienst eingezogen wurde. Das Heereswaffenamt urteilte über seine Arbeit, dass sie nicht unmittelbar von Nutzen sei. Nach dem Krieg unterlag auch er dem Arbeitsverbot der Alliierten, das jedoch aufgehoben wurde [Informatik Kolloquium, 2001].
Die Dienstverpflichtung von John Atanasof in den USA 1942 stoppte den Bau seiner schon fortgeschrittenen elektronischen Rechenmaschine.
IBM unterbrach zum größten Teil Forschungsprojekte, in denen Rechenmaschinen entwickelt werden sollten, und behandelte Regierungsaufträge [Sörgel[1], 1999].

2.8 Fazit

[*Zitat*, Helms[1], 1999] „Große Kriege pflegen auch bedeutende technologische Umwälzungen auszulösen“ Der 2. Weltkrieg verhalf der Kernenergie, dem Computer durch Röhrentechnik, Erfindung des Transistors und großen Projekten für Rechenanlagen zum Durchbruch. Auch die Automation und die telekommunikative Vernetzung haben ihre Wurzeln im 2. Weltkrieg. Auch technische Großprojekte hatten ihren Ursprung als Kriegsobjekte, die V2-Raketenentwicklung, auf deren Basis die Apollo Missionen gründeten, die Radarentwicklung und das Manhattan-Projekt [Tandler, 1997].

Abschließend kann man sagen, dass der Krieg den Computer zwar nicht entwickelt hat, aber er hat die Computerentwicklung sehr stark vorangetrieben.



[Karikatur 1940 – 1950 entstanden, illustriert die Nutzungserwartungen des Militärs in Bezug auf die neue Technik, Quelle: Sörgel[2], 1999]

3. Das Internet

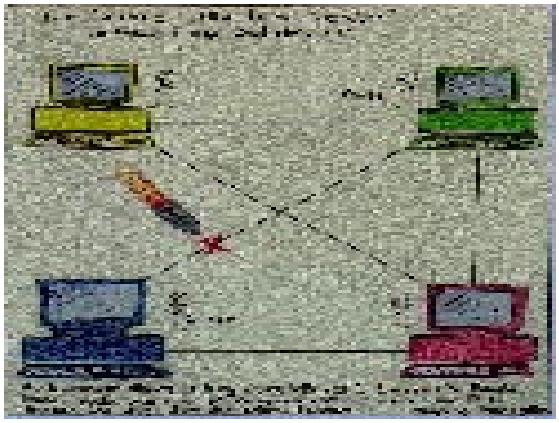
3.1 Der Anlass

Anfang der 60er Jahre machten sich die USA Gedanken über ein strategisches Problem:
Wie kann man die Kommunikation zwischen den staatlichen Einrichtungen und dem Militär nach einem Nuklearkrieg aufrechterhalten?
Anlass zu dieser Frage war die kurzzeitige technische Überlegenheit des Gegners, der UdSSR. Diese hatte nämlich im Jahre 1957 den Satelliten „Sputnik“ ins All geschickt und lösten damit den sogenannten „Sputnik-Schock“ bei den Amerikanern aus.
Das Internet ist somit ein Kind des Kalten Krieges.
Aber wie muss ein solches Netzwerk beschaffen sein, dass es auch nach schwersten Verwüstungen noch kommunikationsfähig bleibt?
Eines war klar: Es durfte nicht zentral gesteuert sein, denn dann bestand die Gefahr des Ausfalls durch einen Nuklearangriff, egal wie gut es geschützt war.
Die Lösung des Problems hieß „Distributed Network“, welches von Larry Roberts und Paul Baran entwickelt wurde. Larry Roberts äußerte später, dass er das Netz nicht entwickelt hatte,

um einem Atomkrieg standzuhalten, sondern dass dieser Grund nur dazu diente, das US - Militär als Geldgeber für die Realisierung zu gewinnen [Vetter].

3.2 Die Grundidee

Die Prinzipien waren simpel: „Das Netzwerk selbst musste dafür Sorge tragen, dass es zuverlässig arbeitete." [*Zitat,* Horibo]. Jeder Knotenpunkt des Netzes hatte somit denselben Status. Jeder Knoten war daher mit seiner eigenen Berechtigung, Daten zu senden, zu empfangen und zu übertragen, ausgestattet. Außerdem wurden die zu übertragenden Daten in Pakete zerlegt („Packet-Switching"). Das Paket wurde dann mit Absender und Adressat versehen. Wenn man nun die Datenpakete an einem Startknoten ins Netz schickte, war es absolut unbedeutend, auf welchem Weg dieses Paket zum Adressaten kam: Der Weg war damit also individuell.
Zwar scheint dieses System sehr ineffizient zu arbeiten, „da Kriterien, wie Laufzeiten der Pakete oder Dauer der gesamten Nachrichtenübermittlung nicht berücksichtigt wurden" [*Zitat,* Horibo], aber es war höchst ausfallsicher, solange Adressat und Absender Zugang zum Netz hatten.



