Proseminar Informatik und Gesellschaft

Abschlussbericht zum Proseminar

Veranstalter:
Rüdiger Valk

Wintersemester 2009/2010

Inhaltsverzeichnis

Vorwort

Das Proseminar Informatik und Gesellschaft fand im Wintersemester 2009/10 mit einer Teilnahme von 20 Studierenden statt. Am ersten Termin wurden vom Veranstalter mögliche Themen vorgeschlagen und verteilt, wobei maximal drei Teilnehmer ein Thema gemeinsam bearbeiten konnten. Am zweiten Termin hat jede Gruppe kurz ihr Thema vorgestellt und es wurden z.T. erste Erfahrungen mit der Präsentation gesammelt.

Der dritte Termin fand in der Bibliothek statt, wo Frau Obernesser eine schöne Einführung in die Literaturrecherche gab. Eine ausführlichere Kurzfassung des Themas wurde dann von jeder Gruppe am vierten Termin gegeben, worauf dann die Gruppen in neun Sitzungen den ausführlichen Vortrag hielten.

Für die Hausarbeit wurde eine LaTex-Vorgabe gestellt, die auch weitgehend befolgt wurde. Dieses Heft enthält eine Zusammenstellung aller Hausarbeiten, wozu kleine Modifikationen der Originalbeiträge notwendig waren. Obwohl die Texterstellung in LaTeX für viele eine Mehrarbeit bedeutete, haben einige im nachhinein dies gegrüßt, da sie auf diese Weise Erfahrung für spätere Examensarbeiten sammeln konnten.

Ich danke Herrn Dr. Moldt für den Vorschlag des Konzepts zur Durchführung des Proseminars und Herrn Dr. Duvigneau für die LaTeX-Vorlage.

Rüdiger Valk Hamburg, April 2010

Vorratsdatenspeicherung

Jan Brendemühl, André Richter, Till Schomborg

Zusammenfassung

Die Ausarbeitung zum Thema Vorratsdatenspeicherung bezieht sich hauptsächlich auf die Enstehungsgeschichte, die Durchführung dieser Thematik, die aufkommende Kritik sowie die zukünftigen Aussichten. Es wird besonders im Detail die Vorgeschichte diesbezüglich betrachtet und die damit verbundenen gesetzlichen Grundlagen, die die Vorratsdatenspeicherung erst ermöglichten. Des Weiteren wird verdeutlicht um welche Daten es sich handelt, warum und wie diese gespeichert werden sowie welcher Zweck im Endeffekt daraus resultiert. Anschließend folgt eine kritische Betrachtung der Vorratsdatenspeicherung, in der vor allem Argumente beider Seiten gegenübergestellt, Statistiken offengelegt und Missstände sowie Bedenken dargelegt werden. Den Abschluss bildet die Darstellung inwiefern versucht wird, sich dagegen zu wehren und welche Aussichten zukünftig bestehen.

1 Hintergründe

1.1 Definition

Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren bestehen. Die Vorratsdatenspeicherung ist eine Vorstufe der Telekommunikationsüberwachung. Die auf Vorrat zu speichernden Daten erlauben weitgehende Analysen persönlicher sozialer Netzwerke. Mit Hilfe der auf Vorrat zu speichernden Daten lässt sich, ohne dass auf Kommunikationsinhalte zugegriffen wird das Kommunikationsverhalten jedes Teilnehmers analysieren. Die Vorratsdatenspeicherung ist verfassungsrechtlich umstritten, da sie anlasslos in die Grundrechtspositionen sämtlicher Nutzer elektronischer Dienste eingreift. In dem Maße, in dem die Kommunikation über elektronische Medien zunimmt, wird die Bedeutung solcher Analysen für die Erstellung von Persönlichkeitsprofilen wachsen[1].

1.2 Vorgeschichte

Auch die Pläne zur Vorratsdatenspeicherung gehen auf den 11. September 2001 zurück. Kurz nach den Anschlägen gegen die Vereinigten Staaten forderte der Ministerrat die EU-Kommission zu Vorschlägen auf, wie Straftaten mittels der Telekommunikationsüberwachung besser aufgeklärt werden könnten.Im Jahr 2002 wurde dann erstmals die Vorratsdatenspeicherung auf europäischer Ebene erörtert; und zwar legte die dänische Regierung, die damals die Ratspräsidentschaft

[1] http://www.vorratsdatenspeicherung.de/content/view/78/86/lang,de/

inne hatte, einen ersten Entwurf zur Vorratsdatenspeicherung vor, der eine Aufbewahrungsfrist der Daten von 12 Monate vorsah. Dieser Entwurf fand jedoch keine Mehrheit. Somit hatte sich das Thema auch wieder gelegt in der EU. Erst nach den Madrider Zuganschlägen vom 11.März 2004 forderte der europäische Rat den Ministerrat auf zu überprüfen, welche Rechtsvorschriften zur Vorratsdatenspeicherung zu erlassen sind. Die Regierungen von Irland, Frankreich, Schweden und Großbritannien übernahmen die Aufgabe und legten einen ersten Entwurf eines Rahmenbeschlusses am 29.April 2004 vor. Der Entwurf sah eine Mindestspeicherfrist von zwölf Monaten und eine Höchstspeicherdauer von 36 Monaten vor. Im Unterschied zum 2002er Entwurf sollte die Vorratsspeicherung auch zur Straftatenverhinderung erfolgen und nicht nur zur Aufklärung und Verfolgung bereits begangener Delikte. Gegner der Vorratsdatenspeicherung und Angehörige des Europäischen Parlaments reagierten auf das Vorhaben mit Kritik und warfen dem Ministerrat Kompetenzanmaßung vor. Sie vertraten die Ansicht, dass die Vorratsdatenspeicherung zumindest zum Teil in die Zuständigkeit des EU-Parlaments eingreife. Die Vorratsdatenspeicherung müsse deshalb durch eine vom EU-Parlament verabschiedete Richtlinie eingeführt werden.

Ein Rahmenbeschluss des Rats reiche nicht aus. Der EU-Justizkommissar Franco Fratini forderte auf, von dem Rahmenbeschluss abzusehen. Allerdings arbeitete der Rat weiter an einem mehrheitsfähigen Rahmenbeschluss, aber die unterschiedlichen Vorstellungen der nationalen Regierungen bezüglich der Speicherfristen machten das Vorhaben problematisch. Die Terroranschläge vom 7.Juli 2005 in London und die Übernahme der Ratspräsidentschaft von Großbritannien lösten einen neuen Schwung bezüglich des Themas Vorratsdatenspeicherung aus, sodass es zu einem neuen Entwurf einer Richtlinie kam. Der Entwurf beinhaltete, dass Internetdaten mindestens 6 Monate und Telefondaten mindestens 12 Monate gespeichert werden sollten. Längere Fristen sollten zugelassen werden. Das Europäische Parlament griff den Entwurf auf, änderte einige Punkte ab und zusätzlich hatte der federführende Berichterstatter Alexander Alvaro mehr als 200 Änderungsanträge der Parlamentarier zu berücksichtigen. Man stand also vor der schwierigen Aufgabe diesen Entwurf für alle optimal abzuändern. Der Alvaro-Entwurf stieß sowohl bei den Befürwortern als auch bei den Gegnern der Vorratsdatenspeicherung auf Kritik. Der Ministerrat ergriff schließlich abermals die Initiative und verhandelte hinter dem Rücken des Berichterstatters mit einflussreichen EU-Parlamentariern unter dem Vorbehalt den vorhandenen Rahmenplan zu verabschieden. Schließlich gelang es dem britischen Innenminister Charles Clarke am 30.November 2005 die Vorsitzenden der christ- und sozialdemokratischen Fraktionen des Europaparlaments in wesentlichen Punkten auf die Position des Rats zufrieden zu stellen. Der geänderte Entwurf wurde dem Europäischen Parlament daraufhin als so genannter Kompromissvorschlag vorgelegt. Am 14. Dezember 2005 stimmte das Europaparlament mit 378 zu 197 Stimmen für den „Kompromissvorschlag“. Der von Charles Clarke ausgehandelte Entwurf hatte damit nach nur drei Monaten die parlamentarische Hürde genommen und wurde somit zur schnellsten verabschiedeten Richtlinie der EU. Der Ministerrat stimmte am 21. Februar 2006 mehrheitlich für den Entwurf. Es erfolgte ein Umsetzung der „Richtlinie 2006/24/EG“ in den EU-Ländern. Lediglich die Slowakei und Irland stimmten aus formalen Gründen gegen die Richtlinie. Sie reichten eine Klage beim europäischen Gerichtshof ein. Am 10. Februar 2009 wies der Europäische Gerichtshof die Klage aber ab. Es sei die

Fraktion	Für das Gesetz	Gegen das Gesetz	Nicht teilgenommen	Enthalten
CDU/CSU	190 (84%)	4 (2%)	30	0
SPD	176 (79%)	7 (3%)	37	2
FDP	0 (0%)	58 (95%)	3	0
Linke	0 (0%)	41 (77%)	12	0
Bündnis 90/Grüne	0 (0%)	45 (88%)	6	0
fraktionslos	0	1	1	0
insgesamt	366 (60%)	156 (25%)	89 (15%)	2

Abbildung 1: Resultat der Bundestagsabstimmung am 9.November 2007
[4]

richtige Rechtsgrundlage gewählt worden, weil die Richtlinie schwerpunktmäßig dazu diene, die Anbieter vor unterschiedlichen Speicherpflichten innerhalb der EU zu schützen. In seinem Urteil stellt der Gerichtshof jedoch klar, „dass sich die von Irland erhobene Klage allein auf die Wahl der Rechtsgrundlage bezieht und nicht auf eine eventuelle Verletzung der Grundrechte als Folge von mit der Richtlinie 2006/24 verbundenen Eingriffen in das Recht auf Privatsphäre.“

2 Durchführung

2.1 Gesetzliche Grundlagen

Das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/ EG“[2] , zeitgleich die letzte Zusatzänderung im BKA-Gesetz, wurde am 9. November 2007 durch die Abstimmung im deutschen Bundestag von der Mehrheit der Abgeordneten beschlossen , am 26. Dezember 2007 von Bundespräsident Horst Köhler unterzeichnet und trat am 1. Januar 2008 in Kraft. Es stellt die gesetzliche Verpflichtung dar Daten aus Telekommunikationsdiensten, sogenannte „Verkehrsdaten“, durch deren Anbieter für einen Mindestzeitraum von 6 Monaten und einen Maximalzeitraum von 7 Monaten zu Speichern. Nach Ablauf dieser Frist besteht allerdings keine unverzügliche Löschungspflicht durch den Anbieter.[3] Mit großer Mehrheit befürwortete vor allem die große Koalition aus CDU/CSU und SPD dieses Gesetz, wobei sich die oppositionellen Parteien nahezu einstimmig dagegen aussprachen. Gerade die SPD versucht gegenwärtig die Gunst der Bevölkerung wieder zu gewinnen und das Gesetz möglichst zu ent-

[2] http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s3198.pdf
[3] http://www.vorratsdatenspeicherung.de/content/view/78/86/lang,de/

schärfen bzw. im Endeffekt wieder abzuschaffen. Grundlegend für diesen Gesetzesbeschluss durch den Bundestag war die „Richtlinie 2006/24/EG“[5] der Europäischen Union über die Vorratsspeicherung von Daten. Zweck dieser Richtlinie ist die Vereinheitlichung der nationalen Vorschriften aller EU-Mitgliedsstaaten bezüglich der Speicherung von sogenannten Verkehrsdaten. Zudem soll sichergestellt werden, dass diese Daten ausschließlich für die Ermittlung und Verfolgung von Straftaten für einen bestimmten Zeitraum aufbewahrt werden. Deutschland setzte diese Richtlinie durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ national um, wobei eine gesetzte Frist der EU diesbezüglich nicht eingehalten wurde. Natürlich steht die Frage im Raum inwiefern die Befürworter in Deutschland dieses Gesetz rechtfertigen. [6]

Eine Auswahl von SPD-Abgeordneten gab freiwillig folgende Begründung dazu ab:

„Trotz schwerwiegender politischer und verfassungsrechtlicher Bedenken werden wir im Ergebnis dem Gesetzentwurf aus folgenden Erwägungen zustimmen. Erstens. Grundsätzlich stimmen wir mit dem Ansatz der Bundesregierung und der Mehrheit unserer Fraktion dahingehend überein, dass die insbesondere durch den internationalen Terrorismus und dessen Folgeerscheinungen entstandene labile Sicherheitslage auch in Deutschland neue Antworten benötigt. Eine Zustimmung ist auch deshalb vertretbar, weil davon auszugehen ist, dass in absehbarer Zeit eine Entscheidung des Bundesverfassungsgerichts möglicherweise verfassungswidrige Bestandteile für unwirksam erklären wird.“[7]

Das Ziel dieser Speicherung von Verkehrsdaten ist also nach Ansicht der Befürworter insbesondere die mögliche Prävention jeglicher Art von Terrorismus. Im Übrigen sind die Abgeordneten sich allerdings schon im Klaren, dass dieses Gesetz im Einzelnen verfassungswidrige Bestandteile enthält, da gewisse Grundgesetze vorsätzlich verletzt wurden. Zudem beschloss der Bundestag am 17. Juni 2009 einen Gesetzesentwurf, der das Protokollieren des Surfverhaltens von Internetnutzern auf staatlichen Seiten bzw. Internetportalen vorsieht.[8]

2.2 Was wird gespeichert?

Hier wird verdeutlicht welche sogenannten Verkehrsdaten die gesetzliche Grundlage zur Speicherung vorsieht. Dabei werden verschiedene Bereiche unterschieden, in denen bestimmte Daten zu speichern sind.

Bei den normalen Telefondiensten sind es die Rufnummern alle Gesprächsteilnehmer, auch bei Gesprächsweiterleitungen, sowie die genaue Uhrzeit und das Datum des Anfangs der Gesprächsverbindung sowie dem Ende. Ebenso muss die Angabe des Dienstes gespeichert werden, den der Gesprächsteilnehmer im

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF

[6] http://de.wikipedia.org/wiki/Richtlinie/2006/24/EG/ueber/die/VorratsspeicherungvonDaten

[7] http://dip.bundestag.de/btp/16/16124.pdf Anhang 4, Seite 90

[8] http://www.vorratsdatenspeicherung.de/content/view/296/152/lang,tr/

Rahmen des Telefondienstes genutzt hat sowie im Übrigen die Kontaktdaten, also Name und Adresse, des Anschlussinhabers. Bei Benutzung von mobilen Telefondiensten ist der Anbieter verpflichtet die internationale Kennung aller Gesprächsteilnehmer, die sogenannte International Mobile Subscriber Identity(IMSI), zu speichern sowie die internationale Kennung aller Geräte, die sogenannte International Mobile Station Equipment Identity(IMEI), die in diesem Zusammenhang genutzt wurden. Ebenso wird die Bezeichnung der Funkzelle gespeichert, in der sich die Gesprächsteilnehmer während der Verbindung befinden. Dadurch ist zudem sogar eine geografische Ortung möglich, da durch das Signal mehrerer Funkmasten in der Zelle die Position des Gerätes errechnet wird.

Bei Benutzung von Internet-Telefondiensten mittels Voice-over-IP (VoIP) durch beispielsweise Skype werden die Verkehrsdaten wie bei den mobilen Telefondiensten gespeichert, also die internationale Kennung aller Gesprächsteilnehmer und der dazugehörigen Geräte sowie die Bezeichnung der genutzten Funkzelle. Des Weiteren wird aber in diesem Fall dazu noch die Internetprotokoll-Adresse gespeichert. Beim Versenden einer Kurz- oder Multimedianachricht wird der Zeitpunkt der Versendung sowie der Zeitpunkt des Empfangs dieser gespeichert.

Bei der Internetkommunikation per E-Mail werden jede E-Mail-Adresse sowie jede Internet-protokoll-Adresse gespeichert. Ebenso noch Uhrzeit, Datum und die dazugehörige Zeitzone beim Versenden der E-Mail mit dem jeweiligen Betreff. Der genaue Inhalt wird hingegen nicht gespeichert bzw. ist nicht einsehbar. Durch die Nutzung eines Internetzugangsdienstes ist der Anbiete verpflichtet die genaue Kennung des Internetanschlusses, über den die Nutzung erfolgt, zu speichern sowie die zugeteilte Internetprotokoll-Adresse. Hinzufügend werden der Beginn und das Ende der Internetnutzung mit der jeweiligen Uhrzeit sowie dem Datum und der zugrundeliegenden Zeitzone gespeichert[9].

2.3 Wie wird gespeichert?

Hier wird darauf eingegangen wie und mit welchen Methoden die Verkehrsdaten aus Telekommunikationsdiensten gespeichert werden und welche Institutionen daraus ihren Nutzen ziehen können bzw. dürfen.

Die Anbieter von Telekommunikationsdiensten speichern Verkehrsdaten auf externen Servern, die sozusagen in gewisser Weise zwischen den Anbindungen geschaltet sind.

Als Art der Visualisierung findet man in Abbildung 2 ein kleines Schema:

Durch diese Art der Speicherung werden vor allem sogenannte Bewegungs- und Kommunikationsprofile erstellt. Es ist ersichtlich wer mit wem zu welchen Uhrzeiten Kontakt aufnimmt, also beispielsweise über das Telefon kommuniziert, sowie an welchen Tagen. Ebenso wird verdeutlicht wer sich zu welchen Uhrzeiten an welchen Orten aufhält bzw. aufgehalten hat mittels geografischer Ortung durch die benutzte Funkzelle. Zu guter Letzt geben die gespeicherten

[9] http://de.wikipedia.org/wiki/Richtlinie/2006/24/EG/über/die/Vorratsspeicherung/von/Daten/Zu/speichernde/Daten

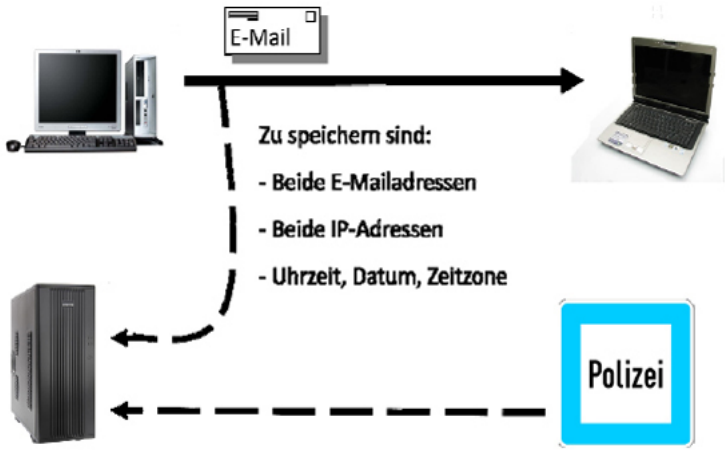


Abbildung 2: Beispiel E-Mail

Daten auch Aufschluss darüber wer wie lange und wo Interzugangsdienste in Anspruch genommen hat. Auf diese gespeicherten Verkehrsdaten und die daraus erstellten Bewegungs- und Kommunikationsprofile haben verschiedene Institutionen Zugriff. Zum einen vor allem der Bundesnachrichtendienst und zum anderen die Polizei einschließlich des Bundeskriminalamts. Der Zugriff auf die gespeicherten Verkehrsdaten darf allerdings nur unter bestimmten Voraussetzungen erfolgen. Es muss ein eindeutiger Tatbestand einer schweren Straftat vorliegen bzw. eine Planung dieser eindeutig ersichtlich sein, um dadurch also erhebliche Gefahren abzuwehren und somit die öffentliche Sicherheit zu gewährleisten. Ebenso können die gespeicherten Verkehrsdaten genutzt werden, wenn Straftaten mit Hilfe von Telekommunikation begangen werden bzw. geplant werden, beispielweise organisierte Kriminalität. Im Allgemeinen sind die Daten zur Erfüllung des Verfassungsschutzes an die jeweiligen Behörden von Bund und Länder zugreifbar.

2.4 Wie lange wird gespeichert?

Anbieter von Telekommunikationsdiensten sind verpflichtet die Verkehrsdaten in Deutschland mindestens 6 Monate und maximal 7 Monate zu speichern.

Diese Regelung der Speicherfristen kann jedes EU-Mitglied in ihren eigenen nationalen Vorschriften selbst auslegen. So sieht die Gesetzeslage in Polen zum Beispiel vor, dass Verkehrsdaten sogar bis zu 15 Jahre gespeichert werden können, was in Deutschland mit Sicherheit nicht realisierbar wäre.

2.5 Die Rolle Schäubles

Im Zusammenhang mit dieser Thematik wollen wir auch darauf eingehen inwiefern der damalige Innenminister und heutige Finanzminister Wolfgang Schäuble

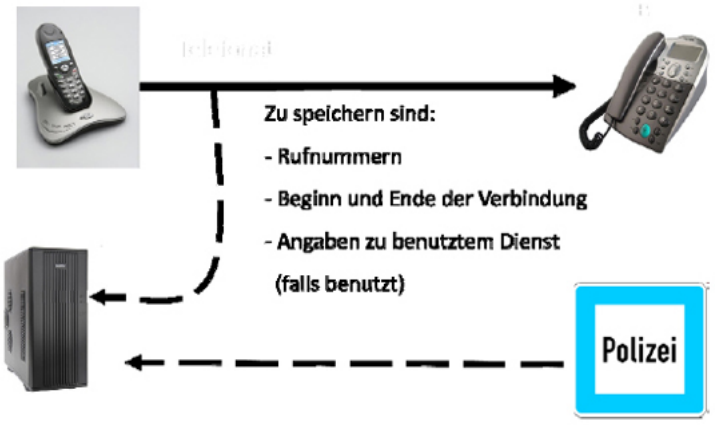


Abbildung 3: Beispiel Telefon

seinen Anteil hatte. Zum einen wird ihm eine Vielzahl von Vorwürfen gemacht, die mit der Thematik zu tun haben.

So wird ihm vorgeworfen, dass er unseren Freiheits- und Rechtsstaat in einen Überwachungs- und Präventivstaat umwandeln will durch jegliche Art von Maßnahmen sowie Methoden der Überwachung. Dieses Vorhaben wird besonders als Frontalangriff auf das bestehende Grundgesetz gesehen. Den Grundrechten soll sozusagen ein fiktives Grundrecht auf Sicherheit ungeordnet werden, was im ersten Moment akzeptabel und nachvollziehbar klingt, aber dennoch durch die angewandten Methoden kritisch betrachtet werden sollte. In diesem Zusammenhang wurde seine Sicherheitspolitik auch „Stasi 2.0“ bezeichnet an Anlehnung an das Ministerium für Staatssicherheit in der ehemaligen DDR und dem Web 2.0 der heutigen Internetgeneration.

Ebenso wird Schäuble vorgeworfen, dass er die Bevölkerung durch diese Methodik verängstigt, dass sich sozusagen jeder Bürger beobachtet fühlt und diese Ängste dazu benutzt, also sogar instrumentalisiert werden, um dieses Vorgehen zu rechtfertigen sowie eine angebliche Akzeptanz dafür zu schaffen. Ein weiterer Vorwurf besteht darin, dass Schäuble einige Fahndungserfolge bereits der Vorratsdatenspeicherung zugesprochen hat, obwohl zu diesem Zeitpunkt noch keine eindeutigen gesetzlichen Grundlagen dazu bestanden. Sozusagen damals bereits eine voreingenommene Rechtfertigung Schäubles.

Besonders kritisch wird sein Vorhaben gesehen, sogenannte „Internierungslager“ für potentielle Schwerstkriminelle zu errichten. In Schäubles Augen wären solche Leute „Gefährder“ der öffentlichen Sicherheit, die eben durch die Vorratsdatenspeicherung und der daraus resultierenden Fahndungen im Vorfeld beobachtet und verhaftet werden können. Es mag sicherlich für den Schutz der öffentlichen Sicherheit akzeptabel klingen, allerdings sollten ähnliche Verhältnisse wie bei

dem amerikanischen Gefangenenlager Guantanamo Bay nicht auftreten bzw. überhaupt nicht realisiert werden können. Herr Schäuble bestritt so ein Vorhaben konkret geäußert zu haben, allerdings wurde dies indirekt aus seinen Aussagen deutlich.

Viele dieser Vorwürfe stützen sich auf den von Herrn Schäuble entworfenen „Schäuble-Katalog“[10] , dessen Bestandteile hier im Einzelnen erläutert werden soll. Zum einen sieht dieser Katalog die Online-Durchsuchung vor, also einen gezielt verdeckten staatlichen Zugriff auf informationstechnische System mit Hilfe von Kommunikationsnetze. Im Klaren also ein Zugriff auf unsere Computer zu Hause oder sonst wo, die verdeckt durchleuchtet werden ohne das die Person etwas davon merkt. Natürlich geschieht dies nur auf richterlichem Beschluss und zur Strafverfolgung sowie Gefahrenabwehr. Dabei sind aber zwei Arten der Online-Durchsuchung zu unterscheiden. Auf der einen Seite die Online-Durchsicht, ein einmaliger Zugriff auf ein System und der Online-Überwachung, wenn sich der Zugriff über einen längeren Zeitraum erstreckt. Dadurch besteht natürlich die Angst einer aufkommenden Geheimpolizei wie sie damals in der DDR existierte, sodass jeder auf Verdacht ausgespitzelt werden kann.

Zum anderen ist durch diesen Katalog die Videoüberwachung und Gesichtserkennung z.B. an Flughäfen vorgesehen. Heutzutage ist die Videoüberwachung an öffentlichen Plätzen zur Normalität geworden, um Straftaten zu verfolgen und präventiv zu handeln. Hingegen ist die Gesichtserkennung eher nicht sehr präsent, aber auf dem Vormarsch. Gerade aufgrund von steigender Kriminalität und dem Hintergrund der steigenden Gefahr durch Terrorismus findet diese Art der Überwachung in der Gesellschaft eine breite Akzeptanz. Menschen fühlen sich zwar sicherer, wenn sie überwacht werden und im Zweifelsfall Hilfe erwarten können. Allerdings verhalten sich Menschen auch anders, wenn sie wissen, dass sie ständig beobachtet werden, als Menschen, die sich unbeobachtet fühlen. Dieser sogenannte Beobachtungsdruck beeinträchtigt die Freiheit und Unbeschwertheit von Menschen, die beobachtet werden oder es stets annehmen. Im Allgemeinen muss man diese Entwicklung aber auch kritisch sehen, da die Gefahr eines totalen Überwachungsstaates besteht, sodass Leute überall auf Schritt und Tritt beobachtet werden.

Als nächsten Bestandteil sieht der Katalog den biometrischen Ausweis und den genetischen Fingerabdruck vor. Auf solchen Ausweisen werden auf kontaktlosen RFID-Chips Daten wie persönliche Daten, Fingerabdruck oder Irismuster gespeichert. Kritisch ist zu sehen, dass auf solchen Ausweisen allerdings alle persönlichen Daten für jeden, der den Ausweis kontrolliert bzw. durch ein Gerät liest, ersichtlich werden. Zusätzlich dann auch, welche Krankheiten man hat oder sonstige intime Eigenschaften. Es besteht die Angst, dass diesbezüglich dann der sogenannte „gläserne Bürger“ entsteht. Der genetische Fingerabdruck hingegen wird bereits oft als Indiz bei Strafverfahren anerkannt, wird allerdings auch durch die teilweise vorherrschende Ungenauigkeit und Verfälschung kritisch betrachtet.

Der „Schäuble-Katalog“ sieht ebenso die bereits bestehende Anti-Terror-Datei

[10] http://www.tagesschau.de/inland/meldung32850.html

vor, die eine gemeinsame Datenbank von verschiedenen deutschen Ermittlungsbehörden, wie beispielsweise dem BKA, darstellt. Sie dient den Ermittlungsbehörden zum Informationsaustausch über mutmaßliche Terroristen und deren Organisationsstrukturen. Zugriff haben insbesondere das Bundeskriminalamt, die Bundespolizeidirektion, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt. Herr Schäuble persönlich forderte zudem noch einen zusätzlich Eintrag der Religionszugehörigkeit und der Berufskenntnisse. Im Allgemeinen gilt der Großteil der dort eingetragenen Personen als unbedenklich, lediglich ein kleiner Teil sei als eine akute Gefahr einzuschätzen. Zweifelhaft daran ist die dadurch eingestellte Trennung zwischen Polizei und Geheimdienst auf Grund der Datensammlungen von Betroffenen und aus deren Umfeld.

Ebenso fordert Schäuble den Einsatz der Bundeswehr auch im Inland für die Sicherung von Großveranstaltungen, Wahlen oder Besuchen von Staatsvertretern. Bei Katastrophenfällen, wie beispielsweise Flutkatastrophen, darf die Bundeswehr im Innern agieren. Normalerweise sollte die militärische von der polizeilichen Gewalt weiterhin getrennt bleiben. Allerdings ist es der Bundeswehr in Zukunft wohl möglich im Innern unter Umständen militärisch zu handeln, wenn die polizeiliche Gewalt nicht mehr ausreichen sollte. Dies soll im Grundgesetzartikel 35 ergänzt werden.[11] Konkret wird dabei auf gezielt geplante Terroranschläge eingegangen, bei denen eine große Anzahl von zivilen Opfern zu erwarten ist. Herr Schäuble spricht sich hingegen für einen generellen Einsatz der Bundeswehr im Inland aus.

Als letzter Punkt sieht der Katalog das Verbot von Anonymisierungs- und Kryptographieverfahren vor. Durch diese Methoden ist es möglich Online-Durchsuchungen, Abhörverfahren oder das allgemeine Speichern von Daten aus Kommunikationsverbindungen zu umgehen. Dies soll laut Herrn Schäuble natürlich unterbunden werden, damit diese ganze Thematik der Vorratsdatenspeicherung und Überwachung nicht durch potenzielle Schwerstkriminelle umgangen wird und jeder weiterhin auf Verdacht überwacht werden kann.

3 Kritik

3.1 Pro Argumentation

Grundsätzlich wird die Vorratsdatenspeicherung mit einer Notwendigkeit für die Kriminalitäts- und Terrorismusbekämpfung begründet. Die Ziele liegen in der Verhinderung von schweren Straftaten sowie einer erleichterten Strafverfolgung. Dabei sieht sich der Staat dazu verpflichtet, seine Bürger zu schützen und ihnen einen maximalen Anspruch auf Sicherheit zu gewährleisten. Basierend auf einer enormen Zunahme elektronischer Kommunikation in den letzten Jahren beruft sich die Richtlinie über die Vorratsdatenspeicherung auf wissenschaftliche Untersuchungen als auch auf praktische Erfahrungen in mehreren Mitgliedsstaaten der Europäischen Union, die zeigen, dass Verkehrsdaten ein notwendiges

[11] http://www.fr-online.de/in/und/ausland/politik/aktuell/1608853/Bundeswehr-darf-im-Inland-eingreifen.html

und wirksames Ermittlungswerkzeug bei der Strafverfolgung darstellen[12]. Vor dem am 14. Dezember 2005 erlassenen Gesetz sammelten die EU-Staaten unterschiedliche, beziehungsweise keine elektronischen Daten. Durch die Vorratsdatenspeicherung liegen nun einheitliche Daten im Binnenmarkt der Europäischen Union vor, die eine leichtere Strafverfolgung innerhalb der Mitgliedsstaaten ermöglichen sollen. Konkret wird sich auf die Aufklärung der geplanten Madrider Zuganschläge im Jahr 2004 berufen, bei deren Aufklärung Telekommunikationsdaten einen entscheidenden Beitrag leisteten.[13] Um das Leben potentieller Opfer vor Anschlägen und anderen Straftaten zu schützen, müssten alle verfügbaren Mittel ausgeschöpft werden.[14] Neben den bereits genannten Punkten sei die Vorratsdatenspeicherung ebenfalls zur Bekämpfung von Kindesmissbrauch, organisierter Kriminalität, Rechtsradikalismus und Phishing erforderlich.[15] Bezug nehmend auf die vielen kritischen Stimmen berufen sich die Befürworter der Vorratsdatenspeicherung darauf, dass keinerlei Inhalte erfasst werden und Zugriffe nur im Einzelfall getätigt werden. Außerdem habe Deutschland nicht mehr als die Mindestanforderungen der EU-Richtlinie umgesetzt.

3.2 Contra Argumentation

Datenschützer, Parteien, Verfassungsrechtler und Vertreter der verschiedensten Berufsgruppen wehren sich gegen die Vorratsdatenspeicherung. Für sie stellt das Gesetz eine Diskrepanz zwischen der Anzahl der Betroffenen und der (erwarteten) Verbrechen dar. Am stärksten kritisieren sie, dass dem Bundeskriminalamt ermöglicht wird, präventive Ermittlungen ohne konkreten Tatverdacht in Eigenregie durchzuführen. Somit kann die Vorratsdatenspeicherung als eine Überwachungsmaßnahme ohne tatsächliche Anhaltspunkte gesehen werden, die Millionen Menschen unbegründet kriminalisiert. Aus Sicht der Kritiker ist die Vorratsdatenspeicherung folglich ein unverhältnismäßiger Eingriff in die Privatsphäre eines jeden Bundesbürgers. Demnach liegt eine Verletzung des Rechts auf informationelle Selbstbestimmung vor, nämlich das Recht, über Offenbarung und Verwendung personenbezogener Daten selbst zu verfügen. Es besteht daher die Gefahr, dass personenbezogene Daten zu teilweisen oder weitgehend vollständigen Persönlichkeitsbildern zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung kontrollieren kann. Die Kritiker warnen vor Folgen von Abschreckung und Hemmungen. Missstände würden unter Umständen nicht weiter an die Presse oder Behörden übermittelt werden und staatskritische Äußerungen ausbleiben. Eine weitere mögliche Konsequenz wäre die Verweigerung, sich in der Not Beratungsstellen, Ärzten oder Anwälten anzuvertrauen. Somit wären berufliche Aktivitäten ebenso wie politische und unternehmerische Tätigkeiten, die Vertraulichkeit voraussetzen, beeinträchtigt.