[Skizze des „Distributed Network" von P. Barans, Vetter]

3.3 Die Entstehung

So entstand kurze Zeit später das erste Computernetz.
Die ARPA (Advanced Research Projects Agency), eine Behörde, die gegründet worden war, um den technologischen Vorsprung der USA nach dem Start des Sputnik durch die Sowjetunion zu bewahren, machte sich nun zum Ziel, die verschiedenen Netzwerke, die entstanden, miteinander zu verbinden [Uelkes, 1997]. Dazu brauchte man ein Netzwerkprotokoll, das es schaffte, Daten zu übermitteln, ohne dass bekannt war, durch

welche Technik dies geschah. Es folgte die Erfindung des TCP/IP. Dieses Protokoll wurde 1983 zum Standard für das ARPANET.
Im Jahre 1990 wurde das ARPANET durch das NSFNET ersetzt. Daraufhin folgte die Öffnung des Netzes: Mehr und mehr Länder und Personen machten nun Gebrauch vom neuen Medium. Die Benutzerzahl stieg stark an. Aber richtig massentauglich wurde das Netz erst durch die Einführung von Hyperlinks, durch die das WWW entstand, sowie die Erfindung leicht bedienbarer Browser.[Vetter]

4.Wichtige Digitale Waffensysteme

4.1 Das Global Positioning System (GPS)

Der Auftrag, das Global Positioning System (GPS) zu entwickeln, stammte vom amerikanischen Verteidigungsministerium Mitte der 80er Jahre. Mit Hilfe des GPS war es möglich, die Bestimmung der eigenen Position in Breite, Länge und Höhe über NN mit einer Genauigkeit von bis zu einem Meter durchzuführen. Allerdings stand diese Genauigkeit nur dem Militär zur Verfügung. Der zivile Nutzer konnte dieses Gerät zwar auch auf dem freien Markt erhalten, doch er musste Abstriche bei der Genauigkeit des GPS in Kauf nehmen: Die Abweichung vom exakten Standort betrug bei den zivilen Geräten 25 Meter [Stolba, 1995].
Das GPS arbeitet mit weltweit verteilten Sendern, die insgesamt ca. 1600 Frequenzen ausstrahlen. „Jede davon bildet ein bis zwei Bit der Information“ [*Zitat*, Stolba, 1995]. Anfällig ist das GPS in dem Fall, dass einzelne Sender problemlos zerstört und damit ganze Regionen der Erde mit keinem Signal mehr versorgt werden können [Stolba, 1995].
Des weiteren ist das Global Positioning System ein Paradebeispiel für ein „dual-use“ Projekt. Das Militär war bei der Entwicklung dieses Systems darauf bedacht, die Kosten für die Geräte durch die Massenfertigung im Zivilbereich möglichst gering werden zu lassen. Dieses Vorhaben gelang, denn der Gerätepreis sank von 100.000 Dollar im Jahre1984 auf unter 1000 Dollar in der Gegenwart. Weiterhin versprach sich das Militär eine rasantere Entwicklung und Forschung durch die zivilen Forschungseinrichtungen [Bernhardt, Ruhmann, 1997].

4.2 EMP-Waffen

Momentan lässt sich bei der Erforschung neuer Waffensysteme feststellen, dass die Entwicklung in Richtung der „sogenannten nichttödlichen Waffen“ [*Zitat*, Stolba, 1995] geht. Besonders bei den Mikrowellen und EMP (Elektromagnetical Pulse)-Waffen ist dies zu beobachten.
Bei der Explosion der ersten überirdisch getesteten Atombombe ist den Forschern aufgefallen, dass der elektromagnetische Impuls der thermonuklearen Explosion eine so starke Überspannung bei elektrischen Geräten im Umkreis verursachte, dass diese zerstört wurden.
Im Laufe der Zeit ist es nun gelungen, diese elektromagnetischen Impulse auch ohne Atomexplosion auszulösen. In naher Zukunft sollen nun Flugzeuge mit diesen Waffen ausgestattet werden. Zur Zerstörung von feindlichen Radaranlagen wird dann ein starkes Signal in der Eigenfrequenz der Radaranlage vom Flugzeug aus ausgelöst. Zur Abwehr solcher Attacken sollen die Radaranlagen abgeschirmt werden und nur mit Glasfaserkabel von außen her ansprechbar sein [Stolba, 1995].

4.3 Smart Weapons

Unter Smart Weapons versteht man „intelligente“ Waffen. Die Amerikaner sind auf diesem Gebiet Weltmarktführer. Solche Waffen sind mit Steuersystemen ausgestattet, die es ihnen erlauben, vollkommen selbstständig Ziele zu erfassen und zu zerstören. Realisiert werden diese Systeme durch leistungsstarke Mikroprozessoren, die diese Waffen „lenken“. Weiterhin kursieren Gerüchte über spektakuläre Waffen, wie zum Beispiel die Entwicklung von „Robotersoldaten in Ameisengröße“ oder silikonfressende Mikroben, die die Elektronik des Gegners „auffressen“ [Sollberger,1997].

5. Forschung und Entwicklung (FuE) in den USA

Die damalige Computerentwicklung wurde maßgeblich durch das Verteidigungsministerium der USA finanziert. Doch durch das Entstehen eines dynamischen Marktes im zivilen Bereich schien sich diese Phase überlebt zu haben. Doch nun im Zeitalter des Information Warfare bekommt die Entwicklung im technologischen Bereich für das Militär eine neue Bedeutung

und daher ist ein erweitertes Bemühen seitens des Militärs in der Entwicklung der Informations- und Kommunikationstechnologie zu beobachten.