Hinzukommt ein eingeschränkter Nutzen, da sich sämtliche Daten auf die Vergangenheit beziehen und somit keine Verbrechen verhindern können. Die gespeicherten Daten dienen ausschließlich der nachträglichen Aufklärung. Auch an der

[12] Vgl. http://www.uni-muenster.de/Jura.itm/hoeren/Inhalte/lehre/Vorratsdatenspeicherung/ Handout.pdf, Stand 6.11.2009

[13] http://www.bmj.bund.de/media/archive/2956.pdf, Stand 6.11.2009

[14] http://www.vorratsdatenspeicherung.de/content/view/83/87/lang,de/, Stand 7.11.2009

[15] http://www.piratenpartei.de/navigation/politik/Überwachung/vorratsdatenspeicherung/hintergrund, 7.11.2009

Abschreckung muss gezweifelt werden, da die Speicherung mehr als leicht umgangen werden kann. Jeder hat die Möglichkeit, öffentliche Telefonzellen oder Internetcafés zu nutzen. Auch für den privaten Bereich gibt es zahlreiche Möglichkeiten, die es leicht machen, sich der Erfassung zu entziehen - auf diese wird allerdings an späterer Stelle noch genauer eingegangen. Das Hauptanliegen der Befürworter, nämlich Terrorismus und Kriminalität zu verhindern, wäre somit nicht realisierbar, da die Vorratsdatenspeicherung von Kriminellen leicht umgangen werden kann. Ebenfalls wird durch die Überwachung die Entwicklung von Verschleierungstaktiken vorangetrieben, eine mehr als kontraproduktive Folge. Einen weiteren Widerspruch im Zusammenhang mit der Datenspeicherung stellt das Post- und Fernmeldegesetz dar, welches nach Artikel 10 des Grundgesetzes als unverletzlich reglementiert wird. So ist eine Vorratsdatenspeicherung bei Briefen beispielsweise unvorstellbar und praktisch auch nicht umsetzbar.

3.3 Statistiken

96 Prozent der deutschen Haushalte verfügen über einen oder mehrere Telefonanschlüsse. 73 Prozent der deutschen Haushalte haben einen Internetanschluss.[16] Durch die Vorratsdatenspeicherung werden jederzeit über 63 Milliarden Verbindungen gespeichert, wobei jährlich 220.000 Verbindungsdaten abgefragt werden. Jährlich wird das Telekommunikationsverhalten von 28 Millionen Bürgern offengelegt.

Laut der polizeilichen Kriminalstatistik des BKA werden überhaupt nur 0,0004 Prozent der gespeicherten Daten abgefragt.[17] Wobei angebracht werden muss, dass vor Einführung der Vorratsdatenspeicherung den Behörden Daten in unter 0,01 Prozent der Fälle fehlten. 83 Prozent aller erfolgreichen Abfragen bringen kein verfahrensrelevantes Ergebnis.[18] Die Kriminalität ist in den letzten 15 Jahren konstant, trotz immer größerer Eingriffsbefugnisse. Vergleicht man diese Werte mit denen Japans, die keine Überwachung nutzen, sind die Zahlen nahezu identisch. Die Aufklärungsrate der Telekommunikationsstraftaten ist im Zuge der Vorratsdatenspeicherung von 44 auf 54 Prozent gestiegen.

Eine Studie des US-Forschungsinstituts MIT (Massachusetts Institute of Technology) zur Auswertung von Telekommunikations-Verbindungsdaten ergab, dass mit einer Trefferquote von 90 Prozent Kollegen, Bekannte und Freunde aller Personen identifiziert werden können. Ebenfalls mit einer Trefferquote von 90 Prozent konnte vorhergesagt werden, ob sich zwei Personen in den nächsten Stunden treffen werden. Zu guter Letzt gaben die Daten zuverlässig Auskunft über Schlafgewohnheiten und Zufriedenheit am Arbeitsplatz.[19]

3.4 Bedenken

> *„Wer grundlegende Freiheiten aufgibt, um vorübergehend ein wenig Sicherheit zu gewinnen, verdient weder Freiheit noch Sicherheit.“*

[16] http://telekom-news.dsl-flatrate-angebote.de/3264-deutsche-haushalte-73-prozent-haben-einen-internetzugang-davon-82-prozent-breitband-zugang, Stand 14.11.2009

[17] BKA, Polizeiliche Kriminalstatistik 2006, S. 65

[18] http://epp.eurostat.ec.europa.eu/portal/page?pageid=2973,64549069,297,Stand 14.11.2009

[19] http://reality.media.mit.edu/dyads.php, Stand 15.11.2009

Benjamin Franklin (1706 bis 1790)

Setzt man sich mit dem Thema Vorratsdatenspeicherung auseinander, hört oder liest man häufig die Aussage: „Wer nichts zu verbergen hat, hat auch nichts zu befürchten“. Dieser Satz macht den Anschein selbstredend zu sein und soll weitere Erklärungen oder Debatten hinfällig erscheinen lassen. Zusätzlich stellt die Äußerung alle Bürger ohne konkrete Anhaltspunkte unter Generalverdacht. So kommt es, dass innerhalb der Gesellschaft zahlreiche Bedenken und Gefahren gesehen werden, die im Zuge der aufkeimenden Vorratsdatenspeicherung relevant erscheinen. Durch die ständige Weiterentwicklung der elektronischen Datenverarbeitung ist es mittlerweile ein Leichtes, Verbindungsdaten auszuwerten, zu verknüpfen oder zu übermitteln. In den Bundesländern Bayern, Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz und Schleswig Holstein nutzt die Polizei bereits Software, um Daten mit der Antiterrordatei, Vernehmungen und bisherigen Verfahren abzugleichen.

Laut einer Studie des Europäischen Parlaments werden in der EU bereits Andersdenkende, Menschenrechtsaktivisten, Journalisten, Studentenführer, Minderheiten, Gewerkschaftsführer und politischen Gegner überwacht.[20] Die Menschenrechtsorganisation Amnesty International steht beispielsweise unter Überwachung des britischen Geheimdienstes GCHQ.[21] Infolgedessen werden immer mehr Stimmen laut, die vor dem „gläsernen Bürger“ warnen. Diese Bezeichnung steht als Metapher für die als negativ empfundene vollständige Durchleuchtung der Menschen und ihres Verhaltens durch einen überwachenden Staat.[22] Im besonderen Fokus der Kritik steht die Erstellung von Persönlichkeits- und Bewegungsprofilen der gesamten Bevölkerung und damit verbunden der Verlust der Privatsphäre.

Abschreckungen und Hemmungen werden als Folgen genannt. Beispielsweise würden sich Menschen in der Not nicht mehr an Institutionen wenden, die Vertrauen voraussetzen, so die Kritiker. Hemmungen könnten somit beim Kontaktieren von Rechtsanwälten, Beratungsstellen, Geistlichen, Ärzten oder Psychologen auftreten. Passend dazu besagt eine Forsa-Umfrage aus 2008, dass 52 Prozent der Bürger nicht mehr per Telefon, Handy oder Email Kontakt zu Vertrauensstellen aufnehmen würden.[23] Weitere Bedenken existieren bei den Kosten der Vorratsdatenspeicherung, welche zwangsläufig auf den Kunden umgelegt werden. Denn mit Einführung der EU-Richtlinie wurden die Provider zu Staatsdiensten dazu gezwungen die Datenspeicherung durchzuführen ohne im Gegenzug dafür entschädigt zu werden. Dass diese Mehrkosten nun wieder auf dem Kunden abgewälzt werden erscheint als logische Konsequenz.

Hinzu kommt die Möglichkeit unbefugten Zugriffes oder krimineller Nutzung. „Der Bundes-Datenschutzbeauftragte schätzt den Wert eines sechsmonatigen Persön-lichkeitsprofils durch Vorratsdaten auf 100 Euro“.[24] Bei 82 Millionen

[20] Omega Foundation, Report (I)
[21] http://www.heise.de/tp/r4/artikel/6/6280/s2.html, Stand 16.11.2009
[22] http://www.leibniz-institut.de/cms/pdf2/banse/glaeserner/mensch.pdf S.10
[23] http://www.daten-speicherung.de/data/forsa/2008-06-03.pdf
[24] http://mrmcd0x8.metarheinmain.de/fahrplan/attachments/1339/
Zur/Verfassungsmäßigkeit/der/Vorratsdatenspeicherung.pdf

Bürger alleine in Deutschland wird deutlich: Vorratsdaten haben einen Milliardenwert und stellen somit ein lukratives Geschäft für die kriminelle Nutzung dar.

3.5 Verletzungen des Grundgesetzes

Artikel 5 Grundgesetz :

Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

Artikel 10 Europäische Menschenrechtskonvention :

Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Hörfunk-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben.

Artikel 8 Europäische Menschenrechtskonvention :

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

Die Gegner der Vorratsdatenspeicherung sehen mit ihrer Einführung eine Aushebelung geltender Gesetze. Für sie stellt die staatliche Speicherung, Verwendung und Weitergabe von personenbezogenen Daten einen Eingriff dar, der im Widerspruch zum Fernmeldegesetz steht. Das Fernmeldegesetz ist nach Artikel 10 (1) Alt.3 des Grundgesetztes als unverletzlich deklariert und soll die Vertraulichkeit des Inhalts und die näheren Umstände eines Telekommunikationsvorgangs gewährleisten.

Ähnliches gilt für das Recht auf informationelle Selbstbestimmung. Hierbei handelt es sich um ein Datenschutz-Grundrecht, welches im Grundgesetz allerdings nicht ausdrücklich erwähnt wird, jedoch eng mit der Menschenwürde (Artikel 1 I GG) sowie der allgemeinen Handlungsfreiheit (Artikel 2 I GG) in Verbindung steht. Das Recht auf informationelle Selbstbestimmung besagt, dass jeder selbst entscheiden kann, ob er personenbezogene Daten von sich preisgeben möchte und zu welchem Zweck diese verwendet werden dürfen. Als personenbezogene Daten werden grundsätzlich Angaben über eine bestimmte oder bestimmbare Person bezeichnet. Eingriffe entgegen dieses Rechts dürfen allerdings nur erfolgen, wenn die Vorteile „für die Allgemeinheit einen höheren Wert haben als die Nachteile für den Einzelnen“.[25]

Durch die gesetzlich vorgeschriebene Datenspeicherung kommt es nun zum Konflikt mit den bestehenden Gesetzen. Entgegen dem Recht auf informationelle

[25] wiki.vorratsdatenspeicherung.de/images/Praesentation/DavidB.ppt, Stand 6.11.2009

Selbstbestimmung kann der Bürger in Deutschland nun nicht mehr über die Speicherung entscheiden. Bereits erwähnt wurde das Fernmeldegesetz welches durch das Brief- und das Postgeheimnis ergänzt wird. Dieses Recht ist durch Artikel 10 des Grundgesetzes reglementiert und wurde dafür geschaffen, unbefugtes Abhören, Unterdrücken, Verwerten oder Erstellens von Fernmeldebotschaften zu verbieten. Die Vorratsdatenspeicherung widerspricht dem und stellt demnach eine Beeinträchtigung eines Grundrechtes dar.

Der Kreis der Kritiker, welcher größtenteils aus Datenschützern, Verfassungsrechtlern, Parteien und Vertretern verschiedener Berufsgruppen besteht, protestiert seit Längerem gegen diese Beeinträchtigungen. Sie zweifeln an dem Sinn einer solchen Maßnahme, die ohne konkrete Anhaltspunkte durchgeführt wird und die den Weg in Richtung Überwachungsstaat weist.

3.6 Umgehungsmöglichkeiten

Das wohl bekannteste Verschlüsselungsprogramm ist PGP (Pretty Good Privacy), das kryp-tographische Methoden verwendet, um Ihre Email mitlesesicher zu machen. Genutzt wird ein öffentlicher Schlüssel, mit dem jeder die Daten für den Empfänger verschlüsseln kann, und ein privater geheimer Schlüssel, den nur der Empfänger besitzt und der durch ein Kennwort geschützt ist. Nachrichten an einen Empfänger werden mit seinem öffentlichen Schlüssel verschlüsselt und können dann ausschließlich durch den privaten Schlüssel des Empfängers entschlüsselt werden. Diese Verfahren werden auch asymmetrische Verfahren genannt, da Sender und Empfänger zwei unterschiedliche Schlüssel verwenden.

Skype: Skype ist eine kostenlose Software mit Funktionen wie Instantmessaging, Dateiüber-tragung und Videotelefonie, welche alle verschlüsselt ablaufen. Skype-Anrufe werden ver-schlüsselt, denn Skype ist End-to-End-verschlüsselt, da es das öffentliche Internet zur Über-tragung der Anrufe und Textnachrichten verwendet und diese Peer-to-Peer über andere Rechner geleitet werden. Durch die Skype-Verschlüsselung wird sichergestellt, dass keine andere Partei bei einem Anruf mithören oder Sofortnachrichten lesen kann. Skype verwendet den erweiterten Verschlüsselungsstandard (Advanced Encryption Standard ^ AES) der auch von US-Regierungsbehörden verwendet wird, um vertrauliche Informationen zu schützen. Skype setzt eine 2048-Bit-RSA-Verschlüsselng ein, um symmetrische AES auszuhandeln. Die öffentlichen Schlüssel von Benutzern werden vom Skype-Server bei der Anmeldung zertifi-ziert.

I2P: I2P (Invisible Internet Project) ist ein Open-Source-Projekt mit dem Ziel, ein anonymes bzw. pseudonymes VPN (Virtual Private Network) zu schaffen, welches eine einfache Über-tragungsschicht mit dem Nutzen der Anonymität und Sicherheit für Applikationen zur Ver-fügung stellt. Das Netzwerk selbst ist nachrichtenbasiert (wie IP), bietet aber auch eine Bibli-othek an, die Streaming von Daten erlaubt und TCP ähnelt. Die Kommunikation ist an beiden Enden verschlüsselt. Es werden dabei insgesamt vier Schichten zur Verschlüsselung je

Paket verwendet.[26]

Tor: Tor ist ein Netzwerk virtueller Tunnel, das es Einzelpersonen und Gruppen ermöglicht, den Schutz ihrer Privatsphäre und ihre Sicherheit im Internet zu verbessern. Es ermöglicht außerdem Softwareentwicklern, neue Kommunikationswerkzeuge zu entwickeln, bei denen die Privatsphäre bereits eingebaut ist. Tor stellt die Grundlage für eine Reihe von Anwendun-gen zur Verfügung, die es Organisationen und Individuen erlaubt, Informationen über öffent-liche Netze auszutauschen, ohne ihre Privatsphäre zu gefährden. Individuen können mittels andere Webseiten daran hindern, ihren Weg beim Surfen aufzuzeichnen. Weiterhin kann man es dazu verwenden, um eine Verbindung zu Nachrichtenseiten oder Instant-Messaging-Services herzustellen, die vom Internet Provider gesperrt wurden. Die versteckten Services von Tor bieten die Möglichkeit, Webseiten und andere Dienste zu veröffentlichen, ohne den Standort der Seite preiszugeben. Menschen nutzen Tor auch, um sensible Informationen auszutauschen: Chaträume und Webforen für Vergewaltigungsopfer und Überlebende von Misshandlungen oder auch Menschen mit Erkrankungen. Beispiel: Journalisten nutzen Tor, um sicherer mit ihren Informanten zu kommunizieren. Nichtstaatliche Organisationen nutzen Tor, damit ihre Mitarbeiter die Organisations-Webseite aufrufen können, während sie sich im Ausland befinden, ohne preiszugeben, dass sie für diese Organisation arbeiten.[27]

4 Zukunftsaussicht

Verfassungsbeschwerde:

Am 31. Dezember 2007 wurde eine vom Arbeitskreis Vorratsdatenspeicherung begleitete Verfassungsbeschwerde gegen die Vorratsdatenspeicherung beim Bundesverfassungsgericht in Karlsruhe eingereicht. In Verbindung mit der über 150-seitigen Beschwerdeschrift wurde auch beantragt, die Datensammlung wegen „offensichtlicher Verfassungswidrigkeit“ durch eine einstweilige Anordnung sofort auszusetzen.

Erstmals in der Geschichte der Bundesrepublik haben 34.939 Beschwerdeführer einen Rechtsanwalt mit der Erhebung einer Verfassungsbeschwerde beauftragt. Eine separate Verfassungsbeschwerde gegen das Gesetz haben FDP-Politiker rund um Burkhard Hirsch eingereicht.

Am 11. März 2008 hat das Bundesverfassungsgericht auf Antrag der acht Erstbeschwerdeführer das Gesetz zur Massenspeicherung von Telefon- und Internetverbindungsdaten per einstweiliger Anordnung stark eingeschränkt. Zwar wurde die Speicherpflicht für Kommunikationsunternehmen nicht ausgesetzt, die Verwendung der Daten durch Ermittlungsbehörden ist aber nur mit Genehmigung eines Ermittlungsrichters und im Zusammenhang mit schweren Straftaten möglich. Bevor auf die gesammelten Vorratsdaten zugegriffen werden kann, muss ein durch Tatsachen begründeter Verdacht vorliegen, und andere Ermittlungsmöglichkeiten müssen wesentlich erschwert oder aussichtslos sein.

[26] http://de.wikipedia.org/wiki/I2p
[27] http://www.torproject.org/overview.html.de#overview

Am 15. Dezember 2009 wird das Bundesverfassungsgericht eine mündliche Verhandlung über die Verfassungsbeschwerden gegen die Vorratsdatenspeicherung abhalten.

Piratenpartei:

Die Piratenpartei (2006 gegründet) verfolgt das Ziel die Freiheit der einzelnen Bürger zu bewahren und somit hat die Partei auch das Ziel, das Gesetz der Vorratsdatenspeicherung wieder abzuschaffen.

5 Literaturverzeichnis

- c't-Magazin 01/2010 Auf der Kippe - Das Bundesverfassungsgericht verhandelt über die Speicherung von Telefon- und Internet-Nutzerspuren
- c't-Magazin 02/2010 Alltägliche Rasterfahndung - Was die Vorratsdatenspeicherung so gefährlich macht
- c't-Magazin 01/2009 Verordneter Datenwust - Trotz Protesten haben sich fast alle Provider auf die Vorratsdatenspeicherung vorbereitet
- c't-Magazin 02/2010 Kommissar Trojaner ermittelt - Nach zweijährigem Streit haben Bund und Länder das BKA-Gesetz verabschiedet
- http://www.spiegel.de/thema/vorratsdatenspeicherung/
- http://www.vorratsdatenspeicherung.de/
- http://dip.bundestag.de
- http://www.piratenpartei.de/
- http://www.heise.de
- BKA, Polizeiliche Kriminalstatistik 2006
- Breyer, Patrick: Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland (Vorratsspeicherung, traffic data retention). Dissertation. Rhombos Verlag, Berlin 2005, ISBN 3-937231-46-3
- Weißnicht, Elmar: IT Risikomanagement und Online-Überwachung von Arbeitnehmern im Konzern: Telekommunikations- und datenschutzrechtliche Aspekte in Deutschland und im Vereinigten Königreich. Eul-Verlag, 2008, ISBN 978-3-89936-658-7

Webstandards I

Bastian Haug

Zusammenfassung

Meine Hausarbeit zum Thema Webstandards bezieht sich hauptsächlich auf die Barrierefreiheit im Internet. Neben der Barrierefreiheit gehe ich aber auch auf allgemeine Webstandards ein, die bei der Entwicklung von Webinhalten beachtet werden sollten. Dies wird besonders durch Beispiele verdeutlicht. Vertiefend möchte ich Einblick in gesellschaftliche und juristische sowie technische Hintergründe geben und die Auswirkungen darstellen.

1 Einführung

1.1 Definition

Als Webstandards werden die Standards bezeichnet, die bei der Entwicklung von Webinhalten beachtet werden sollten. Diese Standards gelten als Richtlinien und sind im Allgemeinen nicht verpflichtend. Es gibt in Deutschland aber Ausnahmen für Behörden der Bundesverwaltung. Deren Webangebote müssen seit 2006 die Anforderungen der Barrierefreie Informationstechnik-Verordnung (BITV) erfüllen. Privaten und kommerziellen Webseiten-Betreibern steht es frei, sich an die Standards zu halten.

1.2 Vorgeschichte

Anfang der 90er Jahren wurde das World Wide Web bereits von einem kleinen Teil der Bevölkerung genutzt. Die Webangebote waren für jeden zugänglich und jeder konnte selbst an der Gestaltung teilnehmen. Die frühere zeilenorientierte Darstellung in Betriebssystemen wie MS-DOS war für blinde oder gehörlose Menschen nutzbar. Jedoch warf der zunehmende grafische Aufbau von Webinhalten das Problem auf, dass diese Inhalte für Menschen mit Behinderung nicht mehr so einfach zugänglich waren.

Hinzu kommt die hohe Komplexität des Webdesigns. Es gibt viele unterschiedliche Technologien, die eigentlich die Erstellung von Webinhalten einfacher machen. Die Zugänglichkeit leidet jedoch darunter. Vielen Webdesignern fehlt außerdem ein Problembewusstsein für die nötige Barrierefreiheit. Und dass marktführende Browser noch heute keine Standardkonformität aufweisen, zeigt noch mehr den Bedarf von umfassenden Standards.

1.3 Begrifsserklärung

1.3.1 W3C

Das World Wide Web Consortium (W3C) ist eine Gemeinschaft zur Standardisierung der im Web eingesetzten Techniken. Es wurde im Oktober 1994 gegrün-

det und entwickelt seit dem technische Richtlinien[1]. Durch das W3C wurden bereits Techniken wie

- HTML,
- XHTML,
- CSS,
- und RSS

standardisiert. Da das W3C nicht dazu berechtigt ist, ISO-Normen festzulegen, werden die Richtlinien lediglich als Empfehlung bezeichnet. Eine der wichtigsten Standardisierungen, auf die später noch eingegangen wird, ist die WCAG 2.0[1].

1.3.2 HTML

Hypertext Markup Language (HTML), ist eine Auszeichnungssprache, die zur Strukturierung von Webinhalten wie Texte oder Bilder dient. HTML wird vom Browser interpretiert und entsprechend dargestellt. Es ist die Grundlage des Webs und enthält neben Inhalten auch Metainformationen, wie den Autor oder eine Beschreibung, um was es auf der Webseite geht. Aktuell wird HTML in der Version 4.01 verwendet. Version 5 ist zur Zeit in der Entwicklung, wird aber teilweise schon eingesetzt. HTML funktioniert über so genannte Tags. Ein H1-Tag z.B. bezeichnet eine Überschrift der obersten Ordnung. In der Anwendung sieht das wie folgt aus:

⟨h1⟩Überschrift⟨/h1⟩

Ein H1-Tag ist ein umschließendes Tag. Hier muss immer ein End-Tag vorhanden sein. Bei Bildern z.B. verwendet man ein alleinstehendes Tag:

⟨img src=”bild.jpg” alt=”Ein Bild”⟩

1.3.3 CSS

Cascading Style Sheets (CSS) ist eine deklarative Sprache, mit der sich festlegen lässt, wie bestimmte Bereiche einer Webseite dargestellt werden sollen. Folgendes Beispiel soll der Verdeutlichung dienen:

```
h1 {
font-size: 16px;
text-decoration: underline;
}
```

Mit dieser Deklaration wird jedes H1-Tag im entsprechenden HTML Dokument in der Schriftgröße 16 Pixel und unterstrichen angezeigt.

1.3.4 JavaScript

JavaScript ist eine Skriptsprache, die hauptsächlich für Browser eingesetzt wird. Ein häufiges Anwendungsgebiet von JavaScript ist die Validierung von Formularfeldern. So kann relativ einfach überprüft werden, ob es sich um eine korrekte E-Mail-Adresse handelt.

[1] http://www.w3.org/Consortium/

1.3.5 Flash

Flash wird häufig benutzt, um multimediale oder interaktive Inhalte zu erstellen. Diese können dann über den Flash Player, ein Plugin, angezeigt werden. Ein großes Einsatzgebiet von Flash ist bspw. Youtube. Hier werden die Videos über den Flash Player abgespielt. Der Benutzer bekommt davon wenig mit, weil sich das gesamte Verfahren im Browser abspielt.

1.3.6 Plugin

Als Plugin (dt. *Erweiterungsmodul*) bezeichnet man ein Programm, das die Funktionalität einer Software erweitert.

1.3.7 Screenreader

Ein Screenreader (dt. *Bildschirmleseprogramm*) bietet Menschen mit Sehbehinderung eine alternative Benutzerschnittstelle. Anstatt einer grafischen Darstellung liest der Screenreader dem Nutzer die Inhalte vor. Die Ausgabe beschränkt sich dabei nicht nur auf Texte. Sofern ein Bild eine alternative Beschreibung enthält[2], wird auch diese akustisch ausgegeben.

2 Richtlinien

2.1 WCAG 1.0

Die Richtlinien für barrierefreie Webinhalte (engl. *Web Content Accessibility Guidelines*, WCAG)[3] wurden 1999 als eine Empfehlung des World Wide Web Consortium (W3C) veröffentlicht und gelten als Leitfaden für Webdesigner und Browserentwickler. Obwohl diese Richtlinien nicht regelmäßig aktualisiert wurden, galten sie noch bis Ende 2008. Durch sie sollte geregelt werden, dass Webseiten auch von Menschen mit motorischen oder sensorischen Behinderungen ohne Einschränkungen genutzt werden können. Im Allgemeinen bezieht sich das auf Personen, die

- nicht sehen, hören oder sich nur eingeschränkt bewegen könnten.
- Schwierigkeiten beim Lesen oder Verstehen von Texten haben.
- Tastaturen oder Mäuse nicht bedienen können.
- einen Bildschirm haben, der nur Text darstellt oder sehr klein ist, oder eine langsame Internetverbindung haben
- die Sprache des geschriebenen Dokumentes nicht fließend verstehen.
- situationsbedingt ihre Augen oder Ohren nur eingeschränkt nutzen können (bspw. auf dem Weg zur Arbeit oder in einer lauten Umgebung).
- eine Version eines Browsers, einen Screenreader oder ein anderes Betriebssystem haben. [2]

[2] siehe Abschnitt 1.3.2, HTML Beispiel 2 (alt="Ein Bild")
[3] `http://www.w3.org/TR/WCAG10/`

2.2 BITV

Nachdem am 1. Mai 2002 in Deutschland das Behindertengleichstellungsgesetz (BGG) in Kraft trat, haben zwei Monate später das Bundesinnenministerium und das Bundesministerium für Arbeit und Soziales die Barrierefreie Informationstechnik-Verordnung[4] verabschiedet.

Die BITV gibt vor, was eine barrierefreie Internetseite zu erfüllen hat, für wen sie gilt und bis wann die Vorgaben zu erfüllen sind. Die Anforderungen werden in §3 BITV geregelt. Sie basieren inhaltlich auf den WCAG 1.0 und sind in zwei Prioritäten aufgeteilt. Im Folgenden sind die Bedingungen mit der Priorität 1 als Beispiel dienend aufgelistet:[3]

1. Für jeden Audio- oder visuellen Inhalt sind geeignete äquivalente Inhalte bereitzustellen, die den gleichen Zweck oder die gleiche Funktion wie der originäre Inhalt erfüllen.

2. Texte und Graphiken müssen auch dann verständlich sein, wenn sie ohne Farbe betrachtet werden.

3. Markup-Sprachen (insbesondere HTML) und Stylesheets sind entsprechend ihrer Spezifikationen und formalen Definitionen zu verwenden.

4. Sprachliche Besonderheiten wie Wechsel der Sprache oder Abkürzungen sind erkennbar zu machen.

5. Tabellen sind mittels der vorgesehenen Elemente der verwendeten Markup-Sprache zu beschreiben und in der Regel nur zur Darstellung tabellarischer Daten zu verwenden.

6. Internetangebote müssen auch dann nutzbar sein, wenn der verwendete Benutzeragent neuere Technologien nicht unterstützt oder diese deaktiviert sind.

7. Zeitgesteuerte Änderungen des Inhalts müssen durch die Nutzerin/den Nutzer kontrollierbar sein.

8. Die direkte Zugänglichkeit der in Internetangeboten eingebetteten Benutzerschnittstellen ist sicherzustellen.

9. Internetangebote sind so zu gestalten, dass Funktionen unabhängig vom Eingabegerät oder Ausgabegerät nutzbar sind.

10. Die Verwendbarkeit von nicht mehr dem jeweils aktuellen Stand der Technik entsprechenden assistiven Technologien und Browsern ist sicherzustellen, soweit der hiermit verbundene Aufwand nicht unverhältnismäßig ist.

11. Die zur Erstellung des Internetangebots verwendeten Technologien sollen öffentlich zugänglich und vollständig dokumentiert sein, wie z. B. die vom World Wide Web Consortium entwickelten Technologien.

12. Der Nutzerin/dem Nutzer sind Informationen zum Kontext und zur Orientierung bereitzustellen.

[4] `http://bundesrecht.juris.de/bitv/index.html`

13. Navigationsmechanismen sind übersichtlich und schlüssig zu gestalten.

14. Das allgemeine Verständnis der angebotenen Inhalte ist durch angemessene Maßnahmen zu fördern.

Der Geltungsbereich schließt nach §1 BITV alle Internet- und Intranetauftritte ein, die öffentlich zugänglich sind und den Behörden der Bundesverwaltung unterstehen. Für die Behörden der Länder gelten eigene Regeln. Diese orientieren sich jedoch stark an der BITV.

> **§1 Sachlicher Geltungsbereich**
> Die Verordnung gilt für:
>
> 1. Internetauftritte und -angebote,
> 2. Intranetauftritte und -angebote, die öffentlich zugänglich sind, und
> 3. mittels Informationstechnik realisierte grafische Programmoberflächen, die öffentlich zugänglich sind,
>
> der Behörden der Bundesverwaltung.[3]

In §4 BITV wird vorgeschrieben, bis wann die vorgegebenen Standards umzusetzen sind. Demnach mussten die Webangebote bis spätestens zum 31. Dezember 2005 an die BITV angepasst werden.

> **§4 Umsetzungsfristen für die Standards**
> (1) Die in §1 dieser Verordnung genannten Angebote, die nach Inkrafttreten dieser Verordnung neu gestaltet oder in wesentlichen Bestandteilen oder größerem Umfang verändert oder angepasst werden, sind gemäß §3 dieser Verordnung zu erstellen. Mindestens ein Zugangspfad zu den genannten Angeboten soll mit der Freischaltung dieser Angebote die Anforderungen und Bedingungen der Priorität I der Anlage zu dieser Verordnung erfüllen. Spätestens bis zum 31. Dezember 2005 müssen alle Zugangspfade zu den genannten Angeboten die Anforderungen und Bedingungen der Priorität I der Anlage dieser Verordnung erfüllen.
>
> (2) Angebote, die vor Inkrafttreten dieser Verordnung im Internet oder im Intranet (§1 Nr. 2) veröffentlicht wurden, sind bis zum 31. Dezember 2003 gemäß § 3 dieser Verordnung zu gestalten, wenn diese Angebote sich speziell an behinderte Menschen im Sinne des § 3 des Behindertengleichstellungsgesetzes richten.
>
> (3) Soweit nicht Absatz 2 gilt, sind die Angebote, die vor Inkrafttreten dieser Verordnung im Internet oder im Intranet (§1 Nr. 2) veröffentlicht wurden, bis zum 31. Dezember 2005 gemäß §3 dieser Verordnung zu gestalten.[3]

2.3 WCAG 2.0

Die Web Content Accessibility Guidelines 2.0[5] wurden am 11. Dezember 2008 als Weiterentwicklung der WCAG 1.0 verabschiedet. Nach mehr als neunjähriger

[5] `http://www.w3.org/TR/WCAG20/`

Bearbeitung wurden die Standards neu formuliert. Das W3C hatte verschiedene Anforderungen an die neuen Richtlinien. Durch Beispielimplementationen wird es dem Entwickler vereinfacht, die Regeln auch in der Praxis umzusetzen. Außerdem wird dem Entwickler genügend Spielraum für eigene Techniken oder Lösungen gelassen, dadurch dass die zu verwendende Technik nicht vorgeschrieben wird. Hinzu kommen noch Testanweisungen, die beschreiben, wie ein Webangebot auf Zugänglichkeit überprüft wird. Neben der Umsetzbarkeit der Richtlinien sollte auch ein nachgewiesener Nutzen für Menschen mit Behinderung existieren.

Die WCAG 2.0 sind auf vier Prinzipien aufgebaut:

- Wahrnehmbar
- Bedienbar
- Verständlich
- Robust

Unter den Prinzipien gibt es insgesamt zwölf Richtlinien, für welche verschiedene Erfolgskriterien zur Verfügung gestellt werden. Diese Kriterien sind in drei Prioritäten eingestuft werden: A (hoch) AA und AAA(gering).[4]

Ein Beispiel: Richtlinie 1.4 schreibt vor, dass es dem Nutzer leichter gemacht werden soll, Inhalte zu sehen und zu hören einschließlich der Trennung von Vorder- und Hintergrund. Als eines von neun Erfolgskriterien wird die Benutzung von Farben vorgeschlagen. Farben sind ein visuelles Mittel um bspw. Informationen zu vermitteln. In einem Formular, das bestimmte Eingabefelder als benötigt aufweist, könnten diese mit einem Stern gekennzeichnet und zusätzlich rot markiert werden. So ist sichergestellt, dass Nutzer sofort erkennen können, dass es hier etwas gibt, das mehr Aufmerksamkeit benötigt, und Menschen mit einer Sehschwäche bekommen eine Alternative zur farbigen Darstellung. Das erwähnte Erfolgskriterium hat Priorität A und sollte somit in jedem Fall umgesetzt werden.[4]

Ein Abschnitt eine Richtlinie kann wie folgt aussehen:
Guideline 1.1 Text Alternatives: Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.
1.1.1 Non-text Content: All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below. (Level A)

1.2.1 Audio-only and Video-only (Prerecorded): For prerecorded audio-only and prerecorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labeled as such: (Level A)

- **Prerecorded Audio-only:** An alternative for time-based media is provided that presents equivalent information for prerecorded audio-only content.

- **Prerecorded Video-only:** Either an alternative for time-based media or an audio track is provided that presents equivalent information for prerecorded video-only content.

1.2.2 Captions (Prerecorded): Captions are provided for all prerecorded audio content in synchronized media, except when the media is a media alternative for text and is clearly labeled as such. (Level A)

1.2.3 Audio Description or Media Alternative (Prerecorded): An alternative for time-based media or audio description of the prerecorded video content is provided for synchronized media, except when the media is a media alternative for text and is clearly labeled as such. (Level A)

1.2.4 Captions (Live): Captions are provided for all live audio content in synchronized media. (Level AA)

1.2.5 Audio Description (Prerecorded): Audio description is provided for all prerecorded video content in synchronized media. (Level AA)

1.2.6 Sign Language (Prerecorded): Sign language interpretation is provided for all prerecorded audio content in synchronized media. (Level AAA)

1.2.7 Extended Audio Description (Prerecorded): Where pauses in foreground audio are insufficient to allow audio descriptions to convey the sense of the video, extended audio description is provided for all prerecorded video content in synchronized media. (Level AAA)

1.2.8 Media Alternative (Prerecorded): An alternative for time-based media is provided for all prerecorded synchronized media and for all prerecorded video-only media. (Level AAA)

1.2.9 Audio-only (Live): An alternative for time-based media that presents equivalent information for live audio-only content is provided. (Level AAA)

Im Gegensatz zu den WCAG 1.0 beschränken sich die neuen Richtlinien nicht mehr auf nur auf HTML und CSS, sondern beschreiben allgemein, wie Webangebote gestaltet werden müssen, damit sie barrierefrei sind. Welche Technologie für die Umsetzung eingesetzt wird, obliegt dem jeweiligen Entwickler. Dies beugt dem Problem vor, dass die WCAG durch die schnelle Entwicklung des Internets frühzeitig veralten. Auch können neue Techniken problemlos integriert werden.

2.4 Zusammenfassung

Da die BITV inhaltlich auf den WCAG 1.0 basiert, ist sie mittlerweile stark veraltet. Obwohl die WCAG 2.0 bereits Ende 2008 veröffentlicht wurden, wurde die BITV noch nicht angepasst. In §5 BITV ist sogar geregelt, dass die Verordnung regelmäßig überprüft werden soll.

> **§5 Folgenabschätzung**
> Die Verordnung ist unter Berücksichtigung der technischen Entwicklung regelmäßig zu überprüfen. Sie wird spätestens nach Ablauf von drei Jahren nach ihrem Inkrafttreten auf ihre Wirkung überprüft.[3]

Die BITV gilt nun seit fast acht Jahren, ist aber immer noch auf dem Stand von über zehn Jahren, als die WCAG 1.0 veröffentlicht wurden. Abschließend lässt sich zur BITV sagen, dass es für die Barrierefreiheit in Deutschland wünschenswert wäre, wenn die zuständigen Stellen zeitnah eine aktualisierte Version veröffentlichen würden. Eine deutschlandweite Verordnung, die nicht nur für Bundesbehörden sondern auch für alle Landesbehörden verbindlich gilt, würde ein standardkonformes Web zusätzlich fördern.

3 Webstandards

3.1 Qualitätsanforderungen

Bei der Entwicklung von Internetseiten spielen die Bedürfnisse verschiedener Personengruppen eine große Rolle. Jede dieser Gruppen hat unterschiedliche Anforderungen an das fertige Produkt.

3.1.1 Endverbraucher

Der Endverbraucher wünscht sich eine Seite, die leicht zugänglich und bedienbar ist. Außerdem sollte sie sich auch bei einer langsamen Internetverbindung schnell aufbauen.

3.1.2 Seitenbetreiber

Der Seitenbetreiber möchte meist, dass sein Webangebot einmalig ist. Es soll möglichst auf dem aktuellen Stand der Entwicklung sein und sich von der Konkurrenz abheben. Außerdem sollte die Internetseite suchmaschinenoptimiert sein.

3.1.3 Entwickler

Der Entwickler hat das Ziel, dass sein Produkt leicht wartbar ist. Der Code sollte gut kommentiert sein, damit sich später auch andere Entwickler mit der Seite befassen können.

3.1.4 Das Problem

Problematisch wird es, wenn man auf alle Anforderungen Rücksicht nehmen will. Moderne Technologien wie Flash schließen häufig Menschen mit Behinderungen aus, da die Inhalte teilweise nur per Maus zugänglich sind oder von Screenreadern nicht gelesen werden können.

3.2 Prinzipien

Um festzulegen, wie ein Webangebot für alle Personengruppen zugänglich gemacht wird, gibt es die Webstandards. Diese lassen sich, wie in der WCAG 2.0 beschrieben, in vier Prinzipien aufteilen. Im Folgenden sind die Prinzipien kurz erläutert und die Richtlinien aufgelistet.[4]

3.2.1 Wahrnehmbar

Webinhalte müssen mit verschiedenen Ausgabegeräten wahrnehmbar sein. Dies kann erreicht werden, indem man bspw. alternative Texte für Grafiken einbindet. Außerdem sollten Inhalte immer so erstellt werden, dass sie auf verschiedene Arten dargestellt werden können. Auch mit einem einfacherem Layout darf eine Webseite weder Struktur noch Informationsgehalt verlieren.

- Stellen Sie Textalternativen für alle Nicht-Text-Inhalte zur Verfügung, so dass diese in andere vom Benutzer benötigte Formen geändert werden können, wie zum Beispiel Großschrift, Braille, Symbole oder einfachere Sprache.
- Stellen Sie Alternativen für zeitbasierte Medien zur Verfügung.
- Erstellen Sie Inhalte, die auf verschiedene Arten dargestellt werden können (zum Beispiel mit einfacherem Layout), ohne dass Informationen oder Strukturen verloren gehen.
- Machen Sie es für den Benutzer leichter, Inhalte zu sehen und zu hören, einschließlich der Trennung zwischen Vordergrund und Hintergrund.

3.2.2 Bedienbar

Benutzeroberflächen, wie Navigationen, müssen mit verschiedenen Eingabegeräten bedienbar sein. Von höchster Priorität ist hier, dass alle Funktionen auch nur mit der Tastatur nutzbar sind. Dem Nutzer sollten außerdem Möglichkeiten gegeben werden, mit denen er einfacher navigieren oder Inhalte finden kann. Eine Sitemap wäre hier die passende Lösung. Auf ihr werden alle wichtigen Inhalte, meist in alphabetischer Reihenfolge, aufgelistet.

- Sorgen Sie dafür, dass alle Funktionalitäten von der Tastatur aus verfügbar sind.
- Geben Sie den Benutzern ausreichend Zeit, Inhalte zu lesen und zu benutzen.
- Gestalten Sie Inhalte nicht auf Arten, von denen bekannt ist, dass sie zu Anfällen führen.
- Stellen Sie Mittel zur Verfügung, um Benutzer dabei zu unterstützen zu navigieren, Inhalte zu finden und zu bestimmen, wo sie sich befinden.

3.2.3 Verständlich

Informationen und die Funktionen der Benutzeroberfläche müssen verständlich sein. Die Sprache von einzelnen Absätzen oder Wörtern kann separat zur Sprache der Webseite festgelegt werden. Wird dies nicht berücksichtigt, kann der Nutzer im Zweifelsfall nicht unterscheiden, ob es sich um ein deutsches oder englisches Wort handelt, wenn beide gleich geschrieben werden.

- Machen Sie Textinhalte lesbar und verständlich.
- Sorgen Sie dafür, dass Webseiten vorhersehbar aussehen und funktionieren.
- Helfen Sie den Benutzern dabei, Fehler zu vermeiden und zu korrigieren.

3.2.4 Robust

Webinhalte müssen robust genug sein, damit sie durch verschiedene Browser verlässlich dargestellt werden können. Außerdem sollten Entwickler darauf achten, dass Inhalt und Layout stets im Code getrennt werden. So ist es später einfacher, dass Layout zu ändern oder zu überarbeiten.

- Maximieren Sie die Kompatibilität mit aktuellen und zukünftigen Benutzeragenten, einschließlich assistierender Techniken.

3.3 Beispiele

```
<html>
<head>
    <title>Meine Seite - Alter Weg</title>
</head>
<body>
    <font style="font-family:times;color:blue;text-decoration:underline;font-
        size:28px;">Hallo Welt</font><br><br>
    <font face="times" color="red" style="text-decoration:none;font-size:
        18px;">Wie geht es dir?</font>
</body>
</html>
```

Abbildung 1: negatives Beispiel für ein HTML-Dokument

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN"
   "http://www.w3.org/TR/html4/strict.dtd">

<html lang="en">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>Meine Seite - Neuer Weg</title>
    <meta name="generator" content="TextMate http://macromates.com/">
    <meta name="author" content="Bastian">
    <!-- Date: 2009-11-21 -->

    <link rel="stylesheet" type="text/css" href="positiv_beispiel_css.css" />
</head>
<body>
    <h1>Hallo Welt</h1>
    <p>Wie geht es dir?</p>
</body>
</html>
```

Abbildung 2: positives Beispiel für ein HTML-Dokument

Die Beispiele der Abbdildungen 1, 2 und 3 verdeutlichen zwei unterschiedliche Varianten, der Implementierung von HTML und CSS. So zeigt Abbildung 1 ein negatives Beispiel, bei dem die CSS-Befehle direkt im HTML-Dokument eingefügt werden. Der Wartungsaufwand wird dadurch enorm erhöht, weil man für jeden Absatz den entsprechenden Stil neu deklarieren müsste.

```css
body {
    font-family: times;
    color: red;
}

h1 {
    text-decoration: underline;
    font-size: 24px;
    color: blue;
}

p {
    font-size: 18px;
}
```

Abbildung 3: positives Beispiel für ein CSS-Dokument

Abbildung 4: Ergebnis beider Implementationen

Abbdildung 2 und 3 sind miteinander verknüpft und positiv zu bewerten. Hier werden HTML- und CSS-Code strikt getrennt behandelt. Außerdem wird für das übergreifende Body-Tag eine Standardschriftart und -farbe festgelegt. So wird jeder neue Absatz automatisch in Rot dargestellt. Im Gegensatz zu Abbildung 1 sind hier auch Metainformationen, wie über den Autor, enthalten.

Beide Implementationen liefern, wie in Abbildung 4 gezeigt, das gleiche Ergebnis.

3.4 Prüfungen

HTML-Dokumente lassen sich z.B. mit Hilfe des W3C-Validators[6] validieren. Durch die Eingabe einer URL erhält man hier schnell ein entsprechendes Ergebnis. Hierbei ist zu beachten, dass der Validator nicht auf die WCAG 2.0 prüft, sondern ob der Quellcode syntaktisch korrekt ist. Ob die Richtlinien der WCAG 2.0 eingehalten wurden, kann nicht automatisiert geprüft werden. Für einzelne Kriterien gibt es Methoden, andere müssen von Hand geprüft werden. Da die WCAG 2.0 aber ausführliche Prüfverfahren bietet, ist das Prüfen von Hand ohne weitreichende Kenntnisse möglich.

4 Barrierefreiheit

4.1 Behinderungen

Barrierefreiheit für das *World Wide Web* wird aus den gleichen Gründen gefordert, wie auch im öffentlichen Sektor. Bildungseinrichtungen, wie Universitäten, und öffentliche Verkehrsmittel sollen für jeden zugänglich sein. Auch für Menschen, die durch unterschiedliche Behinderungen stark eingeschränkt sind. Diese Behinderungen lassen sich grob in zwei Kategorien eingeteilen: sensorische und motorische Behinderungen.

Zu den sensorischen Behinderungen gehört neben Sehschwächen, wie Rot-Grün-Schwäche oder Blindheit, auch Taubheit. Etwa 9% aller Männer leiden an der Rot-Grün-Schwäche[7]. Durch diesen hohen Anteil wird erst recht deutlich, wie wichtig es sein kann, auf bestimmte Farbgebungen zu achten, um bestimmte Personengruppen nicht einzuschränken. Dass sich Rot oder Grün nicht immer vermeiden lassen, ist verständlich. Gerade weil es sich hier um so genannte Signalfarben handelt, werden sie besonders häufig verwendet. Rot signalisiert bspw. meist einen Fehler oder eine fehlerhafte Eingabe.

Als motorische Behinderungen werden körperliche Einschränkungen bezeichnet. Eine Person, die aus gesundheitlichen Gründen, weder Maus noch Tastatur bedienen kann, muss die Möglichkeit haben Webangebote per Spracheingabe zu bedienen. Zu motorischen Behinderungen kann es unter anderem durch Schädigung des zentralen Nervensystems, wie eine Querschnittslähmung, oder durch Amputationen, wegen Unfallschäden oder Tumoren, kommen[8].

4.2 Barrieren

Zu den häufigsten Barrieren zählen folgende Punkte:

[6] `http://validator.w3.org/`
[7] `http://de.wikipedia.org/wiki/Rot-GrÃijn-SehschwÃďche`
[8] `http://www.behinderung.org/koe.htm`

- Browser- und OS-Version
- Plugins
- Auflösung
- Farben, Kontrast
- verschiedene Geräte

Diese Barrieren haben wenig mit den oben erwähnten Behinderungen zu tun. Sie können viel mehr jeden Benutzer betreffen.

4.2.1 Browser- und OS-Version

In verschiedenen Browsern oder Betriebssystemen werden Internetseiten unterschiedlich dargestellt, da sich nicht alle Entwickler dieser Produkte an die gleichen Standards halten. Abstände zwischen bestimmten Bereichen einer Webseite werden z.B. im Internet Explorer anders dargestellt, als im Firefox. Beachtet ein Webentwickler diese Unterschiede nicht, dass ein Webangebot in bestimmten Betriebssystemen oder Browsern nicht zugänglich ist.

4.2.2 Plugins

Plugins sind, wie bereits beschrieben[9], Erweiterungsmodule für Softwareprodukte. Ohne diese Plugins können teilweise Inhalte, wie Videos, nicht angezeigt werden. Bietet der Seitenbetreiber keine Alternativen, so ist der Benutzer darauf angewiesen, sich zusätzliche Software zu installieren.

4.2.3 Auflösung

Webseiten werden zunehmend für große Bildschirme optimiert. Da aber auch kleine Bildschirme, wie sie bei Netbooks verbaut werden, im Moment im Trend liegen, sind manche Seiten nur beschränkt zugänglich. Dem Benutzer wird dadurch zugemutet, dass er horizontal scrollt, um eine Internetseite im ganzen Umfang wahrnehmen zu können.

4.2.4 Farben, Kontrast

Farbgebung ist besonders wichtig, um dem Nutzer die Wahrnehmung von Inhalten zu erleichtern. Durch falsche Farbgebung kann diese aber auch zusätzlich erschwert werden. Das ist der Fall wenn für den Hintergrund und den Text die Farben so gewählt werden, dass ein geringer Kontrast entsteht.

4.2.5 verschiedene Geräte

Als ein Beispiel ist Flash auf einigen mobilen Geräten, wie dem iPhone, nicht verfügbar. Viele Inhalte werden diesen mobilen Benutzern also verweigert, weil vom Seitenbetreiber nur selten eine alternative Darstellung angeboten wird.

[9] siehe Abschnitt 1.3.6, Plugin

4.3 Vorteile

- kurze Ladezeiten
- Konsistenz
- Reichweite steigt

4.3.1 kurze Ladezeiten

Barrierefreiheit kann den Quellcode einer Seite enorm verschlanken und sorgt somit für geringere Ladezeiten. Außerdem kann die Seite auch ohne Layout geladen werden, ohne an Struktur oder inhaltlichen Informationen zu verlieren.

4.3.2 Konsistenz

Die Qualitätssicherung geschieht automatisch durch Beachtung aller Richtlinien. Webseiten sind systemübergreifend zugänglich und sowohl rückwärts als auch vorwärts kompatibel. Der Pflegeaufwand sinkt durch die Trennung von Layout und Inhalt.

4.3.3 Reichweite steigt

Durch die erfolgreiche Umsetzung von Barrierefreiheit können Webangebote problemlos auf verschiedenen Platzformen oder Browsern dargestellt werden. Es wird als nahezu keine Personengruppe mehr ausgeschlossen.

5 Auswirkungen

5.1 Gesellschaft

Im August 2008 ging man davon aus, dass jeder zwölfte Einwohner der Bundesrepublik Deutschland schwerbehindert ist[10]. Auf Grund der zunehmenden Alterung und des demographischen Wandels, ist davon auszugehen, dass diese Zahl in der Zukunft weiter steigen wird. Da unsere Gesellschaft bereits mit dem World Wide Web lebt und auf dessen Fortbestehen angewiesen ist, dürfen wir es uns nicht erlauben, gewisse Gruppen auszuschließen. Die Gesellschaft, hier besonders die Webentwickler und Seitenbetreiber müssen also Rücksicht auf Menschen mit Behinderungen nehmen, damit diese gleichberechtigt in das digitale Leben integriert werden können. Auch wenn die Wirtschaft dadurch zum Teil höhere Kosten tragen muss, sollte dies ein erstrebenswertes Ziel sein.

5.2 Ökonomie

Aus ökonomischer Sicht, weist eine barrierefreie Entwicklung erhöhte kosten auf. Viele Entwickler müssen erst entsprechend fortgebildet werden, um Techniken zur Barrierefreiheit einsetzen zu können. Auch ist die Umstellung bestehender nicht-standardkonformer Inhalte besonders aufwendig und in wenigen Fällen wirklich lohnend.

[10] http://nullbarriere.de/schwerbehinderung-statistik.htm

Viele Seitenbetreiber wollen außerdem ein besonders modernes und interaktives Design für ihre Webseiten. Meist wird das mit Flash realisiert, was nur bedingt barrierefrei umzusetzen ist.

Literatur

[1] Jeffrey Zeldman. *Designing With Web Standards*. englisch, Mai 2003, ISBN 978-0-7357-1201-0, Seite 136f

[2] World Wide Web Consortium (W3C). *Web Content Accessibility Guidelines (WCAG) 1.0*. Mai 1999, `http://www.w3.org/TR/WCAG10/`

[3] Bundesministerium des Innern. *Barrierefreie Informationstechnik-Verordnung*. Juli 2002, `http://bundesrecht.juris.de/bitv/index.html`

[4] World Wide Web Consortium (W3C). *Web Content Accessibility Guidelines (WCAG) 2.0*. Dezember 2008, `http://www.w3.org/TR/WCAG20/`

[5] *Wikipedia*. `http://de.wikipedia.org/`

Webstandards II

José Stiller

Zusammenfassung

Meine Hausarbeit zum Thema „Webstandards mit Fokus auf Barrierefreiheit“ befasst sich mit der Erläuterung der Webstandards, wie diese sich zusammensetzten und warum diese so Wichtig sind. Dabei gehe ich vertiefend auf die Barrierefreiheit ein.

1 Hintergründe

1.1 Definition

Webstandards sind Spezifikationen von Websprachen, die vom „World Wide Web Consortium“[1] (W3C) erarbeitet bzw. anerkannt wurden. Browserhersteller und Webdesigner halten sich an Standards um nicht aneinander vorbei zu arbeiten. Beide Seiten halten sich an Richtlinien für HTML, Extensible Markup Language27[2] (XHTML), Cascading Stylesheets[3] (CSS) oder sogar JS und weitere Websprachen. Webstandards sind also wie Industriestandards zu verstehen.

1.2 Vorgeschichte

Um auf dieses Thema besser einzugehen, damit Sie verstehen warum die "Webstandards" so wichtig sind, muss ich ein wenig ausholen und etwas über die Entwicklung des Internets erzählen. Ursprünglich wurde das "Internet" in den "Vereinigten Staaten von Amerika" (USA) entwickelt um die damaligen Rechenleistungen zu bündeln und Professoren einen schnellen und einfachen Austausch von Daten zu ermöglichen.

> Nach einem weit verbreiteten Gerücht, habe die USA das Internet damals erfunden um die Kommunikation auch nach einem ATOM-Schlag aufrechterhalten zu können.

So entwarf man Metasprachen wie TEX[4], PostScript[5] und "Standard Generalized Markup Language"[6] (SGML) um die Informationen mit einer Bedeutung auszuzeichnen. Man spricht in diesem Zusammenhang auch von Semantik[7]. Anfänglich bestand das "Internet" nur aus der Vernetzung von Universitäten und Forschungsinstituten der USA. 1989 hatten dann "Tim Berners-Lee"[8] und "Robert Cailliau"[9] die Idee von Verknüpften Informationen über alle Plattformen

[1] http://www.w3c.de
[2] http://de.wikipedia.org/wiki/HTML-1
[3] http://de.wikipedia.org/wiki/Cascading_Style_Sheets
[4] http://de.wikipedia.org/wiki/TeX
[5] http://de.wikipedia.org/wiki/PostScript
[6] http://de.wikipedia.org/wiki/SGML
[7] http://de.wikipedia.org/wiki/Semantik
[8] http://de.wikipedia.org/wiki/Tim_Berners-Lee
[9] http://de.wikipedia.org/wiki/Robert_Cailliau

hinweg. Bis dahin hatte man nämlich immer das Problem, dass manche Informationen nur über einen TEX-Browser, andere aber nur über einen PostScript-Browser und wiederum andere nur mit einem SGML-Browser zugänglich waren. "Tim Berners-Lee" realisierte, dass etwas Einfacheres als diese Metasprachen gebraucht wird, was unter anderem die Idee von verknüpften Informationen unterstützt. So schuf "Tim Berners-Lee" 1990 den ersten Webbrowser namens "WorldWideWeb" später dann "Nexus", was treffend so viel heißt wie "Ursprung". Dieser konnte die neu entwickelte Metasprache "Hyper Text Markup Language"[10] (HTML) interpretieren. Im selben Jahr, 1990, wurde das "Internet" dann von der "National Science Foundation"[11] für Kommerzielle Zwecke freigegeben. Sodass fortan das Internet auch für das Volk zugänglich war. So richtig an Fahrt gewann das Internet aber erst 1993 als der Browser namens "Mosaic" von "Marc Andreessen"[12] und "Eric Bina"[13] veröffentlich und zum freien Download freigegeben wurde. Ab jenem Tag war man nun in der Lage Informationen nicht nur durch Texte sondern auch durch Bilder und Gestalterischen Eigenschaften auszuzeichnen. Nur ein Jahr später, 1994, gründete der Leiter des Entwicklungsteams von dem Browser "Mosaic", "Marc Andreessen", das Unternehmen "Netscape Communications Corporation"[14] die dann den Browser "Navigator" auf den Markt brachten. Ein Jahr darauf, 1995, brachte dann das Unternehmen "Microsoft"[15] (MS), das die Bedeutung des Internets bis dahin unterschätzt hatte, den Browser "Internet Explorer"[16] (IE) raus. Bis heute wurden viele weitere Browser entwickelt und veröffentlich. Unter ihnen Browser wie, "Safari"[17], "Opera"[18], "Chrome"[19] und "Firefox"[20]. Nun muss man sich klar machen, dass Browser nichts anderes sind als Interpretatoren die die ausgezeichneten Informationen interpretieren und darstellen. Was aber wenn die verschiedenen Browser der verschiedenen Unternehmen die ausgezeichneten Informationen nun unterschiedlich interpretieren und daher auch unterschiedlich darstellen? Das ganze wird dann auch noch Exponentiell wenn man bedenkt, dass es jeden Browser auch noch in zahllosen Versionen gibt, auf unterschiedlichen Systemen sowie Geräten, wie Computer und Handys, gibt. Das bedeutet dass man zahllose Problemfälle abdecken muss um sicher zu gehen, dass jeder von Ihnen die Webseite korrekt dargestellt bekommt. Anfänglich führte dies dazu dass nahezu jede Webseite irgendwo vermerkte, dass die jeweilige Webseite nur bei einem bestimmten Browser bei einer bestimmten Auflösung funktioniere. Und hier beginnt das Problem, dass man mit den Webstandards versucht zu beheben.

1.3 Fragestellungen

- Was sind Webstandards?

[10] http://de.wikipedia.org/wiki/HTML
[11] http://de.wikipedia.org/wiki/National_Science_Foundation
[12] http://de.wikipedia.org/wiki/Marc_Andreessen
[13] http://de.wikipedia.org/wiki/Eric_Bina
[14] http://de.wikipedia.org/wiki/Netscape_Communications
[15] http://de.wikipedia.org/wiki/Microsoft
[16] http://de.wikipedia.org/wiki/Internet_Explorer
[17] http://de.wikipedia.org/wiki/Apple_Safari
[18] http://de.wikipedia.org/wiki/Opera
[19] http://de.wikipedia.org/wiki/Google_Chrome
[20] http://de.wikipedia.org/wiki/Firefox

- Wie setzen sich die Webstandards zusammen?
- Was haben die Webstandards für Vorteile?
- Was haben die Webstandards für Nachteile?
- Warum werden die Webstandards nicht eingehalten?
- Warum ist Maintainability wichtig?
- Warum ist die Usability wichtig?
- Warum ist die Accessibility wichtig?

1.4 gewählte Fragestellung

Ich habe mich für die Fragestellungen „Was sind Webstandards?“ und „Wie setzen sich diese zusammen“ mit der Vertiefung „Warum ist die Accessibility wichtig?“ entschieden da diese ein ganz beachtlicher Teil meiner Arbeit ist. Sowohl im Berufsleben als auch bei privaten Projekten. Und da dieser Bereich in Zukunft sicher noch mehr an Bedeutung gewinnt nahm ich an, dass es eine gute Sache sei dies Mal näher zu erläutern.

1.5 Zielsetzung

Ziel ist es, dass der Leser nach dem lesen der Hausarbeit weiß was Webstandards sind und wie sich diese zusammensetzen. Er soll verstehen warum die Webstandards so sind wie sie sind und nicht anders. Weiterhin soll er wissen was Barrieren sind und wie man diese durch Webstandards minimieren kann.

1.6 Aufbau

Ich werde zunächst auf die Entstehungsgeschichte des Internets eingehen damit Ihr nachvollziehen könnt wie sich das heutige Internet entwickelt hat und damit auch die Webstandards. In der Einleitung werde ich bereits deutlich machen was die eigentliche Problematik ist und wozu die Webstandards da sind. Weiterführend werde ich erläutern was Webstandards sind und wie sich diese zusammensetzten, warum diese Wichtig sind und warum Ihr sie einhalten solltet und warum sie nicht eingehalten werden. Schlussendlich geh ich nochmal genauer auf die Barrieren ein und erläutere wie diese aussehen können und wie man diese vermeiden bzw. minimieren kann.

2 Was sind Webstandards?

Webstandards sind meiner Meinung nach der Versuch die Bedürfnisse und damit die Anforderungen an eine Webseite[21], aller Parteien, größtmöglich zu erfüllen.

[21] http://de.wikipedia.org/wiki/Webseite

2.1 Wer stellt Anforderungen an die Webseite?

Anforderungen an die Webseite haben sowohl der Entwickler, der Webseitenbetreiber als auch der Webseitenbesucher. Ich manchen Fällen sind aber der Entwickler und der Webseitenbetreiber ein und dieselbe Person.

2.2 Wie sehen diese Anforderungen aus?

2.2.1 Der Entwickler

Der Entwickler möchte einen qualitativ hochwertigen Quelltext, der leicht wart bar (maintainability[22]) und gut zugänglich (accessibility[23]) ist.

2.2.2 Der Webseitenbesucher

Der Webseitenbesucher möchte eine schnelle Webseite (light weight) haben, die sowohl zugänglich als auch leicht zu bedienen (usability[24]) ist.

2.2.3 Der Webseitenbereiter

Der Webseitenbetreiber möchte eine Webseite haben die in den Suchmaschinen[25] (Search Engine Optimization „SEO“[26]) ganz oben steht. Weiterhin möchte der Webseitenbetreiber natürlich auch eine schnell Webseite haben, die sowohl zugänglich als auch leicht zu bedienen ist. Diese Anforderungen ergeben sich aus den Anforderungen der Webseitenbesucher. Denn die Anforderungen als Webseitenbesucher gilt es als Webseitenbetreiber zu erfüllen. Diese wiederum muss der Entwickler schlussendlich umsetzten.

> Aus diesen Anforderungen ergeben sich allerdings Widersprüche, da die Umsetzung der unterschiedlichen Anforderungen unterschiedliche Lösungswege fordert die der Entwickler aber nicht Gleichmaßen umsetzten kann.

2.3 Die Probleme

Der Entwickler möchte einen qualitativ hochwertigen Quelltext[27] haben. Dazu muss er seinen Quellcode Dokumentieren und formatieren. Beides kostet Zeit. Weiterhin brauch der Entwickler mehr Zeit um den Quelltext so zu konzipieren, dass der Quelltext Modularer bzw. Abstrakter ist damit der Quelltext leichter zu warten ist. Auch brauch der Entwickler schlicht und ergreifend Zeit um das ganze so performant[28] wie möglich zu machen. Dies lässt sich leider nur durch Tests ermöglichen. Dies beides kostet ebenfalls wiederum mehr Zeit. Allerdings ist Zeit bekanntlich Geld wodurch der Webseitenbetreiber abwägt ob sich der qualitativ hochwertige Quelltext im Verhältnis zu den Kosten auszahlt. Weiterhin kostet solch ein Dokumentierter[29] und formatierter Quelltext mehr

[22] http://de.wikipedia.org/wiki/Wartbarkeit
[23] http://de.wikipedia.org/wiki/Accessiblity
[24] http://de.wikipedia.org/wiki/Benutzerfreundlichkeit
[25] http://de.wikipedia.org/wiki/Suchmaschine
[26] http://de.wikipedia.org/wiki/Suchmaschinenoptimierung
[27] http://de.wikipedia.org/wiki/Quelltext
[28] http://de.wikipedia.org/wiki/Leistung_=00002528Informatik=00002529
[29] http://de.wikipedia.org/wiki/Dokumentation

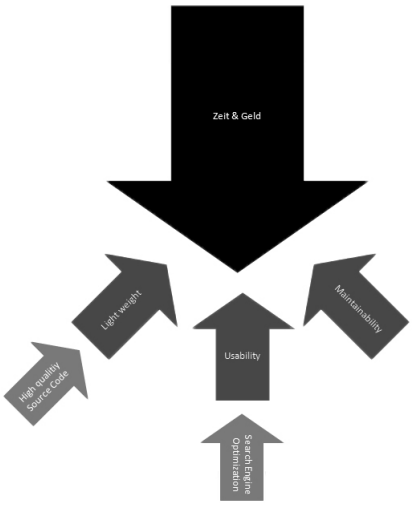


Abbildung 1: Eine abstrakte darstellung der Anforderungskräfte

Speicherplatz, was wiederum zu einer größeren Ladezeit führt. Dies wiederum wiederspricht den Anforderungen des Webseitenbetreibers als auch des Webseitenbesuchers. Der Webseitenbetreiber möchte eine schnelle Webseite haben was wiederum im Gegensatz zu den Anforderungen des Entwicklers als auch gegen sich selbst steht. Denn um eine schnelle Webseite zu konzipieren brauch es Zeit was wiederum Geld kostet. Weiterhin möchte der Webseitenbetreiber eine Webseite die in den Suchmaschinen ganz oben steht, die zugänglich ist und leicht zu bedienen ist. All diese Anforderungen stehen aber im Widerspruch zu sich selbst und damit zu den Anforderungen des Seitenbetreibers und Seitenbesuchers, da man für die Umsetzung für die leichte Benutzbarkeit weitere Technologien wie JavaScript[30] (JS), Extensible Markup Language (XML) [31], Flash[32], Adobe Integrated Runtime (AIR)[33] oder MS Silverlight[34] benötigt. Für diese Technologien brauchen die Browser wiederum Erweiterungen, sogenannte Plug-Ins[35]. Diese müssen wiederum vom Webseitenbesucher installiert werden. Da der Webseitenbesucher im Durchschnitt aber nicht Firm in der Wartung ihres Systems ist weil der Webseitenbesucher Angst hat etwas Falsch und damit kaputt zu machen, wird der Webseitenbesucher nur sehr ungern etwas installieren damit der Webseitenbesucher eine Webseite nutzen kann. Damit ist die Webseite nicht leicht zugänglich. Auch gibt es Webseitenbesucher die im Zuge der Datensammelwut alle Erweiterungen, und damit sind eben diese Plug-Ins gemeint, abschaltet da diese eben erst das ausspähen der Informationen möglich machen. Dadurch ist die Webseite ebenfalls nicht leicht zugänglich. Weiterhin gibt es Webseitenbesucher die in irgendeiner Weise behindert sind. Sei es durch

[30] http://de.wikipedia.org/wiki/JavaScript
[31] http://de.wikipedia.org/wiki/XML
[32] http://de.wikipedia.org/wiki/Adobe_Flash
[33] http://de.wikipedia.org/wiki/Adobe_AIR
[34] http://de.wikipedia.org/wiki/Silverlight
[35] http://de.wikipedia.org/wiki/Plug-in

eine körperliche Behinderung[36] oder durch eine technische Behinderung. Allgemeingefasst nennt man diese Barrieren. Diese Webseitenbesucher benötigen dann unter Umständen Hilfsmittel um eine Webseite wahrnehmen zu können. Was wiederum gesonderte Anforderungen an die Erweiterungen des Browsers stellt, die diese nicht immer erfüllen können. Aber mal davon ausgehend, dass der Webseitenbesucher nicht körperlich behindert ist, die Erweiterungen installiert und aktiviert hat. Gibt es eben noch die unterschiedlichen Browser die den Quelltext unterschiedlich interpretieren und somit unterschiedlich darstellen. Technische Behinderungen. Was zur Folge hat, dass manche Algorithmen in dem einem Browser funktionieren in dem anderem Browser wiederum nicht. Dadurch wiederum muss der Entwickler für jeden Browser der den Quelltext anders interpretiert einen gesonderten Algorithmus entwickeln. Dies wiederum kostet mehr Zeit und damit auch Geld. Weiterhin sind nicht alle Erweiterungen von den Suchmaschinen Lesbar wodurch der Mehrwert den Suchmaschinen verborgen bleibt. Dadurch wiederum erhält die Webseite eine geringere Relevanz was wiederum zu einer schlechteren Platzierung führt. Dies wiederum führt zu einer schlechteren Auffindbarkeit durch Suchmaschinen was zu Folge hat, dass man weniger Webseitenbesucher hat. Dadurch verdient man wiederum weniger Geld durch Werbeeinahmen.

> Aus all diesen Anforderungen und den Problemen die sie mit sich bringen haben sich bestimmte Arbeitsweisen, sogenannte Workflows, durchgesetzt. Diese Workflows wiederum beschreiben das was wir Webstandards nennen.

2.4 Warum solltet Ihr Webstandards einhalten?

Einfach ausgedrückt, weil es nur so richtig und gut ist. Denn wenn Ihr eine Webseite betreibt und gestaltet, hat das auch seine Gründe. So veröffentlicht Ihr etwas weil Ihr damit etwas der Welt mitteilen möchtet. Dies Impliziert, dass das mitgeteilte auch gehört bzw. vielmehr gelesen werden soll. Aber wer liest schon einen unformatierten Text? Also liegt es auch auf der Hand, dass Ihr versucht eure Mitteilung zu strukturieren und zu gestalten sodass man allein beim Betrachten der Mitteilung Lust bekommt das geschriebene auch zu lesen. Dadurch dass Ihr euer geschriebenes strukturieren und gestalten habt Ihr aber das Problem, dass nicht jeder die Webseite so dargestellt bekommt wie Ihr es vielleicht bei euch Zuhause, auf eurem Computer mit eurem Browser der Wahl dargestellt bekommt. Um dieses Problem zu minimieren solltet Ihr euch an die Webstandards halten.

2.5 Was sind die Vorteile?

Offen Grundig liegt der Vorteil zunächst mal nur in der korrekten Darstellung der Webseite. Dies hat allerdings zur Folge, dass die Wahrscheinlichkeit, dass der Webseitenbesucher die Webseite positiv in Erinnerung behält, um ein vielfaches steigt. Dadurch, dass der Webseitenbesucher die Seite positiv in Erinnerung behält, besucht der Webseitenbesucher die Webseite gerne wieder. Hierdurch steigert Ihr bereits die Nachhaltigkeit der Webseite. Weiterhin wird ein Webseitenbesucher, der eine Seite positiv in Erinnerung behält, die Seite auch gerne

[36] http://de.wikipedia.org/wiki/K=000025C3=000025B6rperbehinderung

weiterempfehlen. Dies wiederum führt zu mehr einzigartigen Webseitenbesuchern, sogenannte „Uniqueusern“. Wodurch wir zusätzlich zu unserem bereits vorhandenen Webseitenbesucherstamm weitere Webseitenbesucher akquirieren. Dadurch dass wir mehr Webseitenbesucher auf der Webseite haben, steigt wiederum die Anzahl der Klicks. Was wiederum mehr Geld bedeutet. Denn je mehr Webseitenbesucher eine Seite hat desto mehr Geld bekommt diese Webseite für die Werbung. Weiterhin bekommt eine gut besuchte Webseite mehr Geld pro Klick für die Werbung als eine schlecht besuchte Webseite. Dies liegt daran, dass eine gut besuchte Webseite mehr Aufmerksamkeit bekommt als eine Schlecht besuchte Webseite. Dadurch wollen wiederum viele Leute auf der gut besuchten Webseite ihre Werbung schalten wodurch wiederum der Meistbietende den Zuschlag für die Werbefläche erhält. Weiterhin steigt unsere Webseite bei den Suchmaschinen in der Platzierung, dem sogenannten Ranking. Was wiederum zu weiteren Uniqueusern führt. Auch bekommen wir mehr Aufmerksamkeit, was sich im Ranking wiederspiegelt, wodurch unser Wort im Internet allgemein mehr Anklang findet. Und bei all diesen Folgerungen habe ich zu Beginn Unterschlagen, das wir uns durch das Einhalten der Webstandards auch sozialer geben, da wir dadurch auch all die Menschen berücksichtigen die in irgendeiner Weise Behindert sind. Nicht nur körperlich sondern auch Technisch. Denn mal davon abgesehen, dass es eben Blinde, Schwerhörige Menschen, oder Menschen mit Motorischen Behinderungen gibt. Gibt es eben auch jene die über keine funktionierende Maus verfügen. Oder eben nur über ein Touchscreen da sie über das Handy ins Internet gehen. Oder über einen veralteten Browser weil Sie ihr System nicht warten und entsprechend updaten. Was wahrscheinlich daran liegt, dass diese Menschen nicht ganz so Firm in den neuen Technologien sind und Angst haben etwas Falsch bzw. Kaputt zu machen.

> Zusammengefasst kann man sagen, dass die Wahrscheinlichkeit steigt, dass Webseitenbesucher die Seite positiv in Errinerung behalten wodurch die Seiten mehr Webseitenbesucher erhält und somit mehr Geld verdient.

2.6 Warum werden Webstandards nicht eingehalten?

Begründungen hierfür hört man viele. Im Grunde genommen liegt es aber an genau zwei Dingen. Zum einen der Zeit und zum anderem dem Geld. Denn wie ich bereits anfänglich erklärte, benötigt es für die Umsetzung einer solchen Webseite fundiertes Fachwissen. Weiterhin benötigt die Umsetzung der Webseite auch viel Zeit. Aber sowohl der Entwickler als solches mit seinem Fachwissen kostet viel Geld als auch die Zeit die er benötigt um dies Fachwissen einzusetzen um die Webseite entsprechend umzusetzen. Dies könnte sich ändern wenn alle Browserhersteller die Webstandards einhalten und die Webseitenbesucher ihr System regelmäßig warten. Denn dadurch müssten die Entwickler weniger potentielle Problemfälle berücksichtigen.

> In einem ähnlichen Zusammenhang hat man vor kurzem in den Nachrichten lesen können, dass Große Webseitenbetreiber wie Google[37] oder Amazon den Internet Explorer der Version 6 (IE6) nicht

[37] http://www.golem.de/showhigh2.php?file=00003D/1002/73354.htmlwort =00003DInternetwort[]=00003DExplorer

mehr unterstützen werden. Dies hängt mit Verhältnis zwischen kosten und Nutzen zusammen. Inzwischen gibt es nicht mehr so viele IE6 Nutzer wodurch man die Mehrkosten die man durch die Berücksichtigung des Browsers hat nicht mehr rechtfertigen kann. Sicher gehen dadurch den Webseitenbetreibern einige Webseitenbesucher verloren. Allerdings fällt das durch die geringe Anzahl an Nutzern nicht mehr ins Gewicht, da die Einnahmen durch diese Nutzer ungleich der Kosten für diese Nutzer sind.

3 Barrierefreiheit

Wie Anfangs bereits erwähnt wollen wir einen Fokus auf die Barrierefreiheit[38] legen. Was genau ist aber damit gemeint? Um auf einen Begriff zurückzugreifen den wir bereits verwendet haben – accessibility. Gemeint ist damit die Zugänglichkeit zur Webseite. Also wie gut man die Seite benutzen kann trotz evtl. Barrieren.

3.1 Wie sehen die Barrieren aus?

Diese Barrieren würde ich in zwei größere Gruppen unterteilen. Zum einen die Barrieren die aus einer körperlichen Behinderung eines Webseitenbesuchers resultieren und zum anderem die Barrieren die aus einer technischen Behinderung resultieren.

3.1.1 Körperliche Barrieren

- **Beeinträchtigung des Sehvermögens** – Das Sehvermögen wird benötigt um die Webseite zu sehen um zum Beispiel Texte zu lesen oder Bilder zu betrachten. Man versucht diesen Webseitenbesuchern trotz des beeinträchtigten Sehvermögens durch sogenannte Screen Reader zu helfen. Diese Lesen dem Webseitenbesucher dann vor was auf der Seite steht. Aus diesem Grund ist es auch wichtig die Seite Semantisch korrekt auszuzeichnen sodass der Screen Reader selbst weiß wo er sich gerade im Kontext der Webseite befindet. Also ob er gerade in der Navigation, in der Suche, in dem Artikel, in den Kommentare oder woanders befindet. Das macht es dem Webseitenbesucher ungemein einfacher sich durch die Seite zu bewegen und schnell und einfach das zu finden was der Webseitenbesucher sucht.

- **Beeinträchtigung des Hörvermögens** – Das Hörvermögen wird benötig auf Seiten die viele Multimediale Objekte verwenden. Also Musik oder Videos. Eben all die Objekte bei denen das Hörvermögen eine entscheidende Rolle spielt um den Inhalt zu verstehen. Hier kann man versuchen einen Ausgleich zu schaffen indem man den Inhalt, der durch die Musik oder das Video vermittelt wird, in schriftlicher Form zusammenzufassen.

- **Beeinträchtigung der Motorig** – Die Motorig wird benötigt um durch die Webseite navigieren zu können. Denn die Maus, oder die Tasten der

[38] http://de.wikipedia.org/wiki/Barrierefreies_Internet

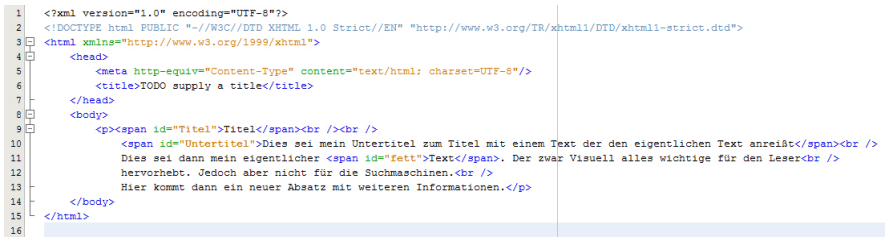
Tastatur bewegen sich nicht von alleine. In diesem Fall sollte der Entwickler einfach dafür sorgen, dass der Webseitenbesucher sowohl mit der Maus als auch mit der Tastatur durch die Webseite navigieren kann.

3.1.2 Technische Barrieren

- **Das Geräte** – Damit ist das Geräte gemeint mit der Webseitenbesucher durch das Internet navigiert. Das könnte zum Beispiel der Computer, der Laptop, das Tablet, das Handy oder das Smartphone sein. * Das Betriebssystem Damit ist das Betriebssystem gemeint. Auch Operating System (OS) genannt. Das könnte zum Beispiel MS Windows 3.11, MS Windows 95, MS Windows 98, MS Windows ME, MS Windows 2000, MS Windows XP, MS Windows Vista, MS Windows 7 sein. Oder aber auch Linux mit all seinen Distributionen wie Ubunto, Open SUSE, Knoppix, Fedora, Debian oder neuerdings Androide. Oder aber Mac OS mit all seinen Versionen.
- **Die Anzahl der Farben** – Damit ist die Anzahl der Farben gemeint. Denn diese reichen von 2 Farben zu 16 Farben zu 256 Farben über 8bit Farben zu 16bit Farben bis hin zu 32bit Farben. Je mehr Farben zur Verfügung stehen desto komplexere Bilder kann man darstellen wie zum Beispiel Fotos oder Videos.
- **Die Auflösung** – Damit ist der Bildschirmausschnitt gemeint. Denn solch ein Handy hat sicher nicht so viel Platz zum Darstellen einer Webseite wie der 26 Zoll Bildschirm zuhause. Zur besseren Vorstellung kann man hier die Fernseher als Beispiel nehmen. Damals hatten diese lediglich die unbunten Farben Schwarz und Weiß bzw. die Graustufen die sich aus diesen Bilden lassen zur Verfügung. Dann kam der Farbfernseher mit einer Auflösung von 853 mal 460. Und der neue HD-Fernseher mit einer Auflösung von 1920 mal 1080 hat zwar nicht mehr Farben als der alte aber dafür eine größere Fläche auf der er den die Bildinformationen darstellen kann wodurch ihm mehr Platz für Details bleiben.
- **Der Browser** – Damit ist der Interpreter der Webseiten gemeint der die Webseiten interpretiert und darstellt. Das könnten der Internet Explorer, der Firefox, der Safari, der Crome, der Opera oder weitere Browser sein. Nicht zu vergessen, dass es jeden dieser Browser in unzähligen Versionen gibt.
- **Die Plug-Ins** – Damit sind die Erweiterungen der Browsers gemeint. Das könnte Flash sein, AIR, Silverlight, Quick Time und unzählige weitere Java-Plug-Ins.
- **Der Quelltext** – Damit ist die Quelltextqualität gemeint. Denn wer unsauber Programmiert, provoziert Fehldarstellungen in Browsern.

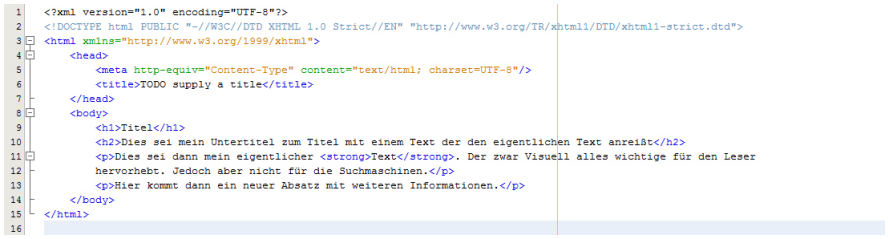
3.2 Was ist Semantik und warum ist Semantik wichtig?

Semantik beschreibt die Bedeutung von etwas im Kontext. Ich versuche das Anhand eines Beispiels zu verdeutlichen. Wenn ich einen Inhalt habe, beispielsweise einen Text, dann kann ich bestimmte Elemente dieses Textes durch Überschriften, Fettungen, Unterstreichungen oder anderen Wahrnehmbaren Eigenschaften



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
        <title>TODO supply a title</title>
    </head>
    <body>
        <p><span id="Titel">Titel</span><br /><br />
            <span id="Untertitel">Dies sei mein Untertitel zum Titel mit einem Text der den eigentlichen Text anreißt</span><br />
            Dies sei dann mein eigentlicher <span id="fett">Text</span>. Der zwar Visuell alles wichtige für den Leser<br />
            hervorhebt. Jedoch aber nicht für die Suchmaschinen.<br />
            Hier kommt dann ein neuer Absatz mit weiteren Informationen.</p>
    </body>
</html>
```