„Der politische Umbruch Ende der 80er Jahre führte für westliche Militärs zwar zu einem Gewinn an militärpolitischer Stabilität zwischen den ehemaligen Machtblöcken, gleichzeitig aber zu Verlusten im Wehretat.“ [*Zitat*, Bernhardt, Ruhmann,1997].

Allein die Förderung und Entwicklung militärischer Computersysteme wurde für so bedeutend gehalten, dass sie von Kürzungen verschont blieb. Bis 1996 kostete die Beschaffung solcher computergestützter Systeme den USA 10Mrd. Dollar.

Daher machte sich das US Militär die „dual-use“ -Forschung zunutze: Hierbei bezeichnet der Begriff „dual-use“ -Forschungen, die sowohl zivil als auch militärisch genutzt werden können. Allerdings muss man zwischen den Begriffen „dual-use“ - Forschung und - Produkt klar differenzieren. So kann sich ein ziviles Produkt als nachträglich militärisch nutzbar herausstellen und wird somit ein „dual-use“ - Produkt.

Die Forschung hingegen stellt die militärische Nutzbarkeit ganz klar in den Vordergrund. Somit gilt sie auch offiziell als Militärforschung.

1994 stellte die USA, oder genauer gesagt das Department of Defense (DoD), ein militärisches FuE-Programm vor. In der Defensive Science and Technology Strategy wurden die verschiedenen Technologie-Gebiete benannt, in denen die Bedürfnisse des Militärapparates abgedeckt werden sollten.

„Im gleichzeitig erschienenen Defense Science and Technology Plan der konkreten militärischen FuE-Projekte bis zum Jahr 2005 werden 19 Technologie-Gebiete benannt, von denen 12 zur Informatik gehören.“ [*Zitat*, Bernhardt, Ruhmann,1997].

Die Kosten betrugen allein bis 1999 14,5 Mrd. Dollar.

Auf dem Gebiet „Computing und Software“ verfolgt das Department of Defense das Ziel, die modernsten und robustesten Computersysteme der Erde zu besitzen. „Die Entwicklung neuer Computerarchitekturen ist am Schlachtfeld orientiert.“ [*Zitat*, Ute Bernhardt und Ingo Ruhmann,1997].

Schon heute fallen im Department of Defense (DoD) mehrere Terabytes an Datenmasse an. Bis 2005 soll eine Steigerung auf 0,5 Petabyte erreicht werden. Um diese enorme Masse an Daten verarbeiten zu können, benötigt man global verteilte, massiv parallele Systeme. Die Komponenten sollen mehrere Billionen Operationen pro Sekunde bearbeiten. Eine Steigerung des Faktors 1000 wird bis 2005 angestrebt. Ferner wird ein Multimedia-Netzwerk mit einem Datendurchsatz von 155-655 MB pro Sekunde benötigt. Allein diese Zahlen sprechen schon für das enorme Interesse des Militärs im Bereich der Informations- und

Telekommunikationsentwicklung. Allerdings gibt es auch einige Probleme bei der Realisierung dieser Projekte: „Als Flaschenhals erweist sich die Verschlüsselung, da existierende Verfahren für die geplanten Geschwindigkeiten zu langsam sind.“ [*Zitat*, Bernhardt, Ruhmann, 1997].

Weiterhin ist die Ausrüstung eines jeden Soldaten mit einem Rechner und dessen Anbindung an Führungsstellen noch nicht realisierbar, da die Kooperation so vieler unabhängiger Computer in einem Netz zu Problemen führt.

Dieses Problem soll mit einer Konvergenz zwischen militärischen und zivilen Systemen zu einer „Single System Software Technology“ gelöst werden.

In Sachen Hardware setzt das DoD auf elektro-optische Komponenten. Der Grund ist nicht nur die höhere Geschwindigkeit dieser Hardware, sondern auch und vor allem ihre Unempfindlichkeit gegenüber Störungen. Schon für 2001 werden 10 Gigahertz-Prozessoren und optische Disks mit 4 Gigabyte Kapazität angepeilt. Bei der Weiterentwicklung des Chip-Design wird vornehmlich darauf geachtet, ihn gegen starke Mikrowellenstrahlung resistent zu halten.

Intelligente Systeme gehören auch zu den Forschungsgebieten des Plans. Die anfallenden Daten „bei der Lenkung von Schlachten per Computer macht nach Ansicht des DoD wissensbasierte Techniken notwendig.“ [*Zitat*, Bernhardt, Ruhmann,1997].

Es sollen sogar künstliche und menschliche Entscheidungsträger „Hand in Hand“ miteinander arbeiten.

Im Jahre 2005 sollen diese Systeme dann über ein gewisses Selbstbewusstsein verfügen, um bei den verschiedenen Operationen den vorliegenden Kontext zu verstehen [Bernhardt, Ruhmann, 1997]. Dies würde bedeuten, dass eventuell ganze Schlachten von diesen Systemen autark geleitet werden könnten. Allerdings ist es fragwürdig, ob dies auch tatsächlich der Fall sein wird.