Abbildung 2: Zusehen ist ein (X)HTML-Quelltext der Semantisch nicht korrekt ist



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
        <title>TODO supply a title</title>
    </head>
    <body>
        <h1>Titel</h1>
        <h2>Dies sei mein Untertitel zum Titel mit einem Text der den eigentlichen Text anreißt</h2>
        <p>Dies sei dann mein eigentlicher <strong>Text</strong>. Der zwar Visuell alles wichtige für den Leser
        hervorhebt. Jedoch aber nicht für die Suchmaschinen.</p>
        <p>Hier kommt dann ein neuer Absatz mit weiteren Informationen.</p>
    </body>
</html>
```

Abbildung 3: Zusehen ist ein (X)HTML-Quelltext der Semantisch korrekt ist

hervorheben und somit den Text strukturieren. Bei der Semantik geht es aber auch um die Technische Auszeichnung dieser Elemente. Das hat den Vorteil, dass Suchmaschinen diesen Text besser lesen und auswerten können. Dies wiederum hat zur Folge, dass die Webseite besser indexiert werden kann wodurch der Inhalt besser gefunden werden kann. Weiterhin wird dem Inhalt höchstwahrscheinlich eine höhere Bedeutung beigemessen wodurch er in der Platzierung sicher weiter Oben anzufinden ist. Weiterhin hilft es den sogenannten Screen Reader, die als Hilfsmittel für Webseitenbesucher zum Einsatz kommen die unter einer Beeinträchtigung ihres Sehvermögens leiden. Wo liegt aber nun der Unterschied genau? Der Unterschied liegt in der Art wie die Elemente ausgezeichnet werden. In der Abb. 3 wird der Titel mit einem „span-tag“ ausgezeichnet. Ein „span-tag“ hat in HTML oder (X)HTML keine größere Bedeutung. Meistens verwendet man diesen „tag“ um Elemente zu makieren um sie dann später via CSS zu selektieren und zu stylen. In der Abb. 4 wird der Titel aber als Titel der ersten Ordnung ausgezeichnet. Als Headline – Überschrift. Damit haben wir es ebenfalls geschafft das gewünschte Element zu makieren und darüber hinaus mit einer Bedeutung auszuzeichnen.

Literatur

[1] Wikipedia: Internet `http://de.wikipedia.org/wiki/Internet`

[2] World Wide Web Consortium (W3C) `http://www.w3.org/MarkUp/historical`

[3] Wikipedia: Browser `http://de.wikipedia.org/wiki/Browser`

[4] Stefan Walter http://www.hessendscher.de/benefits/index.htm

[5] Martin Labuschin
http://www.labuschin.com/journal/was-sind-webstandards

[6] 42 Blue http://42blue.de/webstandards/index.php?id=5

[7] Lingo4u http://www.lingo4u.de/article/checklist

[8] Vorsprung durch Webstandards
http://www.vorsprungdurchwebstandards.de/usability\
_webstandards_und_barrieredreies_internet.html

[9] Eric Eggert
http://www.yatil.de/artikel/zugaenglichkeit-mythen-
und-falsche-vorstellungen

[10] David Maciejewski http://www.macx.de/essays/barrierefrei/

[11] Technikwürze http://www.technikwuerze.de

[12] Webkrauts http://www.webkrauts.de

[13] A List Apart http://www.alistapart.com/articles/journey/

Informatik und Medizin

Julian Kalinowski, Florian von Stosch und Broder Fredrich

Zusammenfassung

Seit es die Informatik gibt, wird sie auch in der Medizin eingesetzt. Sei es in der Verwaltung, Forschung, Behandlung oder zur Kommunikation — der heutige Stand der Medizin wäre ohne Informationstechnologie nicht möglich. Die großen Patientenkapazitäten in Krankenhäusern können nur durch die effektiven Speicherungsmöglichkeiten moderner Computer erreicht werden und auch viele Diagnosesysteme, wie die Computertomographie, sind von Informatikern entwickelt.

Doch dieser Trend ist noch nicht abgeschlossen. Immer mehr deutsche Hochschulen — mittlerweile über 40 — bieten entsprechende Studiengänge und Vertiefungsmöglichkeiten an. Unabhängig vom konkreten Einsatzzweck ergeben sich nicht nur neue Möglichkeiten in der Medizin, sondern in gleichem Maße auch neue Problemstellungen und Anforderungen.

„Nicht nur die Reformen im Gesundheitswesen werden für eine steigende Nachfrage nach Medizinischen Informatikern sorgen“, sagt Carl Dujat, Präsident des Berufsverbands Medizinischer Informatiker (BVMI) in Heidelberg. „Auch weitere innovative Entwicklungen, wie die Einführung der Gesundheitskarte, werden zunehmenden Bedarf an Informatikern mit medizinischen Kenntnissen schaffen.“

Im Rahmen dieser Arbeit betrachten wir qualitative, ethische und datenschutzrechtliche Aspekte der Informatik in der Medizin.

1 Geschichte

Auch wenn Computer erst relativ spät in der Medizin eingesetzt wurden, gab es schon früher viele Entwicklungen, die dazu führten, dass nach der Erfindung des Computers dieser auch schnell effizient in der Medizin einsetzbar war.

Wichtig beim Speichern und Abrufen von Patientenakten in einer großen Datenbank ist eine eindeutige *Identifikation*. Während anfangs die Patientenakten noch nach Namen sortiert waren, entwickelte sich mit der Zeit, auch aufgrund immer größerer Kapazitäten, die Fall- , sowie die Identifikationsnummer, die jedem Fall bzw. jedem Patienten eine eindeutige Nummer zuweist. Im Gegensatz zur heute gängigen Praxis, an die Patienten fortlaufende Nummern zu vergeben, wurde früher versucht, die Nummer aus den erfassten Daten des Patienten, wie Geburtsdatum und Nachname, zu generieren. Dies hat jedoch teilweise zu Problemen geführt, denn wenn eins der benutzten Daten korrigiert wurde, musste auch immer die Identifikationsnummer geändert werden, was zur Verletzung der Objektidentität führte. Ähnliches gilt für die Fallnummer, bei der vor allem wichtig ist, das man keine Rückschlüsse auf das Jahr der Aufnahme oder die aufnehmende Fachabteilung ziehen kann.

Ein wichtiger Aspekt in diesem Fall ist die *Dokumentation*, also die Art, wie die medizinischen Informationen über einen Patienten abgespeichert werden.
Erstmalig wurde Anfang des 16. Jahrhunderts auf Anweisung von Heinrich VIII im St. Bartholomäus-Krankenhaus in London eine Abteilung geschaffen, die dafür zuständig war, Krankengeschichten zu dokumentieren. Zur gleichen Zeit gab es auch erste Anfänge in Deutschland. 1526 legte der Nürnberger Stadtarzt Johannes Magenbuch eine Krankenblattdatei an, sortiert nach Nachnamen mit einem ersten Versuch der Standardisierung. Diese wurde im 17. und 18. Jahrhundert immer weiter vorangetrieben, verbessert und verfeinert. Ende des 18. Jahrhunderts entdeckten Wiener Ärzte die übergeordnete Bedeutung einer guten Krankenbeschreibung. Dazu ein Zitat von Maximilian Stoll, Leiters der Wiener Medizinischen Klinik:
„Wenn man nämlich mehrere Krankengeschichten ein und derselben Krankheit beisammen hat und sie miteinander verglichen hat, kann man Richtlinien für die Praxis ableiten und Lehrsätze aufstellen."
Dies verdeutlicht, dass diese Art des Denkens als Ausgangsbasis für eine maschinelle Verarbeitung der Krankengeschichten herangezogen werden kann. Vor allem aber zeigt es, dass damals schon über 'Leitlinien' nachgedacht wurde. Parallel zu der immer besser werdenden Krankendokumentation entwickelte sich der *Klassifikationsschlüssel*. Hierbei wird jeder Krankheit die für sie typischen Symptome zugeordnet.
Einer der wichtigsten Schritte bei der Erstellung eines ausführlichen Krankheitsschlüssels war die Entwicklung der *Internationalen statistischen Klassifikation der Krankheiten und verwandter Gesundheitsprobleme* (kurz ICD). Grundlage dafür war die 1893 von Jacques Bertillon erarbeitete Bertillon-Klassifikation, einer Todesursachenklassifikation.
Nach und nach wurde das Klassifikationssystem von der WHO immer weiterentwickelt und vervollständigt, da durch die vielen Fortschritte in der Medizin Änderungen und Ergänzungen unabgänglich waren. Die derzeit gültige Ausgabe ist die ICD-10, die von 1983-1992 entwickelt wurde und folgende Kapitel enthält:

Einsatzgebiet sind unter anderem die Behandlung von Patienten mit akuten Schmerzen, bei denen häufig die Angabe von Grund- und Begleiterkrankungen zur Ursachenfindung genügt. Es besteht also die Möglichkeit z.B. im Internet Fragebögen bezüglich der Beschwerden auszufüllen, die dann von einer Software ausgewertet werden und einem anschließend eine Liste der möglichen Krankheiten präsentiert.
Diese bieten eine kostengünstige Alternative zum Arztbesuch. Inwiefern sie auf ähnlich gute Ergebnisse kommt wie ein behandelnder Arzt, bleibt dahingestellt.

Eine andere kostengünstige Methode ist das Stellen von gesundheitlichen Fragen im Internet z.B. in medizinischen Foren. Problem hierbei ist, dass man den Verfasser der Antworten nicht kennt. Es mag sein, dass dort auch Ärzte mit Approbation Ratschläge erteilen, oftmals handelt es sich aber um absolute Laien, weswegen man bei größeren Problemen nicht darauf vertrauen sollte.
Hierzu hat auch Stiftung Warentest die in Deutschland am häufigsten genutzten Expertenforen unter die Lupe genommen **(Abbildung 2)**. Sie ist zu dem Ergebnis gekommen, dass die Ergebnisse im Großen und Ganzen schon eini-

Kapitel	Gliederung	Titel
I	A00-B99	Bestimmte infektiöse und parasitäre Krankheiten
II	C00-D48	Neubildungen
III	D50-D90	Krankheiten des Blutes und der blutbildenden Organe sowie bestimmte Störungen mit Beteiligung des Immunsystems
IV	E00-E90	Endokrine, Ernährungs- und Stoffwechselkrankheiten
V	F00-F99	Psychische und Verhaltensstörungen
VI	G00-G99	Krankheiten des Nervensystems
VII	H00-H59	Krankheiten des Auges und der Augenanhangsgebilde
VIII	H60-H95	Krankheiten des Ohres und des Warzenfortsatzes
IX	I00-I99	Krankheiten des Kreislaufsystems
X	J00-J99	Krankheiten des Atmungssystems
XI	K00-K93	Krankheiten des Verdauungssystems
XII	L00-L99	Krankheiten der Haut und der Unterhaut
XIII	M00-M99	Krankheiten des Muskel-Skelett-Systems und des Bindegewebes
XIV	N00-N99	Krankheiten des Urogenitalsystems
XV	O00-O99	Schwangerschaft, Geburt und Wochenbett
XVI	P00-P96	Bestimmte Zustände, die ihren Ursprung in der Perinatalperiode haben
XVII	Q00-Q99	Angeborene Fehlbildungen, Deformitäten und Chromosomenanomalien
XVIII	R00-R99	Symptome und abnorme klinische und Laborbefunde, die anderenorts nicht klassifiziert sind
XIX	S00-T98	Verletzungen, Vergiftungen und bestimmte andere Folgen äußerer Ursachen

Abbildung 1: Internationale statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme, German Modification, Version 2010 [ICD]

ge allgemeine Rückschlüsse zulassen. Allerdings ist die Qualität der Antworten schwankend, von sehr gut bis sehr schlecht. Das hat zur Folge, dass der Ratsuchende im Einzelfall mit gesundheitlichen Schäden rechnen muss, wenn er den Auskünften immer vertraut. Eine medizinische Internet-Beratung kann dennoch in einigen Fällen sinnvoll sein, etwa um sich auf einen Arztbesuch vorzubereiten, eine zweite Meinung einzuholen, komplizierte Zusammenhänge zu verstehen oder auch um eventuell peinliche Themen anonymisiert anzusprechen.

Ein verhältnismäßig neuer Entwicklungszweig ist die *Medizinisch-technische Informatik*. Sie betrifft alles, was Körpersignale oder Körpervolumina betrifft. Darunter fallen unter anderem EEG sowie EKG, aber z.B. auch die Strahlentherapieplanung. Das EKG dient der Registrierung der Summe der elektrischen Aktivitäten aller Herzmuskelfasern. Durch Experimente an Taubenherzen erkannte Carlo Matteucci 1843 erstmals, dass die Herztätigkeit auf elektrischen Vorgängen beruht. Das erste EKG wurde 1882 von Augustus Desiré Waller an seinem Hund durchgeführt und 1887 die ersten Herzströme mittels eines Kapillarelektrometers aufgezeichnet. Die Instrumente wurden immer weiter verbessert, bis es zu einem brauchbaren Diagnoseverfahren entwickelt und schließlich auch in Kliniken eingeführt wurde.
Die Funktionsweise des EEGs ist ähnlich dem des EKGs, nur das anstatt der Herzströme die Gehirnströme gemessen werden. Ein anderer sehr früher Anwendungsbereich von Computern war die Strahlentherapieplanung. Sie dient der Vorbereitung auf die Strahlentherapie. Ihr Ziel ist es, die Strahlungsintensität der individuellen Körpergeometrie so anzupassen, dass die hohen Dosen möglichst nur im bösartigen Geschwulst realisiert werden, während das umliegende gesunde Gewebe so weit wie möglich geschont werden soll. **Abbildung 3** zeigt beispielhaft wie so ein Bestrahlungsplan bei einer Brustkrebsbehandlung heutzutage aussehen kann.

Durch immer leistungsstärkere Computer konnten diese irgendwann auch zur *Bildverarbeitung* eingesetzt werden, die besondere Ansprüche an die Gra-

Anbieter		Deutsches Medizin Forum	Focus	Gesundheitsberatung	Lifeline	Medicine-Worldwide	Qualimedic
Webadresse www.		medizin-forum.de	focus.de	gesundheitsberatung.de	lifeline.de	m-ww.de	qualimedic.de
Anzahl der Foren / davon durch Experten betreut		74/47	1/1	10/10	44/22	14/7	100/25
Erstanmeldung		Nicht erforderlich	Einfach	Aufwendig	Nicht erforderlich	Nicht erforderlich	Aufwendig
Geforderte Personaldaten		Nickname	Nickname, E-Mail	Name, Anschrift, E-Mail, Alter, Telefon	Nickname	Nickname	Name, Anschrift, E-Mail, Telefon
test-KOMMENTAR	Foren	Sehr viele Foren, überwiegend betreut, zu zahlreichen speziellen Themen	Ein Sammelforum für alle Themen	Foren für wenige spezielle Themen, alle betreut, kein Forum für Allgemeinmedizin / Hausarzt	Viele Foren, die Hälfte davon betreut, für viele Themen	Foren zu wenigen Themen, nur einige betreut, kein Forum für Allgemeinmedizin	Sehr viele Foren für zahlreiche Themen, ein Viertel davon betreut, vor allem zu Schwangerschaft, Geburt und Kindern
	Antworten	nur auf die Hälfte der Anfragen reagiert, diese aber richtig beantwortet; bestes Ergebnis in der Richtigkeit bei schlechtestem Antwortverhalten	alle Anfragen beantwortet: nur eine richtig	auf alle vier Anfragen reagiert, nur drei inhaltlich beantwortet: nur eine überwiegend richtig	Auf alle vier Anfragen reagiert, drei inhaltlich beantwortet: nur eine richtig	auf drei von vier Anfragen reagiert, zwei inhaltlich beantwortet: nur eine überwiegend richtig	alle Anfragen beantwortet: nur eine überwiegend richtig
	Werbe-fenster	störende Werbefenster	keine	keine	keine	keine Werbefenster, aber störende Download-aufforderungen für Zusatzprogramm	keine
	unerbetene Werbe-mails	keine	keine	keine	keine	keine	reichlich unerbetene Werbemails
	Nutzbarkeit	einfach	einfach	einfache Nutzbarkeit, aber aufwendige Erstanmeldung mit vielen persönlichen Daten	einfach	einfach	einfache Nutzbarkeit, aber aufwendige Erstanmeldung mit vielen persönlichen Daten

Abbildung 2: Stiftung Warentest - Bewertung kostenloser Expertenforen [test]

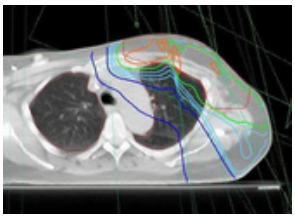


Abbildung 3: CT Schnitt mit Strahlentherapieplanung: Brustkrebs [Georg]

fik und an den Speicher stellt und aus diesem Grund erst in den 70er Jahren ihren Anfang nahm. Zuvor konnte die dreidimensionale Wirklichkeit mit den klassischen Abbildungsverfahren nur zweidimensional dargestellt werden.

Eines der wichtigsten bildverarbeitenden Diagnoseverfahren ist die Computertomographie (CT). Sie wurde durch die Nutzung eines mathematischen Verfahrens möglich, das 1917 entwickelt wurde. Die ersten echten Prototypen entstanden zwischen 1957 und 1963, entwickelt vom Elektrotechniker Godfrey Hounsfield. Nachdem zuerst ausschließlich an Tieren getestet wurde entstand 1971 schließlich die erste CT-Aufnahme am Menschen, ein Jahr später wurde sie schon klinisch eingesetzt.

2 Anwendungsgebiete der Informatik

Die Anwendungen informatischer Leistungen in der Medizin sind zahlreich. Das nachfolgende Kapitel gibt einen Überblick darüber.

2.1 Visualisierung/Analyse

Die digitale Bildverarbeitung spielt in der Medizin eine immer größere Rolle. Mittels moderner Verfahren wird das Innenleben des menschlichen Körpers in seinen feinsten Strukturen sichtbar gemacht. Auf den so gewonnenen Bildern können Strukturen automatisch erkannt und markiert werden. Die visuellen Daten lassen sich - etwa für die Operationsplanung - manipulieren und mittlerweile live während Operationen einblenden.

Man unterscheidet bei der Bildverarbeitung allgemein vier Bereiche: Erzeugung, Darstellung, Auswertung und Speicherung von Bildern. Auf die ersten beiden gehen wir ein, indem wir die namhaftesten Vertreter der Visualisierung des menschlichen Körpers, CT und MRT, vorstellen.

2.1.1 Computertomographie

Bei der Computertomographie (kurz CT) befindet sich der Patient in einer Röhre. Für jedes zweidimensionale Schnittbild (auf axialer, d.h. für den Patienten horizontaler Ebene, z.B. entlang der Hüfte) wird die Röhre insgesamt um 180° rotiert und dabei in fixen Abständen, etwa von 1°, ein eindimensionales Abbild der Absorption von Röntgenstrahlen in dieser Schicht erstellt. Durch ein mathematisches Verfahren, etwa die Fourier-Transformation, lässt sich aus diesen eindimensionalen Daten der zweidimensionale Schnitt rekonstruieren. Heute existieren CTs, die kontinuierlich um den Patienten rotieren, während dieser

langsam vorgeschoben wird. Dadurch wird es ermöglicht, dass ein 30 cm langer Untersuchungsabschnitt in 30 s eingescannt werden kann.

Für das Zusammenfügen mehrerer Schichtbilder zu einer 3D-Ansicht existieren verschiedene Verfahren. Auszugsweise sei hier die **konturbasierte Triangulation** vorgestellt. Dabei müssen auf jeder Schicht von sämtlichen Objekten die Außenkonturen markiert und diese Segmente topologisch sortiert werden. Anschließend verbindet man zwei Schichten zu einem Körper, indem jeweils ein Punkt aus der einen Schicht mit zweien aus der anderen ein Dreieck bildet. Dies lässt eine Parallelisierung des Prozesses zu. Die topologische Sortierung der Segmente lässt sich aufgrund von komplizierten, sich verästelnden Konturen jedoch nur sehr schwer automatisieren.

Neben diesem Modell existiert noch das des *Cone-Beam-CTs*. Bei diesem lassen sich durch den Einsatz eines 2D-Kegelstrahls (cone beam) statt eines eindimensionalen komplette Volumendatensätze mit nur einer Umdrehung der Röhre in unter 1s gewinnen. Dies ist vor allem dann von Vorteil, wenn eine zeitkontinuierliche Aufnahme gefordert ist. Allerdings ist die Bildrekonstruktion sehr aufwändig, u.a. weil sie im Gegensatz zu der vorher beschriebenen Methode nicht parallelisierbar ist. Unter [MeBV 05] wird dies ausführlich dargelegt.

Die Computertomographie ist nicht ungefährlich. So ist die Bestrahlung nach [Wiki CT] bis zu 1000 mal höher als bei einer Röntgen-Thorax-Aufnahme. CTs sollen daher in naher Zukunft für 2 % aller Krebskranken verantwortlich sein [WELT 08].

2.1.2 Magnetresonanztomographie

Die Magnetresonanztomographie (kurz MRT) wird vor allem dort eingesetzt, wo das CT an seine Grenzen stößt: Bei der Visualisierung verschiedener Gewebetypen, etwa zur Lokalisation von Tumoren im Hirn.

Dabei werden - ebenfalls in einer Röhre - mittels starker Magnetfelder (0,2 bis 3 Tesla [Wiki MRT]) die Wasserstoffkerne des Körpers angeregt, wodurch diese beim Abgeben der Energie ein Relaxationssignal senden, welches als Maß für die Protonendichte dient. Über ein Lokalisationsverfahren lassen sich die Signale ihrem Herkunftsort zuordnen. Die Physik dahinter wird unter [MeBV 05] näher erläutert.

Die MRT bietet i.d.R. bessere Auflösung und Kontrast als die CT. Des Weiteren sind anders als bei dieser keine schädigenden Nebenwirkungen bekannt.

2.1.3 Probleme

Bei der Darstellung und Auswertung von Bildern ergibt sich in der Medizinischen Informatik eine Reihe von Problemen. Die Bildauswertung setzt nach [MeBV 05] umfangreiches A-priori-Wissen voraus, welches so formuliert sein muss, dass es sich in einen Algorithmus umsetzen lässt. Aufgrund der großen Vielfalt an verschiedenen Ausprägungen von Körperteilen sowohl zwischen Patienten (z.B. unterschiedlich geformte Schädelknochen) als auch von ein und demselben Patienten zu unterschiedlichen Zeiten ist eine allgemeingültige Formulierung schwer zu treffen. Zudem ist es aufgrund fließender Übergänge oftmals unmöglich, anatomische Objekte klar abzugrenzen.

Des Weiteren ist die menschliche Wahrnehmung nicht geeignet, um Darstellungen räumlich ausgefüllter 3D-Strukturen sinnvoll zu erfassen. Aus diesem

Grund wird derzeit an innovativen Darstellungsmöglichkeiten gefüllter Räume geforscht. Näheres in [FIfF 06].

2.2 Computergestützte Chirurgie

Nach [CoCh 05] werden bei der Computergestützten Chirurgie (computer-assisted surgery, kurz CAS) drei Bereiche nach ihrem zeitlichen Bezug abgegrenzt: präoperative, intraoperative und postoperative Unterstützung.

2.2.1 Präoperativ

Anhand zuvor erstellter Bild- und Labordaten stellt das CAS-Programm ein Modell des Behandlungsortes dar, bietet Methoden zur automatischen Analyse und Segmentierung an und erlaubt die Manipulation des Modells zur Simulation und zum Training des Eingriffs. Eventuell schlägt es sogar selbstständig vor, wie bei der Operation vorgegangen werden soll.

2.2.2 Intraoperativ

Zunächst werden die Ergebnisse der präoperativen Planungsphase mittels eines Abgleichs der Bild- und Messwerte mit aktuellen Werten auf die Operationssituation angepasst. Während der Operation helfen *passive Systeme* dem Chirurgen bei der Orientierung, etwa indem dieser eine Brille trägt, die seine Sicht mit Daten aus einer MRT-Untersuchung überlagert (*augmented reality*). *Semiaktive Systeme* korrigieren Handbewegungen, z.B. beim Lasern, wohingegen *aktive Systeme* komplett selbstständig, aber unter Beobachtung des Arztes, die Operation durchführen.

2.2.3 Postoperativ

Hierbei handelt es sich um die Kontrolle des Heilungsverlaufs und Erkennung etwaiger Komplikationen.

2.2.4 MeVis LiverAnalyzer/Distant Services

ermöglicht die Planung von Leberoperationen. Diese gelten als besonders risikoreich, da sich der Aufbau der Leber aufgrund ihrer Komplexität kaum genau ermitteln lässt. Für die Nutzung des Programms müssen CT- oder MRT-Daten über das Internet an die MeVis-Abteilung der Universität Bremen geschickt werden. Dort werden die Daten automatisch ausgewertet, d.h. Gefäße, Organe und Tumore segmentiert sowie die risikoärmste Schnittführung und deren Erfolgschance berechnet ([FIfF 06]).

2.3 Automatische Diagnose

Das vorhandene medizinische Wissen hat mittlerweile enorme Ausmaße angenommen. Zudem wächst es stetig. So verzeichnet die medizinische Literaturdatenbank Medline [CAD 05] zufolge jährlich 500000 neue Publikationen. Da allein 64000 Publikationen für Internisten monatlich veröffentlicht werden ([SAEZ 08]), kann auch auf einem Fachgebiet ein Arzt schwerlich den Überblick behalten.

Die Ärzte selber sind sich ihres unvollständigen und z.T. stark in die Jahre gekommenen Wissens kaum bewusst. So kommt es laut [ERR 00] in den USA jährlich zu 44000 bis 98000 Todesfällen aufgrund fehlenden ärztlichen Wissens. Dies wirft die Frage auf, inwiefern sich Computer zur Diagnosehilfe eignen.

Expertensysteme sollen gerade dies leisten. Bei Eingabe der Symptome des Patienten sollen sie alle möglichen Diagnosen anzeigen, um eventuelle Wissenslücken des behandelnden Arztes auszumerzen.

Ein solches Expertensystem ist *CADIAG-II*, das für Diagnosen der inneren Medizin in Wien eingesetzt wird. Es basiert auf der Logik der Fuzzy Sets, da die boolesche Logik nicht ausreicht, um die komplexen Wissensbeziehungen der Medizin zu erfassen. So lässt sich kaum eine Aussage „Symptom A impliziert Krankheit X"mit Sicherheit treffen. Die Fuzzy Sets erlauben statt der absoluten Werte 0 und 1 für Mengenzugehörigkeit Werte aus dem Intervall [0,1], sodass wahrscheinlichkeitsbasierte Regeln modelliert werden können. *CADIAG-II* hat laut [CAD 05] je nach Anwendungsgebiet eine Zuverlässigkeit von bis zu 94 %, mit der sich die richtige Diagnose unter den angebotenen befindet. Jedoch landet diese nur in 53 % der Fälle unter den ersten fünf aufgezählten Diagnosen, sodass die eigentliche Entscheidungsfindung nach wie vor beim Arzt verbleiben muss.

Tatsächlich routiniert eingesetzt werden indes nur wenige Expertensysteme, was hauptsächlich daran liegt, dass die Ärzte der Entscheidungsfindung durch Computer skeptisch gegenüberstehen.

2.4 Kommunikation/Verwaltung

Die Verwaltung eines Krankenhauses erfordert immensen Aufwand bei der Verarbeitung, Übermittlung und Speicherung von Informationen. Aus diesem Grund wird in jedem Krankenhaus ein *Krankenhausinformationssystem* (KIS) eingesetzt, welches sowohl alle Bereiche sowie Gebäude des Krankenhauses umfassen als auch für sämtliche dort tätigen Personengruppen konzipiert sein muss.

Die Aufgaben eines KIS umfassen folglich die gesamte Informationsverwaltung des Krankenhaus: Patientenspezifische Daten wie Einweisungsdiagnosen oder Laborberichte werden gespeichert. Den Ärzten wird aktuelles medizinisches Wissen mittels einer Datenbank zugänglich gemacht und möglichst viel Dokumentationsaufwand abgenommen. Zur Koordination der (wirtschaftlichen) Verwaltung des Krankenhauses benötigt das Management detaillierte Informationen über dessen Finanzen sowie in die Informationssystem eingebettete Möglichkeiten, administrativ tätig zu werden. Sämtliche Informationen müssen - unter Wahrung der ärztlichen Schweigepflicht durch entsprechende Sicherheitskonzepte - an jedem Ort des Krankenhaus abrufbar sein, während der Austausch mit anderen medizinischen Einrichtungen und Ärzten gewährleistet wird.

Zur Bewertung eines KIS wird nach [KIS 05] primär der Nutzen für den Patienten betrachtet, da seine Genesung das Ziel des Krankenhauses ist. So hat die Minimierung dokumentarischen Aufwands für die Ärzte Priorität, da hierdurch den Ärzten mehr Zeit für den Umgang mit Patienten bleibt. Wichtig hierbei ist eine ausgewogene Verteilung konventioneller und computergestützter Verwaltungsgeräte, da z.B. der Notizblock nach wie vor in den meisten Fällen handlicher und schneller zu benutzen ist als ein mobiler Computer. Auch der schnelle Zugriff auf Medikamente und Pflegepersonal ist von Bedeutung. Wieviel Erleichterung ein gutes KIS trotz der hohen Kosten bringen kann, zeigt folgende

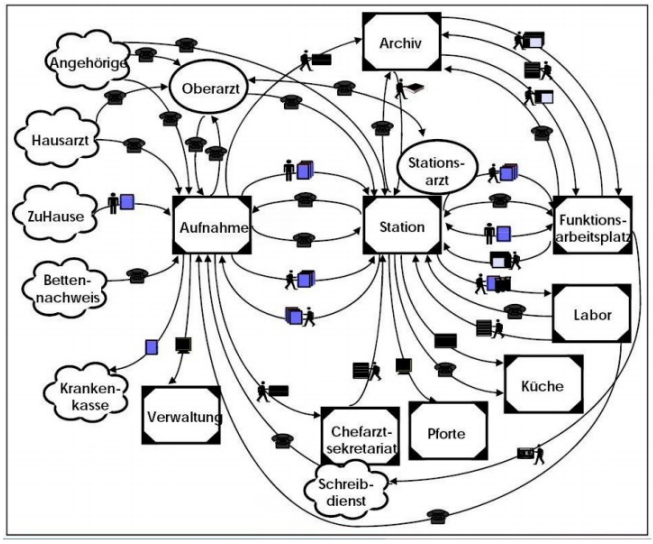


Abbildung 4: Kooperationsbild zur Aufnahme eines Patienten vor Einführung eines KIS [STE 09]

Abbildung:

Wegen der Ausmaße und Kosten eines solchen Systems lohnt es sich für eine Klinik nicht, ihre eigene Softwarelösung zu entwickeln. Vielmehr werden fertige Softwarebausteine gekauft und integriert. In Europa werden gegenwärtig 2,6 Mrd in KIS investiert, in den USA 3 Mrd . Dennoch zeigen Untersuchungen, dass 75–98 % der Bausteine für KIS Fehlschläge waren ([KIS 05]).

2.5 Forschung

Die Informatik ermöglicht einen Großteil der medizinischen Forschung überhaupt erst. Ein Beispiel dafür ist die Erforschung der Proteinfaltung um Erkenntnisse über den Krebs zu erhalten, für die es zahlreiche informationstechnische Lösungen gibt. Zwei davon stellen wir hier vor.

2.5.1 Folding@home

Wegen der Größe der Proteinmoleküle ist es sehr rechenaufwendig, die Proteinfaltung zu simulieren. Um den Vorgang zu beschleunigen, hat die Stanford University im Jahr 2000 das Projekt folding@home ins Leben gerufen, Dieses ermöglicht jedem Computernutzer mittels einer Software, ungenützte Rechenkraft zur Simulation der Faltung zu nutzen. Das Projekt wird von dem Team selbst als Erfolg bezeichnet ([FOLD]).

2.5.2 Foldit

Einen anderen Weg nimmt das Softwareprojekt foldit ([FOLDIT]), das auf die Fertigkeiten des Menschen in der Mustererkennung und dem Knobeln setzt. In Form eines Spiels motiviert es den Benutzer dazu, Proteine durch eigenständiges Falten in eine stabile Lage zu bringen. Zudem soll es demnächst dem Spieler

ermöglichen, eigene Proteine zu kreieren, welche unter Umständen zur Heilung von Krankheiten fähig sein könnten.

3 Softwarequalität

"Unter Softwarequalität allgemein versteht man die Gesamtheit der Merkmale und Merkmalswerte eines Softwareprodukts, die sich auf dessen Eignung beziehen, festgelegte oder vorausgesetzte Erfordernisse zu erfüllen„[Wiki SQ]
Zur Sicherung von Softwarequalität gibt es die DIN Normen, die dem Programmierer als freiwilliger Leitfaden dienen sollen. Sie entstehen auf Anregung und durch Initiativen interessierter Kreise und werden letztendlich vom *Deutschen Institut für Normung* erarbeitet.
Die letzte in Deutschland gültige DIN Norm war die DIN Norm 66272. Sie wurde im Mai durch die ISO/IEC 9126 ersatzlos gestrichen.
Im Gegensatz zur DIN gelten Normen der *International Standards Organisation (ISO)* international, ansonsten sind beide Institute ähnlich. In der ISO werden internationale Normen in allen Bereichen mit Ausnahmen der Elektrik und der Elektronik, für die die *Internationale Elektrotechnische Kommission (IEC)* zuständig ist, erarbeitet.
Die momentan geltende ISO Norm für Software beschreibt die Qualitätsmerkmale der Funktionalität, der Zuverlässigkeit, der Benutzbarkeit, der Effizienz, der Änderbarkeit und der Übertragbarkeit.

Da die Medizin im Gegensatz zu anderen Anwendungsgebieten höhere Ansprüche an die Software stellt, gelten hier darüber hinaus noch weitere Qualitätsmerkmale. Die erhöhten Anforderungen resultieren unter anderem daraus, dass in der Medizin Softwarefehler größere Konsequenzen nach sich ziehen, wodurch Patienten oder das Behandlungspersonal gesundheitlich gefährdet werden könnten. Darüber hinaus haben in der Medizin eingesetzte Geräte oder Software oftmals eine hohe Funktionalität und beschreiben wie die Computertomographie eine schwierige Materie, sind jedoch in den meisten Fällen kein Expertentool, sondern müssen vom ärztlichen Personal bedienbar sein, bei dem kein großes technisches Vorwissen vorausgesetzt werden darf.

Aus diesem Grund haben ISO und IEC für medizinische Software zusätzliche Normen geschaffen.
Eine wichtige Norm ist die IEC 62304. Sie beschreibt den Lebenszyklus von Software in Medizingeräten oder für Medizinprodukte, die ausschließlich aus Software bestehen. Sie beschreibt Anforderungen an den Entwicklungsprozess. Hauptaugenmerk liegt hierbei auf der Nachvollziehbarkeit von Anforderungen, der Risikoanalyse der eigenen Software und der Software von Dritt-Herstellern sowie die Etablierung von Konfigurations- und Änderungsmanagment.

Darüber hinaus gibt es noch die ISO 14971. Sie beschreibt die Anwendung des Risikomanagements auf Medizinprodukte und legt für Hersteller ein Verfahren fest um Gefährdungen durch Medizinprodukte zu erkennen und die Risiken abzuschätzen, zu bewerten und zu kontrollieren. Die Norm erfordert die Erstellung eines Risikomanagementplans, begleitend zum Produktlebenszyklus eines Medizinprodukts. Der Plan muss Folgendes enthalten:

- Anwendungsbereich des Plans, wobei das Medizinprodukt und die Abschnitte seiner Lebenszyklusphasen beschrieben sind

- einen Plan für die Verifizierung
- Zuordnung der Verantwortlichkeiten
- Anforderungen an die Bewertung der Risikomanagement-Aktivitäten
- Kriterien für die Vertretbarkeit von Risiken

Dadurch soll bei jeder Art von Gefährdung eine Rückverfolgung auf die frühere Analyse und Bewertung des Problems möglich gemacht werden.

Über den freiwilligen Normen ISO 14971 und IEC 62304 hinaus gibt es für Medizinprodukte allerdings auch eine EU Richtlinie, die Medical Device Directive [EU MP], die für die Entwickler durch das *Gesetz für medizinische Produkte und Verordnungen* bindend gemacht wird.
Die Medical Device Directive ist das wichtigste Regulierungsinstrument für die Sicherheit von Medizinprodukten im europäischen Raum. Sie klassifiziert die medizinischen Produkte und ermittelt anhand bestimmter Verfahren deren Konformität. Wie alle Richtlinien der EU ist das vorrangige Ziel den freien Warenaustausch innerhalb der Grenzen zu ermöglichen.

Zuletzt noch ein paar Beispiele, bei denen Softwarefehler in der Medizin zu Unfällen führten, die zum Teil tödlich endeten.

Ein besonders schwerwiegender Fall entstand durch die Nutzung des Therac-25. Therac-25 war ein Linearbeschleuniger zur Anwendung in der Strahlentherapie. Durch mangelnde Qualitätssicherung und daraus resultierenden Softwarefehlern kam es zwischen 1985 und 87 mehrmals zu schweren Fehlfunktionen, wodurch die Patienten einer höheren Strahlungsbelastung ausgesetzt waren als üblich. Die dadurch verursachte Strahlung wird im Nachhinein auf 40-200 Gray abgeschätzt. Die bei der Behandlung übliche Strahlung liegt bei unter einem Gray. Insgesamt kostete dieser Programmierfehler 3 Menschen das Leben und führte bei einigen anderen zu starken Verbrennungen.
Ursache für das Fehlverhalten war dabei die fehlerhafte Synchronisation zwischen den beiden unterschiedlichen Modi der Therac-25. Sie war zum Einen für die Messwerterfassung und Steuerung des Geräts und zum Anderen auch für die Benutzerinteraktion zuständig. Die Synchronisation funktionierte allerdings nur dann einwandfrei, wenn der Benutzer seine Eingaben relativ langsam machte. Bei einer schnelleren Bedienung kam die Therac-25 beim Wechseln der Modi nicht mehr mit. Dies führte meist zu Programmfehlern, die jedoch nicht behandelt wurde.
Dieser Fehler hätte durch eine angemessene Qualitätssicherung leicht entdeckt werden können. Zwar wurde das Gerät einigen Sicherheitstests unterzogen, jedoch wurde dabei nur die Hardware getestet. Die Möglichkeit, dass die Software fehlerbehaftet sein könnte, wurde ignoriert.

Ein anderer Softwarefehler führte 2000 im Nationalen Krebs Institut in Panama zum Tod von mindestens acht Patienten. Hier wurde ein Programm benutzt, um die genauen Werte für die Bestrahlung der Patienten zu ermitteln. Das gesunde Gewebe wird bei der Bestrahlung mit Metallschilden geschützt, die individuell angeordnet werden. Das Programm berechnet nun die Position dieser maximal 4 Schilde. Da die Ärzte aber 5 Schilde einsetzen wollten und diese Anzahl vom Programm nicht akzeptiert wurden, haben sie einfach ein einziges Schild angegeben, was ein Loch enthielt, in dem sich dann das carzinogene Gewebe befindet. Dadurch wurde vom Programm allerdings eine andere

Bestrahlungsdosis berechnet und die Patienten wurden zum Teil mit der doppelten Dosis bestahlt, wodurch im 8 Menschen starben und 20 verletzt wurden. Darüber hinaus wurden die behandelnden Ärzte, die nach dem Gesetz alle vom Computer errechneten Wert von Hand überprüfen müssen, wegen Mordes angeklagt.

4 Gesundheitliche Auswirkungen von IT-Arbeit

Bei der Betrachtung der Wechselwirkungen von Medizin und Informatik muss man sich auch die Frage stellen, wie sich IT-Berufe auf die Gesundheit auswirken. Diese Fragestellung lässt sich beantworten, indem man sie auf Projektarbeit überträgt, da Informatiker heute zu einem großen Teil ihre Brötchen in Projekten verdienen.

Dies liegt nicht zuletzt an den großen gesundheitlichen Erwartungen, die man an Projektarbeit hegt. Ein hoher Grad an Freiheit und damit Verantwortung soll das Selbstbewusstsein stärken sowie die Leistung verbessern, während die Kooperation mit Teammitgliedern die Laune heben und den Geist schärfen müsse.

Das Gegenteil scheint jedoch der Fall zu sein.
Nach aktuellen Studien ([GERL 05], Zusammenfassung bei [DUES 05]) sind fast drei Viertel aller Projektarbeiter übermüdet und ein Großteil von ihnen zeigt massive Anzeichen chronischer Erschöpfung sowie Nervosität. Jeder Vierte glaubt nicht, den Druck auf Dauer aushalten zu können, wohingegen ein Drittel der Befragten als direkt Burnout-gefährdet eingestuft wird.

Die Gründe für dergestaltige Befunde liegen vor allem im Zeitdruck, welcher durch widersprüchliche Arbeitsanforderungen wie sich ständig wandelnde und wachsende Anforderungen, die nicht durch entsprechende Terminverzögerungen kompensiert werden, entsteht. Nicht eingeplanter Dokumentationsaufwand und Einarbeitungszeit in immer neue Gebiete sind weitere Schrauben des Drucks. Hinzu kommt nach [FIfF 06], dass in vielen Projekten mehrere Verantwortliche sind und auch Kunden Weisungen erteilen können, was zu einer unklaren Verantwortungsverteilung führt.

5 Datenschutz

5.1 Ärztliche Verschwiegenheitspflicht

In Deutschland gilt die Verschwiegenheitspflicht für alle Angehörigen heilbehandelnder Berufe (§203 StGB), die sich auf alle erhobenen Patientendaten bezieht. Unter die Verschwiegenheitspflicht fallen nicht nur jegliche Daten über Krankheiten und Behandlungsmaßnahmen, sondern schon allein die Tatsache, dass der Betroffene überhaupt unter Behandlung steht.

Als Strafe bei Verstoß wird eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe angesetzt. Die Schweigepflicht ist außerdem in der Berufsordnung der Ärztekammer verankert, so dass zusätzlich auch das Berufsgericht Strafen verordnen kann. So ist zum Beispiel im Psychotherapeutengesetz als Strafe das Verbot der Berufsausübung festgelegt.
Selbst bei einer Praxisauflösung oder sogar im Todesfall des Arztes ist die Verwahrung der Patientendaten gesetzlich geregelt, wobei die Verwahrungspflicht

an den Arzt als Privatperson bzw. die Erben und zuletzt an den Staat übergehen. Bedenklich ist hierbei die Verwahrung bei einer Privatperson, da die Datensicherheit dort nicht immer sichergestellt ist.
Auch elektronisch gespeicherte Patientendaten sind von der Schweigepflicht eingenommen, da diese unabhängig von der Form der Speicherung gilt.

Diese gute Grundlage für eine dem persönlichen Datenschutz gerechte Verwahrung von Patientendaten relativiert sich jedoch zunächst durch die vorgesehenen **Ausnahmen**.

So ist durch *schriftliche Einwilligung* des Patienten eine Weitergabe von Daten möglich. Diese kann dem Patienten in Behandlungsverträgen abverlangt werden, vor allem aber verlangen private Kranken- und Lebensversicherung eine generelle Entbindung behandelnder Ärzte von der Schweigepflicht.
Die Krankenkassen können unter Vorlage dieser Einwilligung Auskünfte von behandelnden Ärzten einholen. Da dies auch elektronisch möglich ist, ist die Echtheit der übermittelten Einwilligung von Seiten des Arztes schwer festzustellen und wird bisweilen auch vernachlässigt.
Gegenüber der gesetzlichen Krankenkassen ist im Sozialgesetzbuch eine *Auskunftspflicht* festgelegt, die Ärzte und Krankenhäuser verpflichtet personenbezogene Daten in großem Umfang weiterzugeben, sodass auch hier die Schweigepflicht außer Kraft gesetzt wird.
Zuletzt gibt es noch Ausnahmen, die dem Schutz der Bevölkerung dienen: Liegt ein *rechtfertigender Notstand* nach §34 StGB vor, darf die Schweigepflicht gebrochen werden. Ein rechtfertigender Notstand liegt beispielsweise vor, wenn klar wird das ein Patient ohne Brille eine Gefährdung des Straßenverkehrs darstellt und sich keine Brille beschafft. Ebenso wird die Schweigepflicht ausgesetzt wenn von einer *stillschweigenden Einwilligung* ausgegangen werden kann, beispielsweise bei einem Wechsel des behandelnden Arztes im Krankenhaus. Auch muss ein Arzt die Kenntnis über von Patienten *angekündigte schwere Straftaten* weitergeben.

Berücksichtigt man, dass in jeder modernen Praxis EDV zum Speichern und Verwalten von Daten eingesetzt wird, ergeben sich viele neue potentielle Datenlecks. Zwar existieren rechtliche Datenschutzrichtlinien, diese bezeichnen aber nur einen sehr allgemeinen Rahmen. Die Landesärztekammer Baden-Württemberg stellt dazu in [LAKBW] fest:

> Die rechtlichen Rahmenbedingungen für eine Praxis-EDV sind entweder sehr allgemein oder auf enge Spezialfragen beschränkt. Es fehlt eine umfassende systematische Regelung.

In der Praxis führt dies zur Missachtung der rechtlichen Anforderungen: Die Praxis EDV ist meist „offen“. Sie ist ans Internet angebunden, verwendet Standardsoftware, die nicht den höheren Sicherheitsansprüchen genügt und bietet die Möglichkeit, private Wechseldatenträger wie USB-Sticks zu benutzen.

Zudem ist die Integrität digital gespeicherter Daten ungleich schwerer festzustellen als die von auf Papier vorhandenen Daten. Eine Manipulation kann stattfinden, ohne das die Änderung bemerkt wird.
Nichtsdestotrotz existieren integrierte Softwarelösungen, die den Anforderungen im Praxisbetrieb gerecht werden sollen. Durch Mittel der Kryptografie, digitale Signaturen und Backups können die oben genannten Probleme von einem integrierten, abgeschlossenen System weitestgehend gelöst werden.

Dass dies trotz vorhandener technischer Möglichkeiten nicht immer gelingt, zeigen die folgenden Beispiele auf.

5.2 Datenschutzpannen: Beispiele

Der US Gesundheitsdienst Kaiser Permanente (zu finden unter den Top 40 der größten Unternehmen der Welt) verschickte im Jahr 2000 858 Antwortmails auf Patientenanfragen an die falschen Empfänger [HeiKP]. Nachdem fälschlicherweise die Mail-Auslieferung stoppte, wurde ein Hotfix zur Lösung des Problems geschrieben, durch den die falschen Empfängeradressen zustande kamen.

Im Thinkpad-Forum [TPF] wurde im Oktober 2009 ein Fall beschrieben, bei dem eine erworbene gebrauchte Festplatte auf noch vorhandene Dateien untersucht wurde. Der Käufer konnte — da keine sichere Löschmethode verwendet wurde — auf der Festplatte Patientendaten, Diagnosen, Rechnungen, Krankheitsverläufe und Passwörter vorfinden, allem Anschein nach aus einem Krankenhaus- oder Praxisbetrieb.

In Österreich wurden Informationen im Laufe von Rettungseinsätzen unverschlüsselt über das POCSAG-Pager-Netz übertragen, sodass es für einen findigen Hacker ein leichtes war, die gesendeten Codes mit frei erhältlicher Software abzuhören, und — dank einer öffentlich zugänglichen Codierungstabelle der Rettungsleitstelle Tirol [LTir] — auch auszuwerten.
Bei jedem der ca. 400.000 Einsätzen pro Jahr wurden der vollständige Name des Patienten, der genaue Einsatzort und das Transportziel sowie der Code für eine detaillierte Erstdiagnose übermittelt. So steht z.B. 26A22 für ein Penisproblem, 10C3 für Brustschmerzen durch Kokainmissbrauch, 25A2 für eine Selbstmordgefährdung und 26O25 für eine Geschlechtskrankheit.
Es stand zwar bereits ein verschlüsseltes Pager-Netz zur Verfügung, aus finanziellen Gründen wurde dessen Ausbau sowie die Anschaffung passender Geräte jedoch nicht vorangetrieben.

5.3 Aktion: Datenschutz in meiner Arztpraxis

Der problematischen Lage bewusst, initiierte das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein zusammen mit der Ärzte- und Zahnärztekammer Schleswig-Holsteins eine Aufklärungs- und Unterstützungsaktion für Ärzte, Arzthelfer und Krankenhausmitarbeiter.
Die im Jahr 2001 beginnende Aktion hatte das Ziel, den häufig unzureichenden Datenschutz wesentlich zu verbessern. Ausgangspunkt stellte eine Befragung von Patienten in der Kieler Innenstadt dar, bei der 95% angaben, das Patientengeheimnis sei ihnen sehr wichtig, 50% der Befragten allerdings schon Erfahrungen mit Indiskretion gemacht hatten.

Obwohl die geltenden Normen strafrechtlicher Natur sind, wurde auf Kooperation mit den Ärzten gesetzt und vor allem eine höhere Sensibilisierung angestrebt.

Dazu wurde zunächst allen Ärzten ein „Selbst-Check“ [SHACheck] angeboten, in dem Fragen zu allen Bereichen der Praxis einschließlich Empfang, Wartebereich und Verwaltung enthalten sind.
Zusätzlich wurden weitere Tipps und Anregungen auf der Webseite der Aktion [SHA] veröffentlicht.

Im weiteren Verlauf wurden individuelle Beratungen und Schulungen angeboten und die Aktion auf Krankenhäuser und Kliniken ausgeweitet.

Die Aktion wurde von den beteiligten Ärzten positiv wahrgenommen. Bei einer abschließenden Umfrage wurde bestätigt, dass die Mehrheit zwar sensibel mit konventionellen Patientenaktion umgeht, bei der Verwendung von EDV allerdings diesbezüglich Defizite hat.

Aus aktuellen Gründen wurde 2005 der Schwerpunkt der Aktion auf das Thema elektronische Gesundheitskarte verlagert.

5.4 Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte (eGK) sollte ursprünglich Anfang 2006 eingeführt werden und die alte Krankenversicherungskarte ablösen [SGB]. Die Einführung verzögerte sich jedoch und bis heute läuft nur eine Testphase in der Region Nordrhein in Nordrhein-Westfalen. Nach aktuellem Stand soll die eGK bis Ende 2010 flächendeckend eingesetzt werden.

Im Unterschied zur herkömmlichen Krankenversicherungskarte ist die eGK eine Prozessor-Chipkarte, die weitere Daten speichern kann und Möglichkeiten zur Identifikation bietet. Vorgesehen ist die Speicherung folgender Daten [Wei 04]:

eRezept Sogenannte e-Rezepte werden vom ausstellenden Arzt erstellt, signiert und auf die eGK geschrieben.

Zum Einlösen soll ein zertifiziertes „Gesundheitsterminal“ z.B. in der Apotheke, das e-Rezept von der Karte lesen, sodass dieses eingelöst werden kann.

Alternativ kann der Transfer auch sicher verschlüsselt über einen Server als Zwischenstation laufen. Die Verschlüsselung, die in beiden Fällen zum Einsatz kommt, basiert auf dem Public-Key Verfahren und gilt als sicher. Einziger Kritikpunkt ist das als abgeschottetes System konzipierte „Gesundheitsterminal“. Bei solch einer „Black-Box“ ist nicht zwangsweise sichergestellt, das die Lösch- und Aufbewahrungsnormen immer eingehalten werden. Wie das Beispiel Wahlautomat demonstriert, sind derartige Systeme auch nicht vor Manipulation geschützt.

Notfallversorgungsdaten Zur schnelleren und besseren Akutbehandlung können z.B. Informationen über chronische Krankheiten, Herzschrittmacher, Blutgruppe auf der Karte gespeichert sein.

elektronischer Arztbrief Die elektronische Variante der Patientenüberweisung

Arzneimitteldokumentation Verabreichte Arzneimittel (Historie)

elektronische Patientenakte Die elektronische Patientenakte (EPA) soll einen integrierten Zugriff auf wichtige Patientendaten (Arztbriefe, Impfungen) ermöglichen. Behandlungen werden nicht mehr wie bisher „problembezogen“ gespeichert sondern „prozessorientiert“. Es soll ein schneller Zugriff auf relevante Vorbehandlungen ermöglicht und eine Doppeluntersuchung vermieden werden.

Ein deutlicher Kritikpunkt ist die gemeinsame Speicherung der gesamten Behandlungsdaten. Diese wären z.B. auch für Lebensversicherungen zur

Risikoabschätzung von Interesse, andere Missbrauchsmöglichkeiten sind ebenfalls denkbar.

Leistungen und Kosten Kosten und Art der in Anspruch genommenen Leistungen

Da der Speicherplatz auf der eGK auf lediglich 32 Kilobyte begrenzt ist, werden von den oben genannten Datensätzen lediglich die Notfallversorgungsdaten *direkt* auf der Karte gespeichert. Alle weiteren Daten liegen zentral auf Servern. Die Karte dient hierbei als Schlüssel, ohne den die Daten nicht ausgelesen werden können. Zentral gespeicherte Daten ziehen gewisse Risiken nach sich:

- Kann gewährleistet werden, das die Daten nicht in falsche Hände geraten?
  Durch eine zentrale Speicherung kann eine Sicherheitslücke den Zugang zu mehreren Millionen Datensätzen gleichzeitig ermöglichen. Bei einer dezentralen Speicherung, d.h. direkt auf der Karte, besteht dieses Problem nicht.

- Ist für den Patienten noch transparent, welche Daten gespeichert sind?
  Andernfalls wäre das Gesetz auf informationelle Selbstbestimmung verletzt.

- Ist die Verfügbarkeit der Daten gewährleistet?
  Ein Angriff auf die Server ist nicht nur kritisch, wenn Daten gestohlen werden, sondern auch wenn Daten z.B. gelöscht werden.
  Ein Fall in den USA zeigt dies anschaulich: Im Mai 2009 brachten Cracker eine Patientendatenbank mit 8 Millionen Einträgen in ihre Kontrolle, verschlüsselten diese und verlangten für die Herausgabe des Passwortes 10 Mio. US-Dollar [HeiCr]

Aufgrund von umfangreichen Bedenken bezüglich des Datenschutzes lehnte der Deutsche Ärztetag 2007 und 2008 die Einführung der eGK mit großer Mehrheit ab.
Trotzdem wird die Einführung fortgesetzt und bis Ende 2010 soll die elektronische Gesundheitskarte deutschlandweit eingeführt sein.

Literatur

[CAD 05] C. Spreckelsen, K. Spitzer. Entscheidungsunterstützung und Wissensbasen in der Medizin. In T.M. Lehmann et al. Handbuch der Medizinischen Informatik, zweite Ausgabe, Seite 483. Hanser, 2005.

[CoCh 05] P. Hassenpflug, H.P. Meinzer, G. von Voigt, T. Tolxdorff, K.H. Englmeier. Computerunterstützte Chirurgie. In T.M. Lehmann et al. Handbuch der Medizinischen Informatik, zweite Ausgabe, Seite 425. Hanser, 2005.

[DUES 05] Zusammenfassung der Gerlmaier-Studie (http://www.iaq.uni-due.de/projekt/iat/nachhalt1.php)

[EGK] Wikipedia: Elektronische Gesundheitskarte (http://de.wikipedia.org/wiki/Elektronische_Gesundheitskarte)

[EU MP] EU Richtlinie 93/42/EWG über Medizinprodukte (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0042:DE:HTML)

[ERR 00] L.T. Kohn, J.M. Corrigan, M.S. Donaldson. To Err is Human: Building A Safer Health System. National Academy Press Washington, D.C., 2000.

[FIfF 06] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.: Gesundheit. FIfF Kommunikation, 1/2006

[FOLD] Folding@Home: Science (http://folding.stanford.edu/English/Science)

[FOLDIT] The Science Behind Foldit: (http://fold.it/portal/info/science)

[Georg] St. Georg, Klinik für Strahlentherapie und Radioonkologie (http://www.sanktgeorg.de/729.html)

[GERL 05] Gerlmaier A, Latniak E. Nachhaltige Arbeitsgestaltung von Projektarbeit im IT-Bereich: Ansatzpunkte und Grenzen, 2005

[HeiCr] Heise Online: Cracker fordern 10 Millionen US-Dollar für Patientendatenbank, 05.05.2009 (ttp://www.heise.de/newsticker/meldung/Cracker-fordern-10-Millionen-US-Dollar-fuer-Patientendatenbank-217345.html)

[HeiKP] Heise Online: Datenschutzpanne bei Kaiser Permanente, 11.08.2000 (http://heise-online.mobi/news/Datenschutzpanne-bei-Online-Gesundheitsdienst-536387.html)

[HeiÖ] Heise Online: Österreichische Patientendaten landen im Netz, 08.09.2009 (http://www.heise.de/ct/meldung/oesterreichische-Patientendaten-landeten-im-Netz-755193.html)

[ICD] Internationale statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme 10. Revision (ICD) (http://www.dimdi.de/static/de/klassi/diagnosen/-icd10/htmlgm2010/index.htm)

[ITWM] uni-protokolle.de Nachrichten: Großes Forschungsprojekt des Fraunhofer ITWM mit der Harvard Medical School, 27.07.2004 (http://www.uni-protokolle.de/nachrichten/id/37366/)

[KIS 05] A. Winter, E. Ammenwerth, B. Brigl, R. Haux. Krankenhausinformationssysteme. In T.M. Lehmann et al. Handbuch der Medizinischen Informatik, zweite Ausgabe, Seite 549. Hanser, 2005.

[Köh] Claus O. Köhler Historie der Medizinischen Informatik in Deutschland von den Anfängen bis 1980

[LAKBW] Schweigepflicht und Datenschutz in der Arztpraxis, Landesärztekammer Baden-Wuerttemberg (http://www.ms-care.eu/typo3conf/ext/nf_downloads/pi1/-passdownload.php?downloaddata=4)

[Leh 05] T.M. Lehmann et al. Handbuch der Medizinischen Informatik, zweite Ausgabe. Hanser, 2005.

[LTir] Leitstelle Tirol, Einsatzcodes (http://www.leitstelle-tirol.at/Downloads.62.0.html)

[MeBV 05] T.M. Lehmann, J. Hiltner, H. Handels. Medizinische Bildverarbeitung. In T.M. Lehmann et al. Handbuch der Medizinischen Informatik, zweite Ausgabe, Seite 361. Hanser, 2005.

[Parz 05] Parzeller M, et al. Zertifizierte Medizinische Fortbildung: Die ärztliche Schweigepflicht, Deutsches Ärzteblatt 102 (4. Februar 2005)

[SAEZ 08] http://www.saez.ch/pdf_d/2008/2008-44/2008-44-1076.PDF

[SEZYKL] Elektroniknet.de: Software-Entwicklung für Medizinprodukte, Lebenszyklus-Modell (http://www.elektroniknet.de/home/medizinelektronik/im-detail/software-entwicklung-fuer-medizinprodukte/3/)

[SFail] netzzeitung.de: Die schlimmsten Software-Fehler aller Zeiten, 09.11.2005 (http://www.netzeitung.de/internet/366911.html)

[SGB] §291a SGB (http://bundesrecht.juris.de/sgb_5/__291a.html)

[SHA] Aktion Datenschutz in meiner Arztpraxis (https://www.datenschutzzentrum.de/medizin/arztprax/aktion.htm)

[SHACheck] Aktion Datenschutz in meiner Arztpraxis: Selbstcheck (https://www.datenschutzzentrum.de/download/selbstch.pdf)

[STE 09] W.G. Bleek. Softwareentwicklung II: Vorlesung Softwaretechnik und Software-Ergonomie. Universität Hamburg, 2009.

[test] Stiftung Warentest: Kostenlose Expertenforen, Heft 04/2003 (http://www.test.de/themen/gesundheit-kosmetik/test/Medizinische-Beratung-im-Internet-Von-richtig-gut-bis-voll-daneben-1091512-1091502/)

[TPF] Thinkpad-Forum Beitrag: Vertrauliche Daten auf gebrauchter HDD (http://www.thinkpad-forum.de/forum-community/was-sonst-nicht-passt/75384-vertrauliche-daten-auf-gebrauchter-hdd/)

[VP] Wikipedia: Verschwiegenheitspflicht (http://de.wikipedia.org/wiki/Verschwiegenheitspflicht)

[Wei 04] T. Weichert. Die elektronische Gesundheitskarte, Datenschutz und Datensicherheit 28, 07/2004 (https://www.datenschutzzentrum.de/medizin/gesundheitskarte/-dud_gesundheitskarte.pdf)

[WELT 08] Welt Online. Krebsgefahr: Experten warnen vor Computertomografie. (http://www.welt.de/wissenschaft/article1667375/-Experten_warnen_vor_Computertomografie.html)

[Wiki CT] Wikipedia: Computertomographie

[Wiki EKG] Wikipedia: EKG
(http://de.wikipedia.org/wiki/EKG)

[Wiki EU] Wikipedia: EU Richtlinie 93/42/EWG über Medizinprodukte
(http://de.wikipedia.org/wiki/Richtlinie_93/42/-
EWG_%C3%BCber_Medizinprodukte)

[Wiki ICD] Wikipedia: ICD
(http://de.wikipedia.org/wiki/Internationale_statistische_Klassifikation_-
der_Krankheiten_und_verwandter_Gesundheitsprobleme)

[Wiki MRT] Wikipedia: Magnetresonanztomographie
(http://de.wikipedia.org/wiki/Magnetresonanztomographie)

[Wiki SQ] Wikipedia: Softwarequalität
(http://de.wikipedia.org/wiki/Softwarequalit%C3%A4t)

[Wiki Th] Wikipedia: Therac-25
(http://de.wikipedia.org/wiki/Therac-25)
(http://de.wikipedia.org/wiki/Computertomographie)

Künstliche Agenten und Ethik

Thies Henken, Daniel Knittel

Zusammenfassung

Diese Zusammenfassung des Vortrags über Künstliche Agenten und Ethik schneidet das gewaltige Themengebiet der künstlichne Intelligenz nur sehr oberflächlich an und vermittelt nicht mehr als eine leichte Idee der Thematik. So gehen wir von den Definitionen der biologischen sowie künstlichen Intelligenz über zu Anwendungsbeispielen bis hin zu Ausschnitten der KI-Geschichte sowie ethischen Gesichtspunkten.

1 Intelligenz

Den Begriff der Intelligenz bringt man in erster Linie mit der Intelligenz des Menschen in Zusammenhang, die sich durch Wissen und geschicktes Anwenden desselben auszeichnet. Dies ist eher eine umgangssprachliche Beschreibung des Begriffs. In unserem Fall könnte man dann auch einem Computer überdurchschnittliche Intelligenz zusprechen, da dieser riesige Zahlen in wenigen Millisekunden multiplizieren oder auf dem man Unmengen an Wissen abspeichern und schnell wiedergeben kann. Deswegen muss der Begriff der Intelligenz noch weiter abgegrenzt werden.

Der Begriff Intelligenz umfasst ein sehr umfangreiches Feld. Es gibt viele Möglichkeiten und Versuche sich ihm über verschiedene Definition zu nähern. Eine Definition beschäftigt sich meist mit dem Inhalt und dem Umfang des Begriffs Intelligenz. Es ist schwer eine allgemein gültige Definition zu formulieren, deshalb handelt es sich bei solchen Versuchen eher um Theorien (Intelligenztheorien). Wir haben uns dafür entschieden nur mit den geläufigsten Interpretationen zu arbeiten und werden im folgenden auf diese eingehen.

Intelligenz ist als ein Oberbegriff für die kognigtive Fähigkeiten zu verstehen. Wissen und Sprache anzuwenden und zu abstrahieren. Hinzu kommt die Erkennung und die Auseinandersetzung mit Problemen und das Finden einer Lösung. Einige Theoretiker sprechen davon, dass Gefühle, wie Schmerz oder Liebe, zu einem Teilbereich der Intelligenz gehören. Für Künstliche Agenten hingegen, steht das Lernen und das Lösen von Problemen an erster Stelle.[1]

1.1 Künstliche Intelligenz