6. Das Militär und die Künstliche Intelligenz

Hochtechnologie wird in der heutigen Zeit als integraler Bestandteil militärischer Überlegenheit und Stärke betrachtet. Daher ist es keine Überraschung, dass die gegenwärtige US-Militärdoktrin die Anwendung Künstlicher Intelligenz und anderer fortgeschrittener Computertechnologie zur Notwendigkeit erklärt hat. Die US-Army hat sich fünf Forschungsgebiete herausgegriffen, von denen vier direkt der Künstlichen Intelligenz

zugeordnet sind, nämlich hochintelligente Beobachtungs- und Zielverfolgungssysteme, verteilte Befehls-, Kontroll-, Kommunikations- und Aufklärungssysteme, selbststeuernde Munition und die Schnittstelle zwischen Soldat und Maschine. Auf diesem Gebiet gibt es schon zahlreiche Fortschritte zu vermelden. Politisch ist es außerdem verantwortungsbewusster, Maschinen in einer Schlacht zu verlieren als Menschen. Weiterhin ist es auch einfacher Maschinen zu bauen als Menschen zur Wehrpflicht zu zwingen. Die KI Forschung außerhalb des Strategic Computing Programs (SCP) hat schon große Fortschritte gemacht: Es wurden sogenannte „brillante“ oder auch „autonome“ Raketen entwickelt, die ihr Ziel selbstständig suchen, und ein Roboter als Hindernisräumpanzer entwickelt, etc.

Das amerikanische Strategic Computing Program (SCP) und die Aspekte der Computerentwicklung von „Star-Wars“ (Strategic Defense Initiative, SDI) sind ein enormer Gegenstand großer Debatten unter den Informatikspezialisten. Das SDI wurde von R. Reagan 1983 ins Leben gerufen. Es war das ehrgeizigste Rüstungsprojekt aller Zeiten. Diese Strategische Verteidigungsinitiative sollte die USA vom Weltraum aus unverwundbar machen. In Anspielung auf seine Schauspielkarriere erhielt das System rasch den Spitznamen „Krieg der Sterne“. Reagans Nachfolger Bush reduzierte SDI auf den Anspruch, maximal 200 versehentlich oder unerlaubt abgefeuerte Raketen abzufangen. Mit dem SCP versuchte das Militär sich auf Jahre in die Computerforschung einzukaufen. Man wollte die nächste Generation von Computern im militärischen Kontext entwickeln. Das SCP kann in Verbindung mit dem SDI als das komplexeste und größte Softwareprojekt der Welt angesehen werden. Die wissenschaftlichen Durchbrüche bei den Computern, die der „Sternen-Krieg“ benötigt, ist das Hauptziel des SCP.

Was das SCP besonders interessant macht, ist der Versuch Maschinenintelligenz zu revolutionieren. Dies ist allerdings nicht ohne fundamentale Durchbrüche in der Computerarchitektur und Symbolverarbeitung möglich. Dazu sagte Stephen Squires, Assistent-Director des Informating Processing Techniques Büro der DARPA: „Wir versuchen, wirklich einen neuen Typ der Computertechnologie zu entwickeln, nicht nur einfach neue Hardware.“ [*Zitat*, Gray].

Bei diesem Vorhaben sind zwar schon entscheidende Fortschritte im Bereich der Hardware erzielt worden, doch gibt es noch erhebliche Mängel bei der Realisierung der zugehörigen Softwareprogramme, die zur Steuerung des „Star Wars“ erforderlich sind [Gray].

7. Information Warfare

7.1 Definition Krieg

Der klassische Krieg ist der völkerrechtlich gehegte Krieg als Auseinandersetzung zwischen zwei oder mehreren Nationalstaaten unter Berücksichtigung der scharfen Unterscheidung zwischen Krieg und Frieden. Es gibt also eine eindeutige Unterscheidung zwischen Zivilisten und Soldaten sowie dem Schlachtfeld und dem zivilen Raum. Als Beispiel kann hier noch in weiten Teilen der erste Weltkrieg gesehen werden.
Der totale Krieg macht keine Unterscheidung mehr zwischen dem Zivilen und Militärischen. Unterschiede zwischen Soldaten und Zivilisten sowie zivilen und militärischen Zielen werden nicht mehr gemacht. Als Beispiel kann man hier den zweiten Weltkrieg anführen.
Der sanfte Krieg wird ohne Gewehr und Kugeln ausgetragen. Es werden „sanfte“ Angriffe gestartet bei denen „sanfte“ Verletzungen des Gegners in Kauf genommen werden. Neu ist nicht, dass der Krieg aufgrund der besseren Information gewonnen wird, sondern dass die Manipulation der Information der Krieg selber ist. Das Schlachtfeld ist der Cyberspace, die Soldaten sind Hacker und Programmierer. Die Folgen eines solchen Krieges werden allerdings in der Öffentlichkeit verharmlost, doch sie können verheerend sein, besonders für eine Informationsgesellschaft.
Da Sozialsysteme der Gesellschaft von der Wirtschaft über die Verwaltung und Wissenschaft auf die Telekommunikation- und Computertechnik angewiesen sind, sind Manipulationen dieser Systeme besonders folgenschwer: Zwei Wochen ohne Strom, Geld oder Telefon würden jedes Industrieland in eine Katastrophe stürzen [Werber, 1998].