Der Begriff "künstliche Intelligenz"(kurz KI, engl. AI für "Artificial Intelligence") wurde 1995 von John McCarthy geprägt und zum ersten mal bei der Dartmouth Conference diskutiert. Alan Turing, McCulloch und Pitts wären in diesem Zusammenhang noch erwähnenswerte Persönlichkeiten, stellen aber auch nur einen Bruchteil der Menschen dar, die zur Entwicklung der künstlichen Intelligenz beigetragen haben. Es gab viele Versuche die KI hinreichend zu umschreiben, was

[1] http://www.profilingportal.de/intelligenz_iq_test/intelligenz.htm

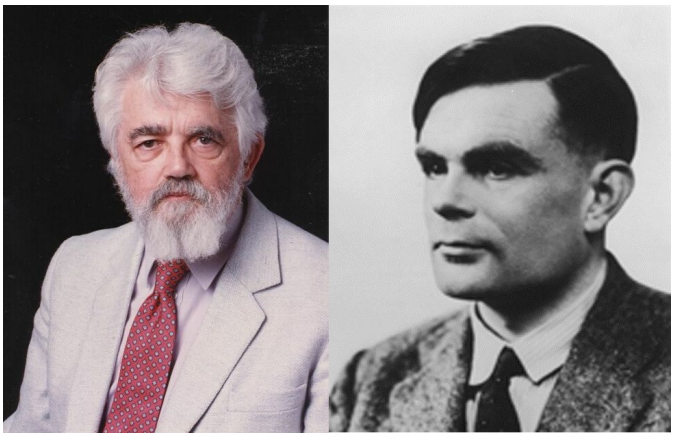


Abbildung 1: v.l.n.r McCarthy, Turing

zu vielen Definitionen führte, die meistens aber nich das komplette Spektrum der künstlichen Intelligenz abdecken konnten oder aber auch Dinge erfassten, die eindeutig nicht zur KI gezählt werden dürften. Das mag deshalb so schwer sein, weil der Mensch die eigene Intelligenz, oder die Essenz derselben selbst noch nicht wirklich durchdrungen hat. So gelten einige Anstrengungen in der KI dem Nachbau von Dingen, die von den Erbauern selbst nicht vollständig verstanden werden.

Dennoch schaffte es Elaine Rich eine passende Beschreibung dieser Teildisziplin der Informatik zu formulieren: "Artificial Intelligence is the study of how to make computers do things at which, at the moment, people are better". Diese Definition umfasst die KI in den meisten ihrer Facetten. [2].

1.2 Turing Test

Der Turing Test ist ein von Alan Turing entwickelter Test der es ermöglichen sollte die Intelligenz einer Maschine messen zu können.

In diesem Test agieren drei Teilnehmer, zwei menschliche und ein Computer. Dabei gibt es einen Interviewer, diesen Part übernimmt ein Mensch, und zwei Antwortgeber. Der Interviewer kann über ein Terminal einem der beiden Teilnehmer eine Frage stellen und anhand dessen Antworten entscheiden, ob es sich bei dem Gegenüber um einen Menschen oder um eine Maschine handelt. Sollte ein durchschnittlich intelligenter Interviewer nach einer 5 minütigen Unterhaltung nur eine 70 prozentige Chance haben eindeutig zwischen Mensch und Maschine unterscheiden zu können, würde die Maschine diesen Test bestehen.

Es ist umstritten inwiefern und ob überhaupt dieser Test aussagekräftig ist, bisher hat es jedoch auch noch keine Maschine geschafft ihn zu bestehen. Doch ebenso ist unklar ob man einer Maschine, die diesen Test besteht, auch wirklich so etwas wie Intelligenz zusprechen kann. Heute gibt es bereits Programme(siehe Chatbot), die mehr oder weniger auf simpler Textanalyse basieren und dennoch in der Lage sind manche Menschen für gewisse Zeit zu täuschen.

[2]Grundkurs Künstliche intelligenz, Wolfgang Erte

Zu Turings Test wurde 1991 der Loebner Preis ins Leben gerufen. Dieser wird dem Programm verliehen, das den Turing Test besteht. Da wir heutzutage noch zu weit von solch einem Programm entfernt sind, werden beim Loebner Preis verschiedene, u.A auch eine entschärfte Version des Tests angewendet.

Der schwerste dieser Tests ist der audiovisuelle Turingtest. Dabei muss eine Maschine sowohl optisch als auch intellektuell, sowie in gesprochener Sprache einen Menschen täuschen können. Das ist der schwerste aller Turingtests und – sofern es überhaupt möglich ist – wird es am längsten dauern solch eine Maschine zu entwickeln.

Der originale Test wie ihn Turing im Sinn hatte ist der schriftliche Test. Dabei soll ganz bewusst der visuelle Teil weggelassen werden um das Augenmerk nur auf die Intelligenz beschränken zu können.

Den Preis für die entschärfte Version des Tests haben schon einige Programme erhalten, unter anderem auch Weizenbaums ELIZA. Dabei wird lediglich das menschenähnlichste Programm gekrönt. Keines also, das tatsächlich einen Menschen täuscht sondern es aus einer Reihe von ähnlichen Programmen nur am besten hinbekommt. [3]

1.3 Schwache künstliche Intelligenz

Ein weiterer Begriff ist die 'schwache Künstliche Intelligenz', diese befasst sich damit konkrete Anwendungsprobleme zu erkennen und zu lösen, für die irgendeine Form von „Intelligenz“ erforderlich ist. „Letztlich geht es der schwachen KI somit um die Simulation intelligenten Verhaltens mit Mitteln der Mathematik und der Informatik, es geht ihr nicht um Schaffung von Bewusstsein oder um ein tieferes Verständnis von Intelligenz.“ [4]

1.4 Starke künstliche Intelligenz

Spricht man heute von künstlicher Intelligenz, denkt ein Laie immer unwillkürlich an intelligente Roboter wie man sie aus vielen Science Fiction Filmen kennt. Maschinen, die die Fähigkeiten eines Menschen auf mindestens demselben Niveau beherrschen, sie meist sogar übersteigen. Maschinen die reden, verstehen und denken können.

Eben das bzw. Teile davon sind das Ziel der starken künstlichen Intelligenz - natürlich möglichst ohne den ganzen negativen Folgen, wie sie in solchen Filmen dargestellt werden.

Welchen Nutzen und welche Konsequenzen das tatsächlich für uns Menschen hätte ist nicht eindeutig zu klären. Prognosen gehen hierbei von utopischen Zuständen über den Verlust des Lebenssinnes bis hin zur Versklavung oder Vernichtung der Menschen. Alles sind denkbare Szenarien mit denen sich viele Wissenschaftler, Philosophen und Künstler beschäftigt haben.

Um so etwas überhaupt bewerkstelligen zu können, müssten Maschinen von einer Simulation der Intelligenz, wie man sie heutzutage bei der schwachen KI beobachten kann, zu richtigem Denken übergehen. Das bedeutet insbesondere, dass sie ein Bewusstsein und im letzten Schritt vielleicht sogar Gefühle und

[3] http://plato.stanford.edu/entries/turing-test/

[4] Siehe Starke Künstliche Intelligenz

Emotionen entwickeln müssen. Man könnte hier von der Erschaffung einer neuen Lebensform reden. [5]

2 Künstliche Agenten

Bei der Bezeichnung 'Künstliche Agenten' spricht man oft auch von Agenten, von Software-Agenten oder von Multiagentensystemen. Diese Künstliche Agenten haben ein gewisses eigenständiges Verhalten, dass wir nun versuchen zu beschreiben. Im folgenden werden wir einige wichtige Eigenschaften des künstlichen Agenten aufzählen und erläutern. Diese Eigenschaften kann er besitzen, muss sie aber nicht zwangsläufig alle aufweisen, um seiner Bezeichnung gerecht zu werden:

Der künstliche Agent ist autonom, dass heißt das Programm beziehungsweise die Maschine arbeitet unabhängig. Es sind also keine äußeren Benutzereingriffe nötig. Dies ist hilfreich wenn es nicht die Möglichkeit gibt den Agenten zu bedienen, wie zum Beispiel ein Bergungsroboter. Dieser ist nicht unbedingt in jeder Situation erreichbar und ein Funkkontakt ist beispielsweise in einer Höhle nicht immer möglich. Ein weiteres Beispiel ist der Marsroboter. Ein Befehl an einen solchen Roboter zu schicken, wäre ein zu großer Zeitaufwand und ist wegen der Entfernung nicht möglich.

Er ist proaktiv. Diese Eigenschaft beschreibt, dass das Programm beziehungsweise die Maschine Aktionen aufgrund einer eigenen Initiative auslöst. Dieser Bereich gehört zu dem, eben beschriebenen, autonomen Verhalten.

Der künstliche Agent reagiert auf Änderungen, man nennt diese Eigenschaft in der Fachsprache: reaktiv.

Man bezeichnet den künstlichen Agenten als sozial, da er mit anderen Agenten kommunizieren kann. Unter dieser Voraussetzung ist es möglich ein Multiagentensystem zu entwickeln.

Ein künstlicher Agent ist lernfähig beziehungsweise anpassungsfähig, das heißt, dass Programm lernt aus den Ergebnissen der zuvor getätigten Entscheidung.

Als einen mobilen Agenten bezeichnet man einen Agenten der die Eigenschaft hat sich zu bewegen beziehungsweise seinen Standort zu wechseln. Dieser hat auch die Fähigkeit zu migirieren, dass bedeutet er kann selbständig den Ausführungsort wechseln und sich an die neue Infrastukur anpassen.

Der intelligente Agent besitzt die Eigenschaft zu Wissen und zu Lernen. Hinzu kommt die Möglichkeit sein Verhalten zu ändern. Programme, die Intelligentes Verhalten aufweisen, werden auch als Software Agenten bezeichnet.

Wir haben in unserem Vortrag bereits einige Beispiele zu den unterschiedlichen Agenten genannt. Diese wollen wir im Folgenden nun nocheinmal ausführen, um ein besseres Verständnis von Agenten zu geben und um zu zeigen in welchen Bereichen Agenten heutzutage schon eingesetzt werden. Wir werden uns auf die Beispiele Texterkennung, Bilderkennung und Textübersetzung beziehen.

[5] http://www.uni-magdeburg.de/iew/web/studentische_projekte/ws04/berger/schwach-stark.htm

2.1 Texterkennung

Statt dem Begriff Texterkennung wird auch die Bezeichnung 'Optische Zeichen Erkennung' (vom Englischen Optical Character Recognnition kurz OCR) verwendet. Er beschreibt die automatische Texterkennung von Bildern (Grafiken). Diese Texterkennung ist in technischer Hinsicht ein Teilbereich des Mustervergleichs. Zu Beginn wird eine Strukturerkennung durchgeführt, die die Textblöcke aus einer Grafik extrahiert und diese Textblöcke dann in Zeilen aufteilt. Diese Zeilen werden daraufhin in wiederum Einzelzeichen aufteilt. Dann beginnt erst der eigentliche Mustervergleich in dem die Einzelzeichen verglichen werden. Anwendungsbereiche für diese Art von Texterkennung sind beispielsweise das Scannen von Dokumenten oder das Schreiben auf einem Organizer. Diese Funktion ermöglicht die Wiedergewinnung von Textinformationen aus Bilddatein. Dadurch können diese Dateien dann durchsucht und weiter bearbeitet werden. Außerdem wird die Texterkennung als Blindenhilfsmittel eingesetzt, indem erkannte Texte mit einer Sprachausgabe-Software vorgelesen werden können.[6]

2.2 Bilderkennung

Die Bilderkennung, im englischem Image analysis, ist ein Teilgebiet der Mustererkennung und der Bildverarbeitung. Das Bild wird zunächst in einzelne Objekte aufgeteilt. Diesen wird daraufhin eine Beschreibung zugewiesen. Diese Funktion wird besonders bei großen Bilder- Datenbanken genutzt, da diese Bilder so automatisch getaggt beziehungsweise gelablet werden können. Bei der Erkennung von Produkten in Bildern ist diese Funktion ebenfalls hilfreich, da sie die Zuordnung zu dem passenden Artikeln automatisiert. Hinzu kommt der Bereich der Personenerkennung. Mit Hilfe der Bilderkennung können Personen bei Zugangskontrollen authenzifiziert werden. Diese Anwendung kommt immer öfter zum Einsatz.[7]

2.3 Maschinelle Übersetzung

Maschienelle Übersetzung (kurz MÜ oder MT, aus dem englischem für machine translation) ist auch unter dem Begriff 'automatische Übersetzung' bekannt. Dieser Begriff beschreibt die Funktion einen Text (Quelltext) in eine bestimmte ausgewählte Sprache zu übersetzen. Die maschienelle Übersetzung ist inzwischen in der Lage recht verständliche Übersetzung zu fertigen. Dennoch bleiben grammatikalische Probleme bestehen, so dass die vollständige Ersetzung eines Dolmetschers nicht möglich ist.[8]

2.4 Maschinen

Der Einsatz eines Agenten im maschinellen Bereich ersetzt einfache oder auch feinfühlige Handgriffe. Besonders in der Industrie sind Agenten hilfreich. Einige Produktionen sind inzwischen ohne ihren Einsatz kaum noch möglich, da die Herstellung vieler Produkte eine sehr genaue Arbeit abverlangt.

Das bekannteste Beispiel für ein solchen Agenten ist wohl der Greifarm. Dieser wird oft in der Autoindustrie, sowie in der Computerherstellung eingesetzt.

[6] http://de.wikipedia.org/wiki/Texterkennung
[7] http://de.wikipedia.org/wiki/Bilderkennung
[8] http://de.wikipedia.org/wiki/Maschinelle_%C3%9Cbersetzung

1961 kam der erste Greifarm in der Autoindustrie zum Einsatz, inzwischen beläuft sich die Anzahl auf weit mehr als eine Million. Dieser Agent hat ein hohes wirtschaftliches Potenzial und die Zahl steigt weiterhin jährlich um über circa 10 Prozent. Heutzutage wird fast jedes Auto von Industrierobotern montiert, verschweißt und lackiert.[9]

2.5 Chatbot

Ein Chatbot ist ein Dialogsystem, das menschlichen Input in Form von geschriebener Sprache analysiert und eine möglichst passende Antwort darauf liefert. Dabei kann man grob zwei Bottypen unterscheiden. So gibt es Chatbots, die nur auf bestimmte Befehle reagieren und dem Menschen zur Navigation oder Informationsbeschaffung dienen.

Die zweite Art der Chatbots ist die weit anspruchsvollere von beiden, sie setzt sich dem Ziel dem Menschen einen ebenbürtigen Gesprächspartner zu liefern oder diesen zumindest hinreichend zu simulieren.

ELIZA, 1966 von Joseph Weizenbaum entwickelt, war eines der ersten Programme dieser Art. ELIZA reagierte auf menschliche Aussagen, indem es diese in Fragen umformulierte. Auch gewisse Schlüsselworter konnten analysiert und in einen Kontext gebracht werden – so fragt ELIZA ob es einem hilft mit ihr zu reden, wenn man das Wort „unglücklich“ (engl. unhappy) erwähnt. Diese Bots sind meist so implementiert, dass sie einen text analysieren, Schlüsselworter darin finden und auf diese mithilfe einer hart gecodeten Datenbank reagieren. Dieses Vorgehen nennt man Top-Down Verfahren.

HAL ist ein weiterer Chatbot, der von Turings Beschreibung einer Child-Machine inspiriert wurde. Hier kommt ein sogenanntes Buttom-Up Verfahren zum Einsatz. Turing war der Meinung, dass man nicht versuchen sollte ein erwachsenes, fertig entwickeltes Gehirn zu simulieren. Stattdessen sollte man ein Kindergehirn entwickelt, dass die Sprache, genauso wie menschliche Kinder, erst erlernt. Sprache wird hier als Fähigkeit angesehen, die sich erst mit der Zeit und Erfahrung entwickelt und nicht einfach anhand von starren Grammatiken simuliert werden kann. So wurden HAL nur einige Lern- und Mustererkennungsalgorithmen sowie die Begierde zum Lernen mitgegeben – aber kein einziges Wort und keine Regeln und Grammatiken. Anfangs produzierte das Programm sinnloses Gebrabbel und lernte erst mit einem „Zuckerbrot und Peitsche“ Training anfangs Leerzeichen in die Endlosstrings einzubinden und Worte zusammenzustellen, später konnte es Verben und Substantive bilden und unterscheiden. Zum Zeitpunkt der Recherche soll HAL auf dem Stand eines 18 Monate alten Kindes gewesen sein.[10] [11]

2.6 Künstliche Neuronale Netze

Künstliche Neuronale Netze (kurz KNN) zeichnen sich durch ihre Lernfähigkeit aus. Das bedeutet konkret, dass Systeme entstehen können, die vorher nicht programmiert worden sondern durch ein Training erst entstanden sind. So können Probleme bewältigt werden, für die es nur sehr schwer bis hin zu unmöglich ist

[9] Künstliche Intelligenz und Robotik - Dokumentation von 3sat
[10] http://www.chatbots.org
[11] http://www.a-i.com

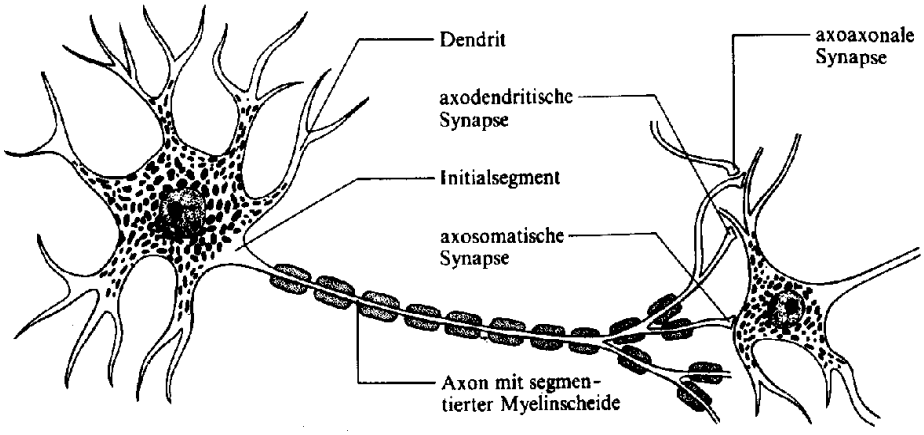


Abbildung 2: Nervenzelle,
Quelle: http://members.chello.at/thomas.knob/PSYSTOFF1.htm

auf traditionelle Art und Weise einen Algorithmus zu finden. Künstliche Neuronale Netze wurden von den biologischen Neuronalen Netzen inspiriert, wie sie höheres Leben auf der Erde aufweist. Sie befinden sich etwa im Gehirn oder anderen Nervenbahnen von Säugetieren.

Ein biologisches Neuronales Netz besteht aus mehreren einzelnen Neuronen, die erst durch ihre spezielle Verbindung zu einem leistungsfähigen Gebilde werden. Eine Nervenzelle besitzt vier wichtige Teile.

Die Dendriten sind stark verästelte Ausläufer der Neuronen, einige von ihnen nehmen die Reize von der Außenwelt oder von anderen Nervenzellen auf. Im Zellkern wird der Reiz verarbeitet und über das Axon, einer längeren Nervenfaser, an andere Zellen weitergeleitet. Am Ende des Axons können sich Verästelungen und Synapsen befinden. Die Synapse ist im Grunde der "Leerraumßwischen zwei Nervenzellen, gefüllt ist dieser Raum mit einer Flüssigkeit. Je intensiver die Nervenzelle beansprucht wird, desto mehr wird diese Flüssigkeit ionisiert und desto besser leitet sie die Reize weiter. Die Synapse ist die Schnittstelle zwischen zwei Nervenzellen. Ein Reiz wird also von den Dendriten aufgenommen, wird im Zellkern verarbeitet, geht weiter über das Axon und wird durch die Synapse an eine andere Zelle weitergeleitet.[12]

Ähnlich ist das bei den KNNs. Künstliche Neuronen werden Einheiten, Knoten oder Units genannt. Die Units sind stark vereinfachte Neuronen, aber sie können genau wie das biologische Vorbild einen Reiz bzw. ein Signal aufnehmen(Dendriten), es verarbeiten(Zelle) und weiterleiten(Axon mit Synapse). Es gibt es drei verschiedene Arten von Units. Die Input Units nehmen Signale aus der Außenwelt auf und leiten sie an die Hidden Units. Diese Hidden Units können die eingegangenen Reize untereinander oder aber an die Output Units weiterleiten. Während also die Input- und die Output Units i.A. fuer die Verarbeitung von In bzw Output sorgen, repräsentieren die Hidden Units die eigentliche Struktur des modellierten Systems.

Verbunden sind diese Unitis durch gewichtete Kanten, diese Kanten stellen

[12]http://wwwmath.uni-muenster.de/SoftComputing/lehre/material/wwwnnscript/bio.html/

den Einfluss eines Neurons auf ein anderes dar. Das "Lernenëines Künstlichen Neuronalen Netzes ist meist über die Gewichtsänderung dieser Kanten definiert. Die Änderung dieser Gewichte kommt durch das oben erwähnte Trainig zustande. Es gibt verschiedene Arten und Regeln des Trainings, grob lassen sie sich in zwei Kategorieen einordnen. Dem überwachten und dem unüberwachten Training. Beim überwachten Training wird ein Output vorgegeben, nach diesem Muster werden die Gewichte des Netzes ausgerichtet. Beim unüberwachten Lernen gibt es keinen Musteroutput, hier orientiert sich die Optimierung der Gewichte alleine durch die Eingegebenen Lernreize.

Nach einer Trainignsphase wird eine Testphase eingeleitet. In dieser überprüft man ob das Netz die gewünschte Lernleistung erbracht hat. Dabei werden die Gewichte der Kanten nicht verändert. Man verwendet entweder dieselben oder aber neue Eingaben um zu sehen, ob das Netz das richtige gelernt hat und ob es dieses "Wissenäuf andere Problemstellungen übertragen kann. Zweiteres ist wichtig, da bei einem KNN die Gefahr einer Überanpassung besteht. Das tritt auf, wenn ein KNN zu lange mit demselben (oder sehr ähnlichen) Lernmaterial trainiert wird und am Ende nur noch für genau diese Problemstellungen zu gebrauchen ist, die Generalisierung auf neue Probleme also nicht mehr stattfindet.

Anwendung finden die KNNs in vielen Bereichen. So ist die KI in vielen Spielen durch ein Künstliches Neuronales Netz umgesetzt, als Beispiel sei der CS Bot von Johannes Lampel gennant. Bei der Bildverarbeitung und Musterekennung ist es meist aufgrund der vielen Messdaten unmöglich einen hinreichenden Algorithmus zu finden, auch hier wird auf KNNs zurückgegriffen. Vor allem die Spracherkennung und Generierung profitieren von dieser Technologie. Auch bei Frühwarnsystemen wird mit ähnlich vielen Messwerten gerechnet. Künstliche Neuronale Netze fanden, vom Laien meist unbemerkt, also bereits Einzug in viele unserer modernen Technologieen und sind nicht so exotisch, wie sie den Anschein erwecken könnten. [13]

3 Multiagentensysteme

Als Multiagentensystem (kurz MAS), bezeichnet man ein System, welches aus mehreren unterschiedlich spezialisierten Einheiten beziehungsweise Agenten besteht, die kollektiv ein Problem löse. Man bezeichnet es deshalb auch als ' Kombinierte Agenten' beziehungsweise 'Kombinierte Agenten Netzte'. Diese Multiagentensysteme besitzen die selben Eigenschaften wie die Agenten (siehe oben), allerdings spielt hier der soziale Bereich und auch kooperations Fähigkeit eine besonders große Rolle. Eine unproblematische Kommunikation der einzelnen Agenten ist die Grundvoraussetzung für ein solches System.[14]

3.1 Marsroboter

Das geläufigste Beispiel für ein Multiagentensystem ist der Marsroboter. Seit Anfang 2004 suchen die beiden Roboter „Spirit“ und „Opportunity“ nach Spuren von Wasser auf dem Planeten Mars, da Wasser die Grundvoraussetzung für die Existenz von Leben ist. Sie untersuchen auf entgegengesetzten Seiten den

[13] http://www.neuronalesnetz.de/einleitung.html/
[14] http://de.wikipedia.org/wiki/Multiagentensystem

roten Planeten. Voraussichtlich sollten die Roboter nur eine Betriebsdauer von 90 Tagen tragen, doch inzwischen ist sogar eine Lebensdauer von 11 Monaten überschritten und das Projekt wurde wegen des guten Zustandes der Agenten auf 18 Monate verlängert. Durch die große Entfernung benötigt ein Befehl eine gewisse Zeit, so dass der Roboter über ein ausgeprägtes autonomes Verhalten verfügen muss. [15]

3.2 Hamburger Hafen

Ein weiteres Beispiel für ein sehr umfangreiches Multiagentensystem befindet sich im Hamburger Hafen. Wo früher noch mehrere hundert Menschen beschäftigt waren, die dort schwere körperliche Arbeit geleistet haben, ist inzwischen keine Menschenseele mehr anzutreffen. Im Hamburger Container Hafen sieht man jetzt ausschließlich Lastwagen ohne Fahrer und Kräne ohne Kranführer. Alles wird von Maschinen und Rechnern kontrolliert. Die Arbeit geht viel schneller und effizienter, denn Computer brauchen keine Pausen und machen keine Fehler. Ganz ohne Menschen funktioniert es allerdings nicht, es gibt beispielsweise noch Containerbrückenfahrer, die das nötige Feingefühl besitzen, welches nicht von einen Computer ersetzt werden kann. Dieser Fahrer belädt die Lastwagen mit Containern, sogenannte AGVs (automatic guided vehicles – auf deutsch automatisch gelenkte Fahrzeuge). Diese durchfahren dann selbständig das gesamte Gelände. Die Orientierung erfolgt über Funk mit Hilfe von circa 16.000 Transpondern die im Boden eingelassen sind. Die AGVs können sehr flexibel eingesetzt werden, sie fahren automatisch zur Tankstation, wenn der 1.200 Liter Tank aufgebraucht ist und werden dort von Robotern wieder aufgetankt. Die AGVs kommen sich nicht in die Quere, da sie miteinander kommunizieren können und aufeinander warten. Natürlich gibt es auch Transportaufträge mit unterschiedliche Prioritäten, ein Transportauftrag mit einer hohen Priorität erhält von den anderen AGVs Vorfahrt. Damit keine Person zu Schaden kommt, darf niemand das Gelände betreten, ansonsten stoppt aus Sicherheitsgründen das ganze System. Neben dem Containerbrückenfahrer gibt es einen weiteren Ort wo noch Menschen aggieren, der Terminal. Im Terminal kontrollieren Menschen über Monitor das alles Reibungslos vonstatten geht, den Rest macht die Software. Am Ende dieser Transportkette, wenn die Container auf die Lastwagen verladen sind und ihr Ziel erreicht haben, ist wieder menschliche Handarbeit gefragt. Denn dort ist der Einsatz von Maschienen zu riskant. Ein Lastwagenfahrer könnte beispielsweise verletzt werden, wenn er zu dicht an einem LKW steht.[16]

3.3 RoboCup

Der Robocup ist die Spielwiese der Forscher und Entwickler von KI und mobiler Systeme. Dabei handelt es sich um ein Turnier fuer Roboter, das jedes Jahr an wechselnden Orten stattfindet und verschiedene Wettbewerbe beinhaltet, einen grossen Teil nimmt dabei das Fussballspiel ein. Selbstverstöndlich steht dabei die Forschung und Förderung der Künstlichen Intelligenz und der mobilen Systeme, sowie die Motivation jüngerer Generationen in Sachen Technik im Fordergrund.

[15] http://www.3sat.de/nano/astuecke/85895/index.html
[16] http://www.daserste.de/wwiewissen/beitrag_dyn uid,3cpmm8ozz5b9nu8j cm.asp

Grob lässt sich der Wettbewerb erstmal in RoboCup Junior und RoboCup Senior aufteilen. Beim ersteren entwickeln und vergleichen Schüler ihre Roboter, die entweder Fussball spielen, Parkure bewöltigen oder schlicht tanzen können. Dazu werden vorgefertigte Roboterbaukästen, manchmal aber auch selbst entwickelte Maschinen verwendet.

RoboCup Senior findet auf einem etwas höheren Niveau statt, hier treten Studenten und Wissenschaftler/Innen gegeneinander an, vergleichen ihre Technologieen und tauschen Erfahrungen aus. Die Seniorliga ist etwas breiter gefächert und weist eine Reihe von Kategorieen auf.

Zwei größere wären dabei die Rescue und die Soccer Liga.

In der Rescue-Liga werden Rettungssysteme vorgestellt, in simulierter (also virtueller) Form aber auch mithilfe mobiler Agenten. Dabei wird das logistische Problem angegangen, dass nach einer Katastrophe verschiedene Rettungsdienste möglichst optimal koordiniert werden sollen. Am Gefahrengebiet müssen hingegen mobile Agenten Aufgaben bewältigen, die Menschen gar nicht oder nur schlecht verrichten können und werden damit vor besondere intellektuelle und motorische Probleme gestellt.

Die Kategorie Soccer beschöftigt sich, wie der Name erahnen lösst, mit Fussball. Hier wird nocheinmal in virtuelles und Roboterspiel unterteilt, wobei sich die Roboter nocheinmal in Größen und Form und virtuelle Simulationen in 2D und 3D Spiele unterteilen lassen.

Betrachtet man diese Einsatzgebiete und Aufgaben wird schnell klar, dass es sich auch hier um Multiagentensysteme handelt.

Ein Fussballroboter muss wissen wo er ist, wo sich seine Mitspieler befinden, die Mitspieler von Gegnern unterscheiden. Er muss wissen, wo das eigene und wo das gegnerische Tor ist und vor allem wie er handelt, wenn er einen Gegenspieler angreift oder wie er sich zu verhalten hat, wenn er vor einem Gegenspieler steht, der ihm den Ball abzunehmen versucht. Dabei dürfen die Roboter nicht direkt miteinander kommunizieren. Für all diese Aufgaben kann man einen individuellen Agenten ausmachen, die alle zusammen erst das Verhalten des Roboters möglich machen. [17]

3.4 Autonome Staubsauger

Das letzte Beispiel lässt sich inzwischen schon in einigen Haushalten finden, der Haushaltsroboter oder auch Staubsaugerroboter. Diese Roboter sind inzwischen schon ab 40 bis zu 1.200 Euro erhältlich. Je nach Preisklasse laden sich die Geräte selbständig auf oder entleeren sich von alleine. Jeder dieser Staubsaugerroboter verfügt über die Funktion ein komplettes Zimmer eigenständig zu saugen und dabei zu wissen an welcher Stelle schon gesaugt wurde. Sie erlernen wie groß das einzelnen Zimmer ist und wieviel Zeit ihre Arbeit in Anspruch nimmt. [18]

[17] http://robocup-german-open.de/

[18] http://de.wikipedia.org/wiki/Staubsaugerroboter

Abbildung 3: Nachbau des Türken, Bild aus wikipedia.de

4 Computerschach - Teil der KI Geschichte

4.1 Der Türke

Ein wichtiger und prominenter Teil der KI Geschichte ist das Computerschach. Von der breiten Masse hat es erst größere Beachtung gefunden, als es tatsächlich so weit war einen Menschen besiegen zu können. Doch die Idee der Schaffunge einer denkenden, in diesem Fall schachspielenden Maschine ist viel älter als man denken mag. Bereits im 18. Jahrhundert unternahm der ungarische Hofrat Wolfgang von Kempelen (1734-1804) den Versuch einen Schachspielenden Automaten zu konstruieren. Veranlasst wurde diesese Unternehmen von der österreichischen Kaiserin Maria Theresia. Dieser Automat wurde einer der berühmtesten in unserer Geschichte und wurde "der Türke"genannt. Dieser Name kommt von der in türkische Gewänder gekleideten, menschenhohen Figur, die Teil des Automaten war und dessen Hand mit vielerlei Geräuschen die Schachfiguren bewegte. Vor dieser Figur befand sich ein 110x75x675 cm geroßer Kasten, auf dem sich das Schachbrett befand. Vor einer jeden Vorführung wurde der Kasten geöffnet und die Zuschauer konnten eine vielzahl an sich drehenden Zahnrädern und anderen mechanischen Einzelteilen bestaunen.

Natürlich konnte diese Figur nicht wirklich Schach spielen, all die Zahnräder, Effekte und Geräusche sollten lediglich von einem kleinwüchsigen Schachspieler ablenken, der sich im inneren des Kastens befand. Viele bekannte Persönlichkeiten haben gegen den Türken Schach gespielt. So verlor Napoleon 1809 drei Partieen. Auch der amerikanische Schriftsteller Edgar Allen Poe trat gegen die Maschine an. 1854 wurde der Türke im Chinesischen Museum in Philadelphia bei einem Brand zerstört. Einen Nachbau kann man heute noch im Heinz Nixdorf Museumsforum in Paderbord besichtigen.[19]

[19] http://www.schachcomputer.at/gesch1.htm

4.2 Turings Schach

Alan Turing war es wieder, der 1947 mit Herrn Champernowne einen Schachautomatismus entwickelte, der wirklich spielen konnte. Da es zu dieser Zeit noch keine entsprechenden Computer gab, wurde der Algorithmus komplett auf dem Papier ausgeführt. Das Programm beinhaltete einen Ein-Zug-Generator mit einer Bewertungsfunktion, die über die Güte der Züge entscheiden sollte. Allerdings machte das Programm nicht in jedem Fall einen richtigen Zug, sodass Turing irgendwann zu dem Schluss kam, dass es nicht möglich sei eine schachspielende Maschine zu bauen.

Tatsächlich dauerte es noch sehr lange, bis ein Programm tatsächlich Schach auf einem höheren Level spielen konnte. Erst 1997, also ein halbes Jahrhundert später, gelang es dem Schachprogramm Fritz den derzeitigen Weltmeister Wladimir Kramnik zu schlagen.[20] [21]

4.3 Dame

Erwähnenswert in diesem Zusammenhang wäre auch das erste Dame-Programm, das 1952 von von Arthur L. Samuel entwickelt wurde. Das Programm kann als Meilenstein der KI Geschichte betrachtet werden, da es seine Züge nicht nur anhand einer Bewertung des nächsten Zuges machte, sondern auch bereits getätigte Züge in seine Überlegungen miteinbezog. Es konnte also lernen und somit nicht nur die Zukunft, sonder auch die Vergangenheit in das Spiel einbauen. Nach einer Weile war dieses Programm sogar in der Lage, einen Meisterspieler zu besiegen.[22]

5 Ethik

Der ethische Bereich schließt das Thema 'Konsequenzen durch den Einsatz von Künstlichen Agenten' mit ein. Eine offensichtliche Konsequenz ist die Abhängigkeit von der Maschine. Desweiteren wird durch die Arbeit mit Agenten, der Mensch durch eine Maschinen ersetzt, so dass zahlreiche Arbeitsplätze wegfallen. Zudem muss sich der Menschen komplett einer solchen Maschine anpassen.

Heutzutage befindet sich in fast jedem Haushalt in Deutschland ein Computer. Für viele Menschen ist ein Leben ohne Computer undenkbar. Beispielweise für die Schule oder für das Studium ist eine solche Maschine geradezu eine Voraussetzung. Auch in vielen anderen Bereichen machen die Computer einen großes Teil der Arbeit und können nicht mehr durch den Menschen ersetzt werden. Wenn heutzutage ein Rechenzentrum oder ein Server ausfällt funktioniert nichts mehr. Die Bahnen würden nicht mehr fahren oder ein Krankenhaus würde im Chaos enden, wenn kein Betriebstopp eingeleitet werden würde.

Der Verlass auf die Maschienen wird immer größer. Das Leben vieler Menschen hängt einzig und allein von Geräten ab, die ihren Körper versorgen. Eine andere Abhänigkeit, unter der ebenfalls viele Menschen leiden, ist die Sucht. In Hamburg gibt es die erste deutsche Suchtklinik, die sich ausschlielich mit der Abhängigkeit von dem Online-Rollenspiel „World of Warcraft“ (kurz: WoW) beschäftigt. Besonders nach dem Vorfall in Asien, wo ein Spieler aufgrund von

[20] http://www.schachcomputer.at/gesch2.htm
[21] http://www.schachcomputer.at/gesch3.htm
[22] http://www.zum.de/ki/

Wasserverlust gestorben ist, wächst der Druck. Wie eine Droge wirken die zahlreichen Games, die ihre Spieler vergessen lassen, dass sie in der Realität Dinge wie Nahrung, Schalf und Wasser benötigen. Ein weiteres Onlinegame, dass für Schlagzeilen dieser Art gesorgt hat, nennt sich 'Second Life'.

Ein großes Problem, dass sich durch den zunehmenden Einsatz von Maschienen entwickelt hat, ist der Verlust vieler Arbeitsplätze. Passend dazu unser Beispiel 'Hamburger Hafen'. Denn wo früher hunderte Menschen gearbeitet haben, sind jetzt nur noch wenige beschäftigt. Auch in der Autoindustrie wird immer weniger von menschlicher Hand getätigt. In dem Modul Informatik im Kontext 2 wurde ein Gegenargument vorgestellt: Durch den Einsatz von Maschinen oder Programmen werden zwar Arbeitsplätze ersetzt, aber die wenigen Menschen, die noch beschäftigt werden verdienen vergleichsweise etwas mehr Geld. Diese Veränderung beeinflusst die Wirtschaft und es können neue Arbeitsplätze entstehen. Die Frage ist nur wie lange dies noch so bleibt, denn in der Zukunft kann dies schon ganz anders aussehen. Die Zeit in denen Kassierer durch sogenannte RFID- Lesegeräte ersetzt werden, rückt immer näher, Pilotenprojekte laufen schon. Diese Geräte sind in der Lage automatisch Artikel einzulesen und abzurechnen, so dass die menschliche Hand bald überflüssig sein wird. Reinigungskräfte könnten es in der Zukunft vielleicht auch schwer haben eine Arbeit zu finden, da die Entwicklung von Haushaltsrobotern immer weiter voran geht, die die Reinigungskräfte ersetzten könnten.

Genau wie die Reinigungskraft von Menschenhand wird der Kundenkontakt zukünftig ausschließlich über Maschienen laufen. Verbale Kommunikation von Mensch zu Mensch ist ein Auslaufmodell. Es wird Zeit sich an die Maschienen zu gewöhnen. Zum Beispiel die lästigen Computerstimmen am Telefon. In Call Centern beantworten nicht nur noch Menschen die Anrufe. In erster Linie hat man inzwischen eine Software am Telefon, die einem versucht eine Lösung zu liefern oder mit einem menschlichen Mitarbeiter zu verbinden. Aber ob dieser einem dann bei technischen Problem helfen kann, ist fragwürdig. An dieser Stelle knüpft das nächste Problem an und zwar, dass der technische Fortschritt für das menschliche Verständnis zu schnell geht. Ständige Schulungen wärenerforderlich, um bei dem neusten technischen Schritt auf dem laufenden zu sein.

5.1 Können Maschinen denken?

Diese Frage ist für die Gegenwart leicht zu beantworten: sie können es nicht. Egal wie intelligent unsere Roboter- und Softwaregehilfen heutzutage auch erscheinen mögen, ihre Taten basieren auf formalisierten Regeln und mathematischen Formeln die nicht viel mit einem Denkvorgang wie wir Menschen ihn kennen gemein haben. Ein autonomer Staubsauger ist sich seiner Aufgabe nicht bewusst, selbst ein ausgereifter Autopilot eines Flugzeugs arbeitet nur ein Programm ab, das Messdaten der verschiedenen Sensoren verwertet und Entscheidungen daraus generiert.

Interessanter ist vielleicht die Frage, ob biologische Intelligenz jemals auf mechanischem Wege nachgebildet werden kann, also ob Maschinen jemals denken werden können. Betrachtet man den exponentiellen Anwachs an Rechnerleistung und bezieht noch die Möglichkeit eines Quantencomputers mit ein scheint zumindest Hardwareseitig eine Grenze noch in weiter Ferne zu sein. Fraglich bleibt also, ob sich das Konzept überhaupt umsetzen lässt oder ob das Bewusstsein oder der Denkprozess Teile beinhaltet, die sich nicht berechnen und somit

nicht nachbauen lassen.[23]

5.2 Verantwortlichkeit

Eine der wichtigsten Fragen bei der Entwicklung von KI, sowohl der starken als auch der schwachen, ist die Frage nach der Verantwortlichkeit. Maschinen und Computer übernehmen immer mehr Arbeiten, die ursprünglich von Menschen verrichtet wurden. Mit der KI dringen die Maschinen jetzt aber auch immer weiter in ein Gebiet ein, das mit einer gewissen Verantwortlichkeit verbunden ist. Das fängt bereits klein bei einem Taschenrechner an, dessen Ergebnis als unanzweifelbar gilt und geht über zu ausgefeilten Flughilfssystemen, die einem Piloten einige Entscheidungen abnehmen. Doch wer trägt die Schuld, wenn ein Taschenrechner oder ein komplexeres Computerprogramm ein falsches Ergebnis liefert? Wer ist Schuld, wenn ein Autopilot oder sonstige Flughilfsmechanismen versagen und zu einem Absturz führen?

Das sind Fragen, die sich nur sehr schwer beantworten lassen. Sicher ist nur, dass ein Computer nicht über das Bewusstsein verfüg für einen Fehler zur Verantwortung gezogen zu werden. Dieser muss zumindest bei unserer heutigen Technologie beim Menschen gesucht werden. Bei komplexen Projekten, welches KI Projekte im Allgemeinen immer sind, arbeiten eine vielzahl an Menschen teils sogar über Generationen hinweg zusammen an einem Stück Software. Selbst wenn ein Fehler also auf die Software zurückgeführt werden kann wird einem schnell klar, dass dabei die Auffindung einer verantwortlichen Person immernoch ein sehr schwieriges Unterfangen ist.

Fraglich ist ebenso, ob man die Verantwortung überhaupt abgeben sollte oder möchte. Sollte es Ziel menschlicher Anstrengungen sein die eigene Existenz auf eine Zuschauerrolle zu reduzieren, sich selbst gewissermaßen zu entmündigen? Desweiteren sollte man sich fragen, wieso eine überlegenere Intelligenzform auf Dauer dem Menschen, aus ihrer Sicht einem minder intellektuellen Wesen dienen sollte. Wäre der Mensch dazu bereit seinem eigenen Werk dieselben Rechte zuzugestehen wie sich selbst? All das sind Dinge, die man bei der Erschaffung einer solchen Technologie überlegen muss, auch wenn letzendlich keine eindeutige Antwort gefunden werden kann. Den Menschen und seine intellektuellen Leistungen aber als den Gipfel der Evolution zu betrachten wird sicherlich irgendwann zu einer Stagnation der Entwicklung führen.[24]

[23] www.wikipedia.de/

[24] Die Ethik von Agenten, Günter Hellbardt, Informatik-Spektrum 19:87-90(1996) Springer-Verlag

RFID- Radio Frequency IDentification

Kristina Fuhrmann, Julia Rehm

1 Einführung

RFID steht für „**R**adio **F**requency **Id**entification“ und benennt die kontaktlose Identifizierung und Lokalisierung von Objekten via (elektro)magnetischer Wellen. Ein RFID-System besteht aus einem Transponder, der ein Objekt kennzeichnet und die Anfrage eines Lesegerätes über Funk beantwortet, wodurch die Kommunikation ohne Kontakt stattfinden kann, dem Objekt und dem Lesegerät, dass die Daten abfragt und bearbeitet.
Die Technik kann in den unterschiedlichsten Bereichen Anwendung finden. Implantate speichern wichtige Daten zu unseren Haustieren, während Mautsysteme Positionen und damit Zeitkontrollen ausgeben. Die Logistik nutzt RFID zum Verwalten und Rückverfolgen ihrer Waren. Im Verkauf bieten Tags Sicherheit vor Diebstahl. Das System verdrängt den Barcode, birgt jedoch auch einige ethische Fragen, die vor dem Einsatz geklärt werden müssen.

2 Szenario

Beginnen wir mit folgendem Szenario:

Ein Einkauf ohne RFID
Jutta möchte ein Glas Milch trinken, beim Blick in den Kühlschrank muss sie feststellen, dass sie keine mehr hat. Als ihre Mitbewohnerin nach Hause kommt klärt sich die Situation: Der Liter Milch wurde zu Milchreis verarbeitet.

Der Einkaufszettel ist geschrieben und Jutta macht sich auf den Weg zum Supermarkt, meist zu Fuß, weil es keine Parkplätze gibt.

Ein Einkauf mit RFID
Jutta möchte Milch trinken. Ihr RFID-Kühlschrank, hat automatisch neue bestellt, die geliefert wurde, als der letzte Liter angebrochen wurde. Jutta geht einkaufen, um Produkte anzuschauen, die ihr der Kühlschrank vorgeschlagen hat.

Die Einkaufsliste ist schnell auf einem RFID-Schlüsselanhänger gespeichert und Jutta macht sich auf den Weg zum Supermarkt.

Im Laden packt Jutta den Wagen voll mit Waren, die nicht auf ihrem Zettel stehen. Ihr Lieblings-Käse ist nicht mehr vorrätig, die Alternative hat nur sehr klein gedruckte Nährwertangaben und der Verpackungsdesigner berücksichtigt nicht alle Angaben.	Der RFID-Einkaufswagen liest den Tag und führt Jutta über einen Monitor zu den Waren. Artikelinformationen und passende Werbung sieht sie auch auf dem Bildschirm. Mitarbeiter erhalten einen Hinweis, wenn Artikel ausgehen.
An der Kasse muss Jutta anstehen. Die Kassiererin hält den Strichcode der Produkte an einen Laserscanner, alle einzeln. Einige Male muss sie den Barcode manuell eintippen, oder Artikel stornieren, weil sie sie doppelt gescannt hat. Als Jutta endlich bezahlen kann, merkt sie, dass sie kein Bargeld dabei hat, aber der Supermarkt akzeptiert auch ihre EC-Karte.	Kassen und Kassierer gibt es hier nicht mehr. Der Einkaufswagen hat die Daten der eingekauften Produkte gespeichert, aber auch ohne Wagen würden die Waren von einem Lesegerät ausgescannt werden und der anfallende Betrag automatisch von ihrem Konto abgebucht werden. Barzahlung ist an einem Automaten möglich der separat angesteuert werden kann.
Zuhause packt sie alle Einkäufe in den Kühlschrank und hofft, dass ihr beim nächsten Mal nichts fehlt.	Zuhause liest der Kühlschrank die neuen Waren ein und fragt bei Verzehr ab, ob die Artikel regelmäßig bestellt werden sollen.

3 Geschichte

Um der Historie des RFID-Systems folgen zu können bedarf es Kenntnissen über Ereignisse die womöglich einige Zeit vor dem tatsächlichen Grundstein liegen, daher klären wir zunächst einige Begrifflichkeiten und ordnen diese geschichtlich ein, um einen besseren Überblick geben zu können.

3.1 Radartechnologie

Radar stand ursprünglich für **R**adio **A**irkraft **D**etection **a**nd **R**anking, heute für **Ra**dio **D**etection **a**nd **R**anking, was Funkortung und -abstandsmessung bedeutet.
1886 entdeckte Heinrich Hertz, der am Beweis der Existenz von elektromagnetischen Wellen arbeitete, dass Metall Radiowellen reflektiert.
Christian Hülsemeyer experimentierte 1904 mit Radiowellen und entwickelte das „Telemobiloskop“, mit dem man die Laufzeit der Signale zu einem metallischen Gegenstand messen konnte. Noch im selben Jahr meldete er sein Verfahren zum Patent an.
1919 ließ sich auch Sir Robert Alexander Watson-Watt ein Patent eintragen, das, zur Ortung von Objekten mittels Radiowellen.
Erst 1930 wurden erste Radargeräte gebaut, die das Problem der Entfernungs-

messung lösten.

Radargeräte senden ein Primärsignal, gebündelte elektromagnetische Wellen, und erhalten ein Echo von den metallischen Objekten. Dieses Sekundärsignal wird von dem Radar ausgewertet und kann beispielsweise folgende Informationen liefern:

- Winkel oder Richtung zum Objekt
- Entfernung zum Objekt
- die Relativbewegung
- Absolutgeschwindigkeit oder zurückgelegte Strecke eines Objekts
- Objektumrisse (Planetenerkundung, Flugzeugzuordnung)

Wir unterscheiden weiter in Primär- und Sekundärradar. [Wiki]

3.1.1 Primärradar

Eine Primärradaranlage sendet einen Hochfrequenzimpuls und errechnet sein Ergebnis aus dem empfangenen Echo, welche das angepeilte Objekt durch Reflexion zurückwirft (was dem Prinzip der Fledermaus gleicht).
Dabei ist das Objekt, in Abgrenzung zum Sekundärradar passiv, reflektiert also lediglich das eintreffende Signal ohne eigene Informationen aufzumodulieren. Einsatz findet dieses Radar zum Beispiel bei Geschwindigkeitskontrollen im Straßenverkehr, als auch bei der Luftraumüberwachung, wobei es besonders wichtig ist ein System zu haben, das nicht auf Rücksignale angewiesen ist. Allerdings müssen sie leistungsstärker sein als Sekundärradarsysteme, um die gleiche Reichweite zu erzielen. [Wiki]

3.1.2 Sekundärradar

Im Gegensatz zum Primärradar arbeitet ein Sekundärradar mit aktiven Zielen, die ein eingehendes Signal, via Interrogator, einem Abfragegerät, gesendet, mit einem Datensignal beantworten.
So können beispielsweise Identifizierungen vorgenommen werden. Zudem hat dieses System den Vorteil eine höhere Reichweite erzielen zu können. [Wiki]
Sollte jedoch die Frequenz eines der Geräte geändert werden, könnten die Signale nicht mehr genutzt werden.

3.2 Harry Stockman

Die Grundlage für RFID wurde im Oktober 1948 mit der Veröffentlichung „Communication by Means of Reflected Power“ von Harry Stockman gelegt. Als Leiter der Kommunikationstechnik- Abteilung der damals neu gegründeten Cambridge Field Station (CFS) der US Army Air Force, hatte er freien Zugang zu Gerätschaften und allen Forschungsunterlagen. [Wiki, Rosol]
Er widmete sich zunächst der Gehirnwellen-Forschung, wie schon sein ehemaliger Lehrer Leon Chaffee, der 1934 Mini-Spulen in Affenhirne implantierte, um deren Nervenzellen zu steuern. Durch „microwave and infrared reception of

the radiation“ versuchte Stockman Forschungsgelder der CFS genehmigt zu bekommen. Sein Antrag wurde von der gerade eigenständig erhobenen Air Force abgelehnt, so experimentierte er in der telereflektorischen Kommunikation weiter. 1946 kam ihm die Idee zu einer neuen Kommunikationsmethode, die auf Radartechnologie basieren würde- „Reflected Power Communication“.

Bisher basierte Kommunikation auf dem Sender-/Empfängerprinzip (a), dabei gibt es eine Information sendende (TRM) Station und eine empfangende (RCV) Einheit, die ein weit gestreutes Signal (Intelligence) erhält. Ein Austausch über eine größere Distanz verläuft mit Zwischenstationen. Stockmans Methode sah vor, die Trägerwellen (Carrier) mittels hochgerichteter Reflektoren zu bündeln und mit einem aufmodulierten Signal weiterzuleiten (Point-to-Point).

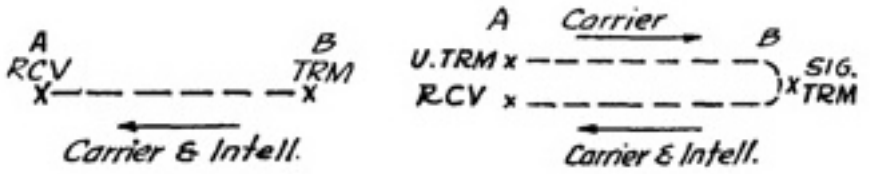
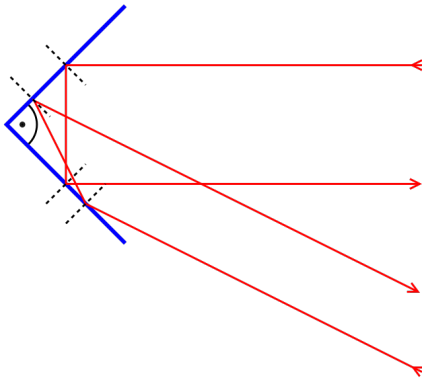


Abbildung 1: a) Sender-/Empfängerprinzip und b) Stockman's Kommunikation

Der Vorteil, neben der höheren Reichweite, die durch Anwendung von Mikrowellen erreicht wurde, war die Abhörsicherheit, denn das Abrufen der Signale implizierte den direkten Zugriff auf den Reflexionsstrahl, der nicht unbemerkt bliebe.
Bislang wurden Mikrowellen und Reflektoren eingesetzt um Metall zu finden, es diente dazu den Feind vom Freund zu unterscheiden.

Wie zuvor erwähnt konnte Stockman sich an dem Fundus der Kriegsforschung bedienen und entschied sich für Winkelreflektoren. [Rosol]
„A corner reflector has the important proberty that a ray, which enters the corner, will experience a reflection from each of the surfaces, and will return in the direction from which it came.“
Weiter erklärt er in diesem Abschnitt seines Berichtes, dass die Winkelreflektoren daher so gut zur Kanalbildung geeignet seien, weil sie die eintreffende Strahlung in dem Trichter so oft spiegeln und die Signale so verstärken, dass die ausgehende Strahlung optimal zu verwenden sei. [Stockman]
Er begann ein Aussenprojekt, für das er die Reflektorapparatur „tripple turret reflector“ herstellte. Ein drehbarer Turm, aufgebaut aus drei voneinander abgekoppelten Aufhängungen, ausgestattet mit je vier Winkelreflektoren, wurde von einem Motor angetrieben, sodass sich die Turrets einzeln drehen konnten. Abzulesen waren beim Messen drei verschiedene Frequenzen, die sich daraus ergaben, dass jedes Turret geändert werden konnte, sich so die Winkel änderten und sie den Trägerwellen unterschiedliche Signale aufmodulierten.
Das Ergebnis sind drei Frequenzen, die sich daraus ergeben, dass jeder Reflektor



Ein Signal trifft auf den Reflektor mit einer bestimmten Frequenz ein und wird zurückgeworfen. Aus diesen beiden Frequenzen resultiert dann das Ergebnis. Die unterschiedlichen Eintrittswinkel spielen dabei eine bedeutende Rolle, denn im Innenwinkel wird das Signal am stärksten zurückgeworfen.

Abbildung 2: Ein Winkelreflektor mit zwei Signalen

das Signal, auf Grund der Umdrehungsgeschwindigkeit und des Eintrittswinkels, individuell zurückwirft. An einem Beispiel: Die Reflektoren bewegen sich mit 8, 14 und 20 cps (counts per sec.), dann ergibt sich daraus die maximale Auslenkung von 24, 56 und 80 Hz, wegen der vier Reflektoren pro Turret.
Dabei ist es irrelevant in welcher Reihenfolge die Werte stehen, weil der Empfänger den eindeutigen Code ausgibt, sie mussten nur 2 Hz auseinander liegen und in dem Bereich von 15 und 85 Hz.

$$\frac{35!}{3!(35-3)!}$$

Hier ergeben sich, in Stockmans Number-Identification-Taget-System (NIT), 6545! Codierungen. Dies könnte die rudimentäre Form eines passiven RFID-Systems sein- ein Backscatter. [Rosol]

Die Forschungen die zur Entwicklung von RFID führten, fanden größtenteils gleichzeitig statt. Während des Zweiten Weltkrieges wurde die erste Anwendung eingesetzt. Es handelt sich um ein Sekundärrader, das in Flugzeugen und Panzern eingesetzt, zur Freund-Feind-Erkennung genutzt wurde.

3.3 Freund-Feind-Erkennung (IFF)

Das IFF-System basiert auf dem Sekundärradar. Ein Interrogator sendet auf einer bestimmten Frequenz ein Signal an einen Transponder, der mit einem kryptografischen Schlüssel antwortet, um sich zu identifizieren. Stimmen die Schlüssel beider Stationen überein wird das Objekt als „Freund“ erkannt. [Wiki]

3.3.1 Deutschland

Die Idee der Freund-Feind-Erkennung geht zurück auf den Zweiten Weltkrieg. Britische Truppen entdeckten, dass sich deutsche Flieger synchron überschlugen. Mit den gegebenen Informationen ist leicht zu erkennen, dass die Flugzeuge auf einen Befehl ihrer Abfrageeinheit antworteten, indem sie die Polarisierung ihrer Reflexionen änderten. Seit 1938 tüftelten die Deutschen an einem Gerät, dass aktiv arbeiten sollte. Die Musterversion „Stichling“ brachte 1940 die Weiterführung „Zwilling“ hervor, auf der wiederum „Neuling“ basiert, das eine

Bord-zu-Bord-Abfrage vorsah. Die Systeme arbeiten mit einer Morsekennung, die aus zwei identischen Schlüsseln bestand. Der Funker hörte die auf die Trägerfrequenz aufmodulierten Töne und identifizierte Objekte mit gleichem Schlüssel als „Freunde“. [Rosol]

3.3.2 England

Sir Robert Alexander Watson-Watt, der sich bereits mit dem Radar-System einen Namen gemacht hatte, entwickelte, ebenfalls im Zweiten Weltkrieg, eine horizontal polarisierenden Dipol, dessen Pole bei Abfrage zusammengeschaltet wurden. Aktiviert sendete das System auf der Frequenz des Chain Home, einer Radar-Stationen-Kette, um das Objekt orten zu können.
1940 wurde das erste aktive IFF-System, Mark I, eingesetzt. Die Empfangseinheit sendete ein Echo an den Sender zurück, jedoch musste die Frequenz fein eingestellt werden. Die Weiterentwicklung Mk III hatte den Vorteil eines eigenen Frequenzbereiches und ist vom Prinzip ein Sekundärradar mit Interrogator und Antwortcode, jedoch konnte diese Kennung auch vom Gegner empfangen werden.

Bei dem IFF-System könnte sich um eine Vorform des aktiven RFID-Systems handeln. [Rosol]

Es sei nun noch erwähnt, dass Donald Brewer Harris, Stockmans „Reflected Power Communication“ 1952 ausarbeitete, allerdings um ein Funkübertragungssystem mit passiven Responder zu erfinden. Es sollte ein Batterieloses Prinzip zum Sprachverkehr entstehen, das ebenfalls mit Sender und zu aktivierendem Empfänger arbeitete.
Der Forschungen an diesen sehr ähnlichen Systemen verdanken wir die heutige RFID-Technik.

4 Technik

4.1 Transponder

Der Begriff Transponder setzt sich aus den Wörtern Transmitter (z. Dt. Funksender) und Responder (z. Dt. der Antwortende) zusammen, was soviel bedeutet wie „Antwortsender“.
Das Prinzip des Aufbaus eines Transponders, Tags oder Chips ist einheitlich. Er besteht aus einem Mikrochip, der als Speicher für Informationen dient, einer Antenne, meist eine Spule (magnetisch) oder einem Dipol (elektromagnetisch) und einem Träger. Die Etiketten oder Smart Labels sind passive Transponder, sie verfügen über keine eigene Stromversorgung und speichern die Daten auf dem eingebauten Mikrochip. Ein entsprechendes Lesegerät sendet ein Signal an den Transponder, dessen Antenne die Energie aus dem elektromagnetischem Feld als Induktionsstrom an einen Kondensator weiterleitet und diesen so auflädt. Die erhaltene Energie nutzt der Tag, um die angeforderten Informationen an den Reader zu senden. [Improve, Journal, Wiki]

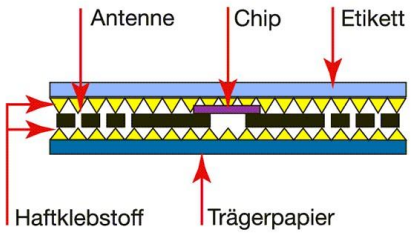


Abbildung 3: Etikett mit Inlay

Die einfachste Form ist ein Inlay, dabei sind ein Mikrochip und eine Antenne auf eine Folie geklebt. Ein Inlay findet bei weiteren Formen Verwendung, z.B bei einem Etiketten-Transponder. Hier ist das Inlay unter einem Etikett mit Beschriftung befestigt. [Journal, Schreiner]

Neben der passiven Variante gibt es aktive Transponder mit einer eigenen Stromversorgung, die so selbstständig Informationen aussenden, die zudem verschlüsselt werden können. Die Batterie versorgt den Mikrochip immer dann mit Energie, wenn von einem Lesegerät die entsprechende Aufforderung durch ein Signal eingeht.
Diese Art von Chip hat den Vorteil gegenüber der passiven, dass höhere Reichweiten erreicht werden können. Zusätzlich können die Transponder mit Sensoren ausgestattet werden, um Parameter wie die Temperatur zu überwachen. Jedoch sind die Kosten und der Umfang der Einheit, auf Grund der teureren Ausstattung, höher. Ein Einsatz lohnt sich daher eher an fest installierten oder permanent einzusetzenden Objekten, bei denen auch ein größerer Tag nicht stört.

Semi-passive Chips vereinigen beide Varianten miteinander. Daraus entsteht ein Transponder, mit einer kleinen, gedruckten Batterieeinheit, die nur den Mikrochip mit Energie versorgt und platzsparend untergebracht werden kann, der eine hohe Reichweite erreichen kann. [Improve, Journal, Marktplatz, Wiki]

Es gibt drei Speicherarten für Transponder. Die einfachste Lösung, bietet keinen zusätzlichen Platz, das heißt es wird lediglich die Basisinformation übermittelt, wie z.B. die Produktnummer. Eine andere Klasse stellt einen einmalig beschreibbaren Speicher zur Verfügung. Hier könnten weitere Produktinformationen gesichert werden. Die letzte Art ist ein permanent wiederbeschreibbarer Chip, der einen großen Speicher eingebaut hat. [Improve]

4.1.1 Transponderformen

Abhängig vom Einsatzgebiet fallen Größe und Qualität der Tags aus. Während Implantate möglichst klein sein und eine höhe Lebensdauer aufweisen sollten, ist die Größe eher irrelevant bei der Identifizierung von Containern und die Haltbarkeit ein weniger wichtiger Aspekt bei Etiketten auf unempfindlichen Lebensmitteln.
RFID-Tags können in vielen Formen hergestellt werden, so dass man oft nicht erkennen kann, dass man es mit Empfängern zu tun hat. In der Logistik können Kisten beispielsweise mit Nägeln oder Heftzwecken gespickt werden in denen ein Transponder eingesetzt ist.
Chipkarten gewähren mit Funkabfrage Zutritt, das Auto verriegelt die Türen per Knopfdruck auf die Fernbedienung und deaktiviert die Wegfahrsperre nur

mit dem passenden Transponder, die Parkmünze wird mit RFID freigeschaltet und öffentliche Verkehrsmittel setzen die Technik für ihre Fahrkarten ein, ohne dass die Nutzer darüber informiert werden.

Abbildung 4: Implantat

Etwas bekannter ist der Ohrchip bei der Tieridentifikation oder Implantate bei Hunden, aber auch Armbänder oder Anhänger sind verbreitet. Ein durchschnittlicher RFID-Chip hat eine ungefähre Lebensdauer von zehn Jahren. Transponder fallen je nach der Größe ihrer Antenne aus, die die Erreichbarkeit ausmacht. Eine hohe Reichweitefordert somit einen großen Empfänger.

Auch das Magnetfeld hat Einfluss auf die Reichweite, je nachdem ob ein magnetisch erzeugtes Nahfeld oder ein elektromagnetisches Fernfeld besteht.
Weitere Unterscheidungsmerkmale, neben der Lesereichweite, dem Speicherplatz, der Größe und der Lebensdauer, sind das Anwendungsgebiet, die Taktfrequenz, die Übertragungsrate, sowie die Kosten.
Zur Zeit liegen diese auf Grund der Unschätzbarkeit zwischen 5 Cent und einem Euro.
Durch die, meist bei passiven Einheiten, niedrigen Preise entfallen auch Wartungsarbeiten an den Transpondern. Sie werden einfach ersetzt. [Journal]

4.2 Lesegerät

Der Reader eines RFID-Systems ist sich wie ein Computer vorzustellen. Er ist die Schnittstelle an der gearbeitet wird. Ein Lesegerät kann bis zu 400 RFID Chips pro Sekunde auslesen.

Abbildung 5: Etikett mit Inlay

Die Einheit sendet ein elektromagnetisches Feld aus, das Tags anspricht.
Der Sender fungiert teilweise auch als Energiequelle, denn die Funkwellen müssen ausreichend sein, um auch den Transponder mit Strom zu versorgen. Der so aktivierte Mikrochip decodiert den gesendeten Befehl und sendet die Antwort. Das Lesegerät reagiert auf die Feldschwächung und zieht die angeforderten Informationen daraus.

Schreibgeräte, die auch Lesegeräte gleichermaßen sein können, ermöglichen das