7.2 Definition Information Warfare

„Information Warfare ist ein explosives Gemisch aus Wirtschaftskrieg, Spionage, elektronischer, psychologischer und virtueller Kriegsführung.“ [*Zitat,* Krempel, 1998] Die Abhängigkeit der heutigen Gesellschaft von der Informationstechnologie und Kommunikationssystemen nimmt in allen Bereichen immer mehr zu, in militärischen als auch in zivilen Informationsinfrastrukturen (IT-Infrastrukturen). Dadurch entsteht eine ungeahnte Verletzlichkeit. Sie stellt eine Schwachstelle dar, die zur Durchsetzung von unterschiedlichen Interessen ausgenutzt werden kann. Der Begriff Information Warfare steht für eine Kriegsführung mit Mitteln der Informationstechnologie, wie z.B. dem Internet, um politische

und wirtschaftliche Interessen gegenüber anderen Parteien durchsetzen, unter Ausnutzung einer Schwachstelle, die sich in einem jeden Kommunikations- und Informationssystem befinden kann.

Opfer des Information Warfare sind generell die Informationssysteme eines Gegners, also dessen Kommandosystem, auch bekannt unter C3I, d.h. Command-Control Communications-Intelligence.

Information Warfare wird auch als Krieg der Zukunft bezeichnet. Peter Leuthner, Leiter der Abteilung Systemtechnik Bodensysteme bei Daimler Benz Aerospace machte folgende Aussage: „Information Warfare findet ständig und überall statt und braucht keine Kriegserklärung.“ [*Zitat*, Krempel, 1998] Die Waffen in diesem Krieg sind Trojanische Pferde, Viren, die in den Computern und in den Netzen ihrer Nutzer ein unkontrollierbares, verheerendes Eigenleben hervorrufen können. Eine weitaus gefährlichere Waffe ist eine medial gesteuerte Desinformation, die den Nutzer falsche Schlussfolgerungen ziehen lässt. Auch E-Bomben gehören zum Arsenal des Informationskrieges. Bei ihrer Detonation werden elektromagnetische Impulse freigesetzt, die nicht nur Systemausfälle von Computern, sondern auch den Zusammenbruch von Funk- und Radaranlagen auslösen können.

Die Ziele eines solchen Krieges sind die vollständige Störung, Lähmung oder Zerstörung einer oder aller Informations- und Kommunikationssysteme. Eine vollständige Desinformation und Manipulation kann zum selben Ziel führen.

Als Täter kommen nicht nur feindlich gesonnene Staaten und Terroristen in Frage, sondern auch einzelne Personen mit beliebigem Motiv können diese Ziele erreichen.

Der eigentliche Begriff Information Warfare bezeichnete Anfang der 70er Jahre noch die Rolle von Medien im Krieg. 1976 wurde die heutige Sicht des Begriffs auf computergestützte Waffensysteme zurückgeführt. In den 80er Jahren betrieben US Militärs Analysen über den Wert und die systematische Nutzbarkeit von Daten und Informationen im Konfliktfall. 1994 erschien eine Studie der amerikanischen RAND – Corporation, in der Ideen zur Verteidigung und zum Angriff computergestützter Systeme präsentiert wurden [Bendrath, 1999].

7.3 Beispiel: Kosovo-Krieg

Im Mai 1999 schreckte das US-Nachrichtenmagazin Newsweek die Öffentlichkeit mit einer nach Science-Fiction klingenden Meldung: Demnach sollen Hacker des US-Geheimdienstes

CIA in die Computer ausländischer Banken eingedrungen sein, um die Konten Milosevics zu löschen. Autorisiert sei dieser Plan von Bill Clinton selber.
Der stellvertretende US-Verteidigungsminister bezeichnete den Krieg gegen Jugoslawien bereits im April als den ersten Cyberkrieg, den die USA führen.
Allerdings waren die Cyberattacken für den Ausgang des Krieges nicht entscheidend. Auch die Kriege in naher Zukunft werden noch keine unblutigen Kriege im Internet werden. Auffällig ist nur, dass sich auch politisierte Hackergruppen als neue Kriegsparteien auf das virtuelle Schlachtfeld gesellen.
Das amerikanische Konzept bei diesem Konflikt bestand aber nicht allein aus der Manipulation der Bankonten, sondern vor allem der Medien. Dies ist das eigentlich Entscheidende am Kosovo-Krieg: Wichtig ist nicht der Sieg auf dem Schlachtfeld (das es in diesem Luftkrieg nicht gab), sondern die Manipulation der medialen Repräsentation [Bendrath, 1999].

7.4 Denial of Service Attacks

Eine der größten Gefahren im Internet stellen sogenannte „Denial of Service-Attacks“ dar: Bei diesen Attacken werden Rechner im Internet zu Absturz gebracht, die dann vorübergehend anderen Nutzern nicht zur Verfügung stehen (deshalb auch „Denial of Service“, übersetzt soviel etwa wie „Verweigerung des Dienstes“). Eines haben fast alle Attacken gemeinsam: Sie nutzen die Löcher von „unsauber“ programmierten TCP/IP-Portierungen und schlecht administrierten Netzwerken aus.
Die erste Attacke erfolgte kurz vor Ostern auf ein elektronisches Postfach der NATO durch einen Belgrader Computer. Es war allerdings nur eine Massensendung von mehreren Tausend Emails, die das Postfach für mehrere Tage unzugänglich machte.
Von einigen Experten wird aber eher vermutet, dass sich die NATO den Computervirus „Melissa“ eingefangen hat, welcher die Adressverzeichnisse von Email-Programmen benutzt, um sich selbstständig weiterzuleiten. Dieser Virus hatte bereits im März im Pentagon sein Unwesen getrieben.
Des Weiteren wurde von US News berichtet, dass in Belgrad ein Netz aus mehr als tausend Studenten und Schülern in sechs Computerzentren existierte, das die kriegsbedingten Ferien dazu nutzte, im Internet gegen die NATO aktiv vorzugehen. Ihre Aufgabe bestand aus dem Füttern der Newsgroups und Pflege der zahlreichen Websites. Allerdings könnte der Virus oder der Datenmüll auch von hier stammen.

Insgesamt wurden fünf neue Viren in das Computernetz des westlichen Militärbündnisses übertragen [Bendrath, 1999].

Bei einer anderen Art von Angriff auf die öffentlichen Server der NATO wurde die Internet-Funktion „Ping“ genutzt.

Hierbei wird ein kleines Datenpaket an den Rechner gesendet, welches dieser an den Absender zurückschickt. Opfer einer massenhaften Ping-Anfrage wurde die NATO Ende März, was dazu führte, dass die Rechner überlastet waren. Nach Angaben der NATO kamen diese Angriffe ebenfalls aus Serbien.

Diese Art Angriffe, bei denen reguläre Funktionen so geballt benutzt werden, wobei der Rechner bei dementsprechend häufigen Aufrufen der Funktion lahmgelegt wird, nennt man „Denial of Service Attacks“. Dies ist allerdings eine recht simple Art der Störung.

Anders sieht es bei direkten Angriffen auf diverse Webseiten aus. Hacker aus Serbien sind in Webserver aus NATO-Staaten eingedrungen und haben die abrufbaren Web-Sites manipuliert. Die serbische Hackergruppe *CHC* ersetzte Anfang April die Internetseiten zweier US-Regierungseinrichtungen sowie der Stadt Croydon durch eine Anti-NATO-Seite. Hierbei wurde die NATO als „**N**ational **A**merican **T**errorist **O**rganisation“ diffamiert. Diese Angriffe richteten sich gegen die öffentliche Darstellung der NATO oder von NATO-Staaten im World Wide Web.

Die Kriegsunfähigkeit der NATO kann hiermit allerdings nicht erzwungen werden, denn die internen Kommunikations- und Kommandonetze verlaufen über andere Netze. Die Kommunikation zur Leitung der Kriegseinsätze ist nicht direkt mit dem Internet verbunden und somit sind hier die Sicherheitsvorkehrungen doch weit höher als bei Webservern oder Mailboxrechnern.

Des Weiteren laufen auf Militärcomputern meist Programme und Betriebssysteme, die auf dem freien Markt nicht erhältlich sind.

Einen Schritt weiter als Web-Hacker sind daher Versuche, direkt in Militärcomputer einzudringen. Dies versuchte ein Mitglied der serbischen Hackergruppe „Schwarze Hand“.

Er hat dabei angeblich die Daten eines Navy-Computers gelöscht, nachdem er in das System eingedrungen war. Obwohl das US-Verteidigungsministerium diesen Vorfall nie bestätigte, war der Rechner zeitweilig nicht über das Internet erreichbar.

Die „Schwarze Hand“ hatte schon im Jahr 1998 die Webseite des gemäßigten Albanerführers Ibrahim Rugova gehackt.

Nach der „versehentlichen“ Bombardierung der chinesischen Botschaft in Belgrad durch US-Kampfflugzeuge haben auch chinesische Hacker Gefallen daran gefunden, gegen Webseiten

amerikanischer Institutionen vorzugehen. Dabei wurde mehrmals das Internet-Angebot der amerikanischen Botschaft in Peking, des Energieministeriums und des Innenministeriums manipuliert. Auf diesen Seiten tauchten nun Texte, wie z.B. „Nieder mit den Barbaren!“ oder „Wir sind chinesische Hacker, die sich nicht um Politik kümmern, aber wir dulden es nicht, wenn wir sehen müssen, dass chinesische Journalisten getötet worden
sind.“[*Zitat*, Bendrath, 1999] auf.
Sogar die Webseite des Weißen Hauses wurde gehackt und war drei Tage lang nicht online, so einige Hackerforen.
Auch die russischen Hacker blieben nicht passiv, sondern griffen ein. Die Hackergruppe „From Russia With Love“ hat eine NATO-Webseite mit dem Vermerk „Haut ab aus Kosovo“ versehen. Es bildeten sich sogar regelrechte Koalitionen unter den russischen Hackergruppen, die nun gegen etliche Webseiten der USA und NATO vorgingen und Internetseiten reihenweise manipulierten.
Nach Angaben der NATO wurden mindestens vierzehn militärische oder staatliche Internetseiten gehackt.
Auf der anderen Seite der „virtuellen“ Front blieb man aber auch nicht tatenlos, sondern versuchte ebenfalls, Internetseiten zu manipulieren, zu löschen und zu hacken.
Hacker aus den USA sollen versucht haben, die Webseite der jugoslawischen Regierung zu knacken, die als extrem sicher gilt.
Die Kosovo Hacker Group (Verbindung aus albanischen und europäische Hackern) soll mindestens fünf verschiedene serbische Webseiten gelöscht haben und durch eine schwarzrote Flagge mit der Aufschrift „Freiheit für Kosovo“ ersetzt haben [Bendrath, 1999].

7.5 Die Gegenmaßnahmen

Der Besonderheit des Information Warfare (IW) und seinen schweren Auswirkungen können nur spezielle, auf den IW zugeschnittene Sicherheitsvorkehrungen entgegenwirken. Aufgrund der Vielfalt des Information Warfare, von einem isolierten Angriff auf ein unbestimmtes Computersystem bis zu einem strategisch geplanten Eindringen mit verschiedenen Mitteln der Informationstechnik zur Bedrohung des C3I eines Unternehmens oder eines Staates, sind daher verschiedene Gegenmaßnahmen erforderlich. Die Integrität und die Verfügbarkeit eines Individuums oder einer Institution ist besonders im IW gefährdet. Auch in diesem Bereich müssen starke Sicherheitsvorkehrungen getroffen werden.

In der Informationsstruktur des zu schützenden Bereichs, sei es in einem Unternehmen oder in einem Staat, muss eine Trennung erfolgen. Die Trennung muss nach den Gesichtspunkten „lebenswichtig“ und damit besonders schützenswert und „nicht lebenswichtig“ erfolgen. Diese Aufteilung erleichtert die Sicherheitsvorkehrungen und ist kostengünstiger, da sich die Vorkehrungen auf ein Mindestmaß reduzieren und die Angriffsfläche kleiner wird. Dadurch entstehen zwei unabhängige Systeme, das heißt, es ist für einen Außenstehenden nicht möglich, das „lebenswichtige“ System anzugreifen. Eventuelle Daten, die von einem System zum anderen übertragen werden, könnte man auf Datenträger kopieren und in das entsprechende System einbinden. Um die Unverletzlichkeit zu garantieren, ist es ratsam, die Datenträger auf Viren oder Trojanische Pferde zu überprüfen. Je größer ein Netz ist, desto anfälliger ist es für den IW. „Ziel muss es dabei sein, den Grad der Vernetzung – insbesondere für lebenswichtige Anwendungen – auf das erforderliche Minimum zu reduzieren.“ [*Zitat*, Cerny].
Der größte Schwachpunkt eines Netzes ist die Schnittstelle zwischen dem externen Netz (Internet) und dem Inneren. Daher ist es zwingend notwendig, diese Stellen besonders zu schützen. Dazu sind Programme notwendig, die Eindringversuche erkennen, entsprechend unterbinden und zurückverfolgen, um den Täter, bzw. seinen Rechner, ausfindig machen zu können. Es müssen insbesondere Verschlüsselungsverfahren angewendet werden, um die Integrität von vertraulichen Informationen zu wahren. Herstellerfirmen – wie zum Beispiel Microsoft – müssen die Sicherheitseigenschaften ihrer Produkte verbessern oder Produkte mit speziellen Sicherheitsvorkehrungen für Unternehmen entwickeln, da ein großer Prozentsatz der Unternehmen nicht in der Lage ist, ein eigenes Betriebssystem zu erstellen. Eine unabhängige Behörde könnte zum Beispiel diese Produkte einer Untersuchung unterziehen und bei Erfüllung aller Anforderungen ein Zertifikat erstellen [Cerny].

8. Fazit

Durch die Entwicklung neuer Informations- und Kommunikationssysteme ist das Militär seit der Existenz des Information Warfare dazu gezwungen, neuere und bessere Systeme als seine Gegner herzustellen. Denn wenn das Szenario eintreten sollte, dass man nur einen Rechner und ein Modem braucht, um einem Staat den Krieg zu erklären, würde dieser sein Gewaltmonopol verlieren.
Aus diesem Grund werden die Wehretats bei der Computerentwicklung auch nicht gekürzt.

Außerdem geht der Trend von den Massenvernichtungswaffen hin zu den „nichttödlichen Waffen“ und gezielten Waffen, bei denen ein starker Anteil von digitalen Systemen genutzt wird.
Abschließend läßt sich sagen, dass der Militärapparat nicht wie im 2. Weltkrieg die Computerentwicklung gefördert hat, sondern sie heutzutage für die eigenen Interessen eher benutzt, als sie eigenständig zu entwickeln.

Literaturverzeichnis

[Bayrischer Rundfunk, 1998]. Bayrischer Rundfunk *Dynamik der Technologie*, 14.10.1998 http://www.br-online.de/wissenschaft/deutsches-museum/macht_sc.html

[Bendrath, 1999] Bendrath, Ralf *Der Kosovo-Krieg im Cyberspace*, 1999 http://www.heise.de/tp/deutsch/special/info/6449/1.html

[Bernhardt, Ruhmann, 1997] Bernhardt, Ute; Ruhmann, Ingo *Rüstungsforschung in der Informatik* http://fiff.informatik.uni-bremen.de/ruin/funde.htm

[Beutelsbacher, 1996] Beutelsbacher, Albrecht *Kryptologie*, 1996 http://www.e-algebra.de/buecher/krypto.html

[Cerny] Cerny, Dietrich *Information Warfare – Eine Neue Bedrohung für Staat und Wirtschaft* http://www.bsi.de/literat/tagungsb/cerny.htm

[Geschichte] *Geschichte des Computers* http://www.darmstadt.gmd.de/schulen/AKG/Schule/Faecher/Kunst2/Produkte/jutta/gesch.html

[Gray] Gray, Chris H. *Das Strategic Computing Program nach vier Jahren* http://www.uni-muenster.de/PeaCon/wuf/wf-87/8750700m.htm

[heise-online] *Dokumentation von Alan Turings Colossus II freigegeben, 0*4.10.2000 http://www.heise.de/newsticker/data/wst-04.10.00-01.html

[Helms[1], 1999] Helms, Hans G. *Datenverarbeitung bei Militär und SS*, 28.12.1999 http://www.jungewelt.de/start.html

[Helms[2], 1999] Helms, Hans G. *Militarisierung der Gesellschaft*, 29.12.1999 http://www.jungewelt.de/start.html

[Horibo] Horibo *Die Geschichte des Internet* http://www.users.comcity.de/~horibo/history.htm

[Informatik Kolloquium, 2001] Zuse, Horst *Vortrag : Geschichte des Computers*, 8.5.2001

[Korb, Siefkes, Törpel, 1999] Korb, Joachim; Siefkes, Christian; Törpel, Bettina *Programmierhilfsmittel Flowcharts – Historische Entwicklung*, 21.04.1999 http://tal.cs.tu-berlin.de/gazzi/wise98/ausarbeitungen/flowcharts/flowcharts.html

[Krempel, 1998] Krempel, Stefan *Nicht erklärte Kriege – Geheimdienste und Militärs haben Computer und Datennetze im Visier*, Zeit Nr.48, 1998 http://www.archiv.ZEIT.de/daten/pages/199848.comp_-

infowar.html

[Lion, 2000] Lion, *Mediengeschichte – Informationsgesellschaft – Cyberethik, Thema: Colossus, Bomba, Enigma,* Februar 2000
http://www.unibw-muenchen.de/campus/SOWI/instfak/wige/seising/ega/Lion.html

[McCormick[1+2]] McCormick, Jim *Essay über das Silicon Valley*
http://www.members.aol.com/CompHist/valley.html

[Netzwerk für Wissensweitergabe] Netzwerk für Wissensweitergabe
Computergeschichte – Beteiligte Persönlichkeiten,
http://www.susas.de/com_personen.html

[Netzwerk für Wissensweitergabe[1]] Netzwerk für Wissensweitergabe *Die Rechenarbeiten des IPM in Darmstadt unter Leitung Alwin Walther*
http://www.susas.de/computergeschichte10.html

[Revolution] *Der weite Weg bis technischen Revolution*
http://museum.ruhr.de/docs/history2.html

[Singh, 1999] Singh, Simon *Geheime Botschaften – Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet (Seite 295 –298),*
Hanser Verlag, 1999

[Sollberger, 1997] Sollberger, Adi *Im nächsten Krieg sind Datennetze das Angriffsziel,*
Weltwoche,1997
http://www.weltwoche.ch/archiv/ausland/04.97.warfare.html

[Sörgel[1], 1999] Sörgel, Hartmut *Computergeschichte als Teil einer Technikgeschichte*
http://www.uni-lueneburg.de/einricht/rz/Veranst/einf/Geschichte/C_Geschichte.html

[Sörgel[2], 1999] Sörgel, Hartmut *2.Weltkrieg*
http://www.uni-lueneburg.de/einricht/rz/Veranst/einf/Geschichte/C_Geschichte.8.html

[Stolba, 1995] Stolba, Daniel *Information Warfare – elektronische Kriegsführung,*
1995
http://www.foebud.org/texte/ccc/ccc95/artikel/warfare.htm

[Tandler, 1997] Tandler, Agnes Charlotte *Zukunftsvisionen,* 1997
http://www.zigt.ze.tu-muenchen.de/braun97.html

[Uelkes, 1997] Dr. Uelkes, Peter *World Wide Web – Vorreiter der globalen Kommunikation,* erschienen in der Zeitschrift „Wechselwirkung“ im Februar 1997

[Verlag Heinz Heise GmbH] *Armageddon des Internets : Information Warfare*
http://www.heise.de/tp/deutsch/special/info/6271/4.html

[Vetter] Vetter, Tobias *Die Geschichte des Internets*
http://www.phil-fak.uni-duesseldorf.de/mmedia/web/index6.html

[Werber, 1998] Werber, Niels *Der Krieg hat schon begonnen – und jeder kann mitmachen,* 1998
http://www.heise.de/tp/deutsch/special/info/6300/1.html