Aktualisieren der gespeicherten Daten auf den Transpondern. [Journal, Folie, Wiki]

4.3 RFID-System

Der Datenaustausch eines RFID-Systems, basiert auf immer dem gleichen Prinzip. Das Lesegerät erzeugt ein elektromagnetisches Feld, das von der Transponder-Antenne empfangen und an den Mikrochip geleitet wird. Der Chip sendet seine Informationen, z.B. eine eindeutige Seriennummer, über das bestehende (elektro)magnetische Feld zurück an das Lesegerät. Dabei verändert der Empfänger das elektronische Feld, der Sender wertet die Änderungen als Antwort aus. Die gesamten Daten können mit dem Modulationsverfahren in eine höhere Frequenzlage gebracht werden. [Journal, Wiki]

4.3.1 Datenübertragung

Es gibt zwei Verfahren zum Datenaustausch bei RFID-Systemen.
Das Halb- und Vollduplexverfahren unterscheiden sich grundsätzlich in der Art der Energieübertragung. Während beim Halbduplexverfahren Daten nur abwechselnd zwischen Sender und Empfänger ausgetauscht werden, beinhaltet die Vollduplex einen gleichzeitigen Tausch.
Die Lastmodulation findet Anwendung bei dieser Variante. Dabei antwortet der Transponder auf den Empfang von Magnetstrahlen, indem er dem Lesegerät die nötige Energie entzieht, welche dieses ausgleicht und die entstehende Differenz registriert. Eine andere Möglichkeit die Informationen des Transponders zu übermitteln, bietet die Messung der reflektierten Mikrowellen, der modulierte Rückstrahlquerschnitt oder allgemeiner „Backscatting“, der wiederum in sub- und anharmonisch unterteilt wird.
Da das Halbduplexverfahren eine Übertragung der Energie vorhersieht, müssen die Transponder mit einem Kondensator ausgestattet sein, der diese Energie kurzzeitig speichert.

Der Ablauf der Datenübertragung benötigt in der Theorie lediglich einen Bruchteil einer Sekunde, jedoch können einige Faktoren zu einer Störung des Systems beitragen, die beispielsweise die Distanz verringert.
Störsignale entstehen bei aufeinander liegenden Chips, Flüssigkeiten oder Metallen, weil sie Reflexionen auslösen oder das Feld dämpfen. Auch Produkte mit einer hohen Dichte, wie Nudeln, können einen Störfaktor darstellen, wenn der Tag direkt an der Ware angebracht ist, allerdings ist die Lösung für dieses Problem simpel und nur theoretischer Natur, da schon ein Anbringen des Chips im rechten Winkel Erfolg verspricht. [Journal]

4.4 Kosten

Die Gesamtkosten für ein RFID-System setzen sich aus den Einzelbeträgen für alle Transponder, genügend Lesegerät, um die zurückzulegenden Wege zu verfolgen und den benötigten Datenbanken zusammen. [Journal]

4.4.1 Kostenbeispiel

Ein Kaufhaus müsste zum Umstellen, des funktionierenden Systems, zunächst investieren. So fallen einmalige Kosten für mehrere Lesegeräte an, die über die gesamte zu bewachende Fläche verteilt stehen müssten, für Kasseneinheiten die mit RFID ausgestattet sind und für die Datenbank, die benötigt wird. Hierbei entstehen Personalkosten für die Einrichtung und die Administration, sowie die Schulung des Kassenpersonals.
Zudem fallen wiederkehrende Beträge für die Transponder an, die in diesem Beispiel Smart-Tags, kleine Etiketten, die nach Gebrauch weggeworfen werden, wären.
Konzerne können die tatsächlichen Anschaffungskosten zur Zeit nicht kalkulieren, weil die Preise wegen der geringen Auflagen noch verfälscht dargestellt werden, hohe Abnahmen die Kosten drücken und die Rabatte, die zur Beschleunigung der Einführung gewährt werden, eine Berechnung erschweren. [Journal]

4.5 Frequenzen

- **Übersicht über verwendete Frequenzen und ihre Reichweiten**
  - 125 kHz/ 134 kHz — 1cm - 0,5cm
  - 13.56 MHz — 1cm - 0,5cm
  - 2,4/2,5 und 5,8 GHz — 0,5m - 6m
  - 869 MHz/ 915 MHz — einige Meter
  - 2459 MHz — bis zu mehreren hundert Metern
  - Grundsätzlich sind Entfernung bis zu einem Kilometer möglich [Folie, Wiki]

Die niedrigen Frequenzen werden bei der RFID-Technologie am häufigsten eingesetzt, weil die Herstellung der Transponder für diese Systeme am preisgünstigsten ist.
Obwohl diese Chips nur eine geringe Reichweite überbrücken können, werden sie viel genutzt, weil die Störfaktoren bei diesen Frequenzen seltener auftauchen, beispielsweise können die Tags auch auf Metall angebracht werden und sind Wetter unempfindlich. Der Bereich bei 13.56 MHz ermöglicht eine schnelle Datenübertragung und bietet eine Signalverschlüsselung.
Die Frequenzen im GHz-Bereich sind Mikrowellen mit sehr höher Lesegeschwindigkeit- allerdings nur für semi-passive Transponder zu nutzen.
Höhere Frequenzen bieten zwar auch hohe Raten und Reichweiten, sind allerdings teurer zu unterhalten und nicht für den Massengebrauch geeignet. Sie werden nicht an Wegwerfartikeln angebracht, sondern eher für langlebige Produkte, wie Mautsysteme, verwendet. [Journal, Wiki]

4.6 Verschlüsselung

Um auch auf kleinem Raum mehrere Transponder und Lesegeräte installieren zu können muss eine Nachbarschaft gut abgestimmt werden. Einem Reader werden daher beieinander liegende Kanäle zugeteilt um Kollisionen zu vermeiden, wenn Tags gleichzeitig senden. RFID-Chips senden ihre Daten aber nicht zwangsläufig im Klartext, sie können auch codiert geschickt werden oder nur bestimmte

Speicherregionen freigeben. Die Modulation oder Keying ist ein Verfahren um digitale Signale über analoge Leitungen übertragen zu können.

- Amplitude Shift Keying
- Frequency Shift Keying
- Phase Shift Keying

Das Encoding, also die Zeichenkodierung und das Anpassen wiederum basiert auf verschiedenen Verfahren, dabei sind zu nennen:

- Biphase-Mark-Code
- Pulsphasenmodulation und RZ-Code
- Manchester-Code
- Miller-Code [Wiki]

5 Entwicklung

Nachdem die Grundsteine für RFID nun gelegt waren entwickelte sich die Technik schnell weiter.
Als eine der ersten eingesetzten passiven Systeme gilt die „Car Identification“ von Siemens aus dem Jahr 1960, mit dem es möglich war Eisenbahnwagen und Autoteile zu identifizieren. In den verschiedenen Bauschritten bot sich eine Eindeutigkeit der Teile an, weshalb sie mit Hohlraumresonatoren ausgestattet waren, die Daten über 12Bit abdeckten und über eine lineare Frequenzrampe abgefragt wurden.
Das erste kommerzielle System wurde ab 1970 zum Verkauf angeboten- ein Warensicherungssystem. Die Transponder hatten lediglich 1Bit Speicherplatz und sendeten per Induktionsübertragung ein Signal an das Lesegerät, um einen Alarm auszulösen.
1975 wurde der erste passive Backscatter vorgestellt, dessen Bauart noch heute aktiv ist.
Für die Landwirtschaft wurde RFID 1979 bedeutend, als die Tieridentifikation mit Ohrchips oder Ringen auf den Markt kam.
Durch die gute Resonanz wurde die Anwendung stetig weiterentwickelt, bis 1980 die Mautsysteme, speziell in Norwegen als auch in Amerika, eingeführt wurden, wo sie sich bis in die USA (1990) ausbreiteten.
Weiterhin wurde RFID für Zutrittskontrollen, Ausfahrtsysteme, Pässe, Schlösser oder Wegfahrsperren eingesetzt.
Von 1999 bis 2003 wurde die Auto-ID, zu der RFID, Barcode, Smart Label oder Chipkarten gehören, als globaler Standard zur Warenidentifikation durchgesetzt, die Forschungsergebnisse liegen EPCglobal Inc. vor.
Seit 2006 gibt es temperaturempfindliche Tags in metallischen Bauteilen, die während des Fertigungsprozesses eingegossen werde, das Verfahren wird weiter erforscht. [Wiki]

6 Abgrenzung zu anderen Technologien

Da RFID auf der Weiterentwicklung und Kopplung verschiedener anderer Systeme basiert, stellt man einige Ähnlichkeiten zu bestehenden Technologien fest. Dabei sind das Radar und die Funkwellentechnik zu nennen, sowie die Chipkarte und das Barcode-Prinzip, die sehr ähnliche Verfahren sind.

Radar Das Radar funktioniert mit der Reflexion von Funkwellen, dem sogenannten Echo. Das System ist passiv, da die Empfänger nur als Zielobjekt dienen, um Informationen zu übermitteln.
Im Gegensatz dazu kann RFID auch aktive Transponder haben, die ein eintreffendes Funksignal beantworten.

Funk Beim Funken, kann jeder Teilnehmer zu beliebiger Zeit eine Anfrage senden und Antworten empfangen. RFID hingegen ist ein Serverdienst, bei dem ein Rücksignal übertragen wird, wenn ein Reader danach fragt, ansonsten verhält es sich passiv.

Chipkarten Eine Mikroprozessor Chipkarte verfolgt das gleiche Prinzip wie die RFID-Technik, allerdings benötigt eine Chipkarte direkten Kontakt zum Lesegerät. RFID bietet somit Vorteile durch kontaktloses Lesen und dadurch Schnelligkeit und die Pulkerkennung, die später erläutert wird. [Seminar]

Barcode
Ein Barcode ist eine optoelektronisch lesbare Schrift mit verschieden breiten Strichen, die binäre Symbole codieren. Der bekannteste Code ist der EAN- European Article Number- mit meistens 13 Zeichen, davon eine Prüfziffer aus dem Zeichenvorrat 0-9.

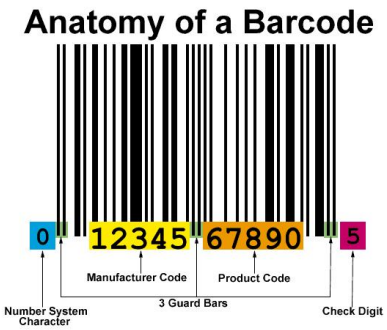


Abbildung 6: Barcode-Aufbau

Bei RFID können ebenso Seriennummern auf einem Mikrochip gespeichert werden, die Methode bietet aber noch mehr Möglichkeiten, Chips sind somit nicht nur lesbar, wie Barcodes, sondern auch beschreibbar.
Beide Verfahren bieten den Vorteil, dass Daten codiert und gelesen werden können, wodurch der Artikel nur einmal beschrieben werden muss und danach bei Eingabe aus einer Datenbank aufgerufen werden kann.

Ein Barcode muss in geringer Entfernung an ein Lesegerät gehalten werden und zählt als aktiv, weil er immer abrufbereit ist wohingegen ein Transponder erst von einem Reader angesprochen werden muss, aber auch größere Reichweiten überbrücken kann.

Inzwischen kann man Tags herstellen, die wenig empfindlich reagieren, was bedeutet, dass sie auch bei Verschmutzung oder Beschädigung ohne Störung funktionieren.

Da RFID eine sehr viel umfangreichere Technologie darstellt, weil sie Informationen sehr genau wiedergeben kann (komplette Handelskette im Gegensatz zu Hersteller und Warenart), ist es schwer mit dem Barcode zu vergleichen, zumal die Datenschutzfrage aufkommt, wenn eine solche Menge an Daten abgefragt werden kann. [Journal, Wiki, Improve]

7 Anwendungsbeispiele

7.1 Logistik

„Wenn dann die Waren und Produkte den Hersteller verlassen, wird dies von einem Lesegerät erfasst, so dass der Hersteller genau weiß, wann welches seiner Produkte die Fabrikationshalle verlassen hat. Auf den Transportwägen können sich dann die nächsten Lesegeräte befinden, die wiederum protokollieren, wann die Waren verladen wurden und wann sie dann zum Beispiel beim nächsten Zwischenhändler angekommen sind. Diesem Zwischenhändler müssen zuvor natürlich die EPCs mitgeteilt werden, denn dann kann dieser die Produkte mit seinem Lesegerät identifizieren. Der Zwischenhändler kann dann die Waren und Produkte wiederum auf eine Reise schicken, wobei auch er nun immer die Kontrolle über den Aufenthaltsort der Ware hat und wenn der Endhändler ebenfalls mit einem RFID-System ausgestattet ist, dann können die ausgelieferten Produkte automatisch als "verkauftïn der Datenbank registriert werden. Der große Nutzen, der sich aus solch einem System ergibt, ist die ständige Kontrolle, die sowohl Produzent, Zwischenhändler als auch Endhändler besitzen, denn wenn die Angaben in der Datenbank zum Beispiel nicht mit den von den Lesegeräten erfassten Daten übereinstimmen, ist klar, dass auf dem Transportweg Waren oder Produkte verloren gegangen sind oder beschädigt wurden, oder, dass zu viele Waren verschickt wurden.“

7.2 Verkauf

„In der Verkaufshalle sollten Lesegeräte auch an den Regalen angebracht sein, die dann wiederum erkennen, wenn Waren entnommen werden. Wenn dies dann an das Verkaufspersonal weitergeleitet wird, gehören leere Regale der Vergangenheit an. An der Kasse können dann die Waren wiederum gelesen und in der Datenbank als "verkauft"notiert werden. Im Idealfall müssen die Waren dazu nicht einmal aus dem Wagen genommen werden, sondern werden vom Lesegerät der Kasse einfach registriert.“

7.3 Öffentlichkeit

„Wenn alle Produkte mit einem Transponder ausgestattet sind, dann können diese Produkte auch nach dem Verkauf noch beim Endkunden weiter verfolgt und auch in der Öffentlichkeit ausgelesen werden. So könnten Lesegeräte zum Beispiel Produkte in einer Einkaufstasche erfassen und dazu passende Werbung in ein Schaufenster einspielen. Hier spricht man von personalisierter Werbung.

Auch kann so zum Beispiel von der Müllabfuhr erkannt werden, ob der Müll richtig getrennt wurde, denn ein Müllbeutel wird von einem Lesegerät einfach gelesen und wenn sich falsche Dinge darin befinden, kann sie einfach stehen gelassen werden. So ist es natürlich auch möglich widerrechtlich abgeladenen Müll einem Verursacher zuzuordnen, denn es muss mit den Transpondern nur ermittelt werden, wo die Waren gekauft wurden. In der Datenbank des entsprechenden Ladens kann dann der Müllsünder entdeckt werden."

„Eine ganz andere Anwendungsmöglichkeit in der Öffentlichkeit, ist der Einsatz von RFID-Systemen für Veranstaltungen wie zum Beispiel Konzerte. Wer nicht das nötige Ticket mit Transponder besitzt, kommt dann gar nicht erst hinein. Ähnliches ist auch für die öffentlichen Verkehrsmittel denkbar, wenn auch diese Tickets mit Transponder ausgestattet werden." [Journal]

8 Diskussion

Neben den Vorteilen eines RFID-Systems, die in den vorhergehenden Abschnitten angesprochen wurden, birgt die Technik noch einige Nachteile. Hier beleuchten wir diese etwas genauer.

8.1 Pulkerkennung

Die Pulkerkennung, die als Vorteil angesehen wird, beschreibt ein Verfahren zum Identifizieren mehrerer Transponder, die beispielsweise Artikel auf einer Palette markieren. Es ist ein sich selbst organisierender Prozess, der die Tags nacheinander ausliest. Das beinhaltet, dass sich diese nicht alle zur gleichen Zeit bei dem Reader zurückmelden, um möglichst nur einmal gelesen zu werden und nach dem Lesen nicht mehr zu antworten.
Bis zu diesem Zeitpunkt ist das Verfahren noch nicht ausgereift, denn es besteht keine Möglichkeit die Transponder oder Objekte zu zählen, was eine Prüfung der Vollständigkeit oder Inventarerfassung ausschließt. [Wiki]

8.2 Datensicherung

Ein klarer Vorteil der RFID- Technik ist der, dass Objekte permanent beschrieben werden und so die Informationen den aktuellsten Stand beinhalten und Lieferwege und Herkunft nachvollzogen werden können. Zudem können zusätzliche Informationen eingefügt und geändert werden.
Dies zieht allerdings das Problem der Datensicherung nach sich.
Das Auslesen eines Transponders könnte die Gefahr des Kopieren der Identifikationsnummer nach sich ziehen. Ausserdem könnte die Übertragung eines Lesevorganges gestört werden. Diese beiden Aspekte werden an einem konkreten Beispiel erläutert.

8.2.1 Funkfernbedienung

Eine Fernbedienung zur Zentralverriegelung eines Autos und auch die Wegfahrsperre basieren auf RFID. Aktuell wird in den Medien über ein System zum „knacken" der Funktechnik berichtet.
Dabei sendet ein handelsübliches Funkgerät auf der gleichen Frequenz wie die

Fernbedienung des Autos. Durch das stärkere Funksignal wird der Schließbefehl überlagert und kommt so nicht beim Lesegerät an.
Die Zentralverriegelung kann zwar nur ausgeschaltet werden, wenn ein passender Schlüssel vorhanden ist, aber eine entsprechende Software lockt sich in das System ein und deaktiviert die Wegfahrsperre, sodass das Auto nicht mehr blockiert und gestartet werden kann, selbst mit einem Schlüssel mit einer anderen ID. [Galileo]

Eine weitere Methode ist die, mit Hilfe einer Software, die Daten des Autos mitsamt der Schlüssel-ID auf einen anderen Schlüssel zu übertragen. Es entsteht eine perfekte Kopie und das Auto kann gefahren werden.

Abbildung 7: Funkfernbedienung

In einer Zeit der „Datensammelwut“ bietet RFID eine neue Möglichkeit kontaktlos Daten aufzuzeichnen und als Kundenprofil zu speichern. Wie in dem Szenario beschrieben, könnte der Einkaufswagen einer Person zu Standardeinkäufen leiten oder auf sie abgestimmte Werbung einspielen. Dies lässt nicht nur den Verbraucherschutz aufhören, auch könnten diese Daten für Verbrecher nützlich werden, um beispielsweise Einkaufszeiten zu ermitteln.
Stimmen werden laut, dass RFID nur ein weiteres Teil des „Kontrollstaates“ sei. [IKON]

Klare Verstöße gegen die Datenschutzbestimmungen liegen vor, sobald Personen unwissentlich mit Transpondern ausgestattet werden. Die Ausstattung von Arbeitnehmern über den Firmenausweis oder eingenäht in die Kleidung stellt eine Option zur Überwachung von Pausenzeiten und Arbeitsverhalten dar. Aber auch Privatpersonen könnten überwacht werden, indem sie ein Produkt mit einem eingearbeitetem Tag erworben haben und nicht wissen, dass sie potentiell gelesen werden können. Es werden nicht nur Daten über den Artikel sondern auch über den Käufer abgefragt, was ohne ausdrückliche Zustimmung nicht rechtens ist. Werden mehrere Chips bei einer Person verteilt, wie am Auto, der Kleidung, der Geldbörse und in der Wohnung, kann ein genaues Profil dieser Person erstellt werden.
Zur Zeit geben die Verbraucher den Firmen durch den Kauf eines mit RFID ausgestatteten Produktes die Zustimmung ihre Daten auszulesen und zu sammeln. Daher kämpfen Datenschützer dafür, dass Konzerne die RFID einsetzen ihre Artikel der Filialen kennzeichnen und die Kunden informieren müssen. An einem „Blocker Tag“ der das ungefragte Auslesen verhindern soll, wird geforscht.

Durch die Möglichkeit auf Kundendaten zuzugreifen und die Transponderinformationen abzufangen, besteht prinzipiell auch die Option für Unbefugte Kundenkarten auszulesen und auf deren Rechnung einzukaufen, was durchaus schwierig zu entdecken wäre.
Auch der entstehende Elektrosmog ist ein Nachteil von RFID, der aber noch nicht eingeschätzt werden kann. Genau wie die nicht auszublendenden Störge-

räusche, die Übertragungen teilweise unmöglich machen.
Der greifbarste Nachteil der Systeme ist der, der Verbreitung. Die Einrichtung der Technik ist teuer und durch die weitere Forschung fallen bei jeder Aufrüstung erneut Kosten an, sodass die wenigsten Firmen mit RFID arbeiten. Andererseits würde eine Einheit preiswerter werden, wenn viele investieren würden. Die zu nehmende Hürde ist somit das Vermarkten des Produktes. Zudem müssten einheitliche RFID- Anlagen verkauft werden und nicht nur geschlossene Systeme in einem Betrieb. [Journal]

Abschließend ist zu sagen, dass RFID definitiv viele Vorteile hat, das System aber auch Nachteile birgt, die grundlegend nicht zu akzeptieren sind und die gesetzlich geregelt werden sollten. Eine persönliche Entscheidung über Kaufen oder nicht akzeptieren von Transponder gekennzeichneter Ware, bzw. das tragen von „Blocker Tags“ würde die Konsumenten in zwei Gruppen spalten und voraussetzen, dass sich Menschen vor der Industrie schützen müssen, anstatt bei Interesse der Datenfreigabe zuzustimmen.

Wir hoffen auf eine Weiterentwicklung!

Literatur

[Wiki] http://www.wikipedia.de; Suchbegriffe: RFID, Harry Stockman, Radar und alle Weiterführungen

[Rosol] Christoph Rosol: RFID- Vom Ursprung einer (all)gegenwärtigen Kulturtechnologie;Seite 63-132

[Stockman] Harry Stockman: „Communication by Means of Reflected Power“ proceeding of the I.R.E.; Seite 1196-1204

[Journal] http://www.rfid-journal.de

[Schreiner] http://www.schreiner-logidata.de

[Improve] http://www.improve-mtc.de/Veroffentlichungen/RFID/rfid.html

[Marktplatz] http://www.marktplatz-rfid-im-blick.de

[Folie] http://www.stuttgart.ihk24.de

[Seminar] http://home.arcor.de/ivenae/files Geschichte der RFID Technologie

[Galileo] http://www.prosieben.de/tv/galileo Bericht: Funkfalle

[IKON] Arno Rolf: "MIKROPOLIS 2010 – Menschen, Computer, Internet in der globalen Gesellschaft"

[Abb.1] Harry Stockman: „Communication by Means of Reflected Power“ proceeding of the I.R.E.; Seite 1196-1204

[Abb.2] http://www.wikipedia.de

[Abb.3] http://www.schreiner-logidata.de

[Abb.4] http://images.idgentertainment.de

[Abb.5] http://rfid-informationen.de

[Abb.6] http://getcontagio.us

[Abb.7] http://www.panmobil.de

Informatik und Rüstung

Henning Pridöhl, Ewald Herber

Zusammenfassung

Die Informatik war insbesondere in ihren Anfängen eng mit dem Militär und der Rüstungsindustrie vernetzt. Im Folgenden werden wir darstellen, welche Verwendungszwecke informatischer Technologien es für das Militär in der Geschichte der Informatik gab und betrachten, ob und in wie weit sich diese in der heutigen Zeit geändert haben. Wir werden diese Technologien kritisch bezüglich ihrer moralisch-ethischen Aspekte hinterfragen und dabei einen Ausblick geben, welche weiteren Probleme bei zukünftigen Entwicklungen noch auftreten können.

1 Geschichte

Das Militär hat die Informatik in ihren Anfängen besonders voran getrieben. Ohne die Finanzierung des Militärs wäre die Forschung heute deutlich weniger fortgeschritten. Die Form der heutigen Kriege wäre ohne die ganzen Entwicklungen auf dem Gebiet der Informatik gar nicht denkbar. Daher werden wir darstellen, welche Interessen es seitens des Militärs in der Informatik von ihrer Entstehung an bis heute gab und zu welchen Ergebnissen die Forschung gekommen ist. Des Weiteren zeigen wir auch auf, wie weit diese auch Einfluss auf damalige Konflikte und Kriege, wie zum Beispiel den zweiten Weltkrieg oder den kalten Krieg hatten.

Da die Geschichte der Informatik in Bezug auf Rüstung sehr umfangreich ist und ganze Bücher füllen kann, beschränken wir uns daher auf folgende Themen und erläutern diese jeweils beispielhaft.

Berechnungen durch Computer: Die ersten Computer wurden maßgeblich vom Militär finanziert und dienten z.B. zur Berechnung von ballistischen Flugbahnen oder zur Simulation von Vorgängen in Atomwaffen. Wir stellen als Beispiel für so einen Computer dieser Art den ENIAC vor.

Telekommunikation: Die Erfindung moderner Telekommunikation, wie zum Beispiel der Telegraf oder das Telefon, ermöglichte neue Formen der Kriegsführung, da Mitteilungen viel schneller verschickt werden konnten. Wir betrachten in dieser Arbeit das ARPANET, das als Vorgänger des Internets angesehen werden kann.

Kryptografie: Die schon mehrere Jahrhunderte alte Wissenschaft wurde auch schon vor dem Entstehen der Informatik militärisch genutzt. Die Informatik hat neue Verfahren hervorgebracht, die insbesondere die militärische Telekommunikation absichern sollten. Wir beschäftigen uns in dieser Arbeit mit der ENIGMA und ihrer Bedeutung im zweiten Weltkrieg.

Waffentechnologie: Viele Waffensysteme enthalten Computer oder werden von solchen gesteuert. So konnte durch Elektronik die Treffgenauigkeit von Raketen deutlich verbessert werden. Als ein ambitioniertes Projekt betrachten wir die Strategic Defense Initiative.

1.1 Electronic Numerical Integrator and Computer (ENIAC)

Der ENIAC war der erste rein elektronische Rechner in den Vereinigten Staaten. Er wurde von J. Presper Eckert und John W. Mauchly an der University of Pennsylvania entwickelt. Der erste Entwurf von Mauchly stammt aus dem Jahr 1942, die eigentliche Entwicklung begann jedoch erst 1943. Am 15. Februar wurde der ENIAC dann der Öffentlichkeit präsentiert. Finanziert wurde das Projekt mit einer halben Million US-Dollar von der US-Armee. Er diente zur Berechnung von ballistischen Flugbahnen. [4]

Vor Erfindung der ENIAC wurden die ballistische Flugbahnen entweder per Hand berechnet und in Tabellen erfasst oder von einem „Differential Analyzer“ berechnet. Ersteres erforderte einen enormen Aufwand und war sehr fehleranfällig. So wurde zum Beispiel bei einer Berechnung vergessen, die Werte vorher von Yard in Meter umzurechnen, so dass das ganze Ergebnis nicht mehr zu gebrauchen war. Der „Differential Analyzer“ hatte den Nachteil, dass er aufgrund seiner analogen Bauart nur ungenaue Ergebnisse lieferte und im Vergleich zum ENIAC deutlich langsamer war. So konnte der ENIAC Flugbahnen in unter einer Minute genau berechnen, für die der „Differential Analyzer“ eine halbe Stunde bei ungenaueren Ergebnis gebraucht hätte. [19]

Der ENIAC rechnete, anders als heutige Computer, nicht im Binärsystem sondern im Dezimalsystem. Gewöhnlich rechnete er mit zehnstelligen Dezimalzahlen, konnte jedoch auch bis zu zwangzigstellige Zahlen verarbeiten. Er beherrschte neben der einfachen Addition und Subtraktion noch weitere Operationen, wie beispielweise die Multiplikation, das Dividieren und das ziehen von Quadratwurzeln. Diese waren jedoch im Vergleich deutlich langsamer. So brauchte eine einzelne Addition nur eine fünftausendstel Sekunde während die Multiplikation $p+4$ mal so lange dauerte wie eine Addition, wobei p die Anzahl an Stellen des Faktors ist, mit dem multiplizert werden sollte. Das Ziehen einer Quadratwurzel war die langsamste Operation: Sie brauchte die Zeit von $13(p+1)$ Additionen, wobei p hier die Anzahl Stellen der Zahl ist, dessen Quadratwurzel bestimmt werden sollte. [8]

Der ENIAC bestand aus 40 Panels, die in einer U-Form angeordnet wurden. Zusammen enthielten die Komponenten ca. 18.000 Röhren und 1500 Relais. Die Panels wurden so miteinander kombiniert, dass 30 funktionale Einheiten entstanden, die eine oder mehrere Funktionen übernahmen. Die Einheiten, die hauptsächlich mit Addition und Subtraktion beschäftigt waren, waren Akkumulatoren. Diese konnten zehnstellige Zahlen in sich speichern und eine weitere Zahl auf die gespeicherte addieren oder subtrahieren. Von diesen Akkumulatoren gab es bei der ENIAC 20 Stück. Für die Multiplikation, die Division und das Quadratwurzelziehen gab es weitere Einheiten. Eine weitere Einheit, der sogenannte „constant transmitter“, war für das Einlesen von Zahlen zuständig. So konnten Zahlen auf Lochkarten über ein Lesegerät in den „constant transmitter“ eingegeben werden, die dieser dann in elektrische Signale umwandelte und an die benötigten Einheiten übermittelte. Berechnungen wurden durchgeführt, in-

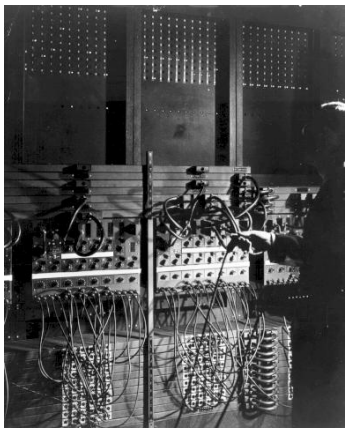


Abbildung 1: ENIAC mit den typischen Verdrahtungen [27]

dem die passenden Einheiten mit Kabeln verbunden und an einem Drehschalter die gewünschte Operation eingestellt wurde. [8]

Programmiert wurde der ENIAC von Frauen, die zum Teil schon vorher mit an der Konstruktion der ENIAC beteiligt waren oder vorher Flugbahnen berechnet haben. [7]

Neben dem Berechnungen von Flugbahnen, zu dem die ENIAC hauptsächlich benutzt wurde, gab es auch eine Reihe weiterer Berechnungen. Fritz listet einige in seinem Papier „ENIAC-a problem solver“ [6] auf:

- Eine Tabelle mit den Werten der Fakultäten von 1! bis 1000! (Jeweils die 20 höchstwertigsten Stellen)
- Inverse von Matrizen der Ordnung 5 bis 9.
- Tabellen für die Werte von Sinus und Kosinus
- Wahrscheinlichkeitsverteilungen

Dieses zeigt deutlich, dass die ENIAC nicht für nur eine Art von Berechnungen spezialisiert war, sondern für sehr verschiedene Berechnungen einsetzbar war.

Die Erfinder Eckert und Mauchly beantragten 1947, ein Jahr nachdem sie ihre Firma (Eckert-Mauchly Computer Corporation) gegründeten hatten, ein Patent auf die Konstruktionsweise der ENIAC. Dieses wurde am 4. Februar 1964 als US-Patent 3,120,606 ausgestellt. Nach einem längeren Gerichtsstreit wurde dieses jedoch 1973 für ungültig erklärt, da das Patent Entwürfe John Atanasoff, der am Iowa State College einen Rechner baute, enthielt und somit als abgeleitetes Werk galt. [15]

1.2 Advanced Research Projects Agency Network (ARPANET)

Das ARPANET war das weltweit erste Netzwerk, das auf dem Austausch von Paketen basierte. Die Daten wurden dabei in kleine Stücke aufgeteilt und in Paketen über das Netzwerk geschickt. Dabei mussten die Pakete weder in der

ursprünglichen Reihenfolge ankommen noch den gleichen Weg durch das Netzwerk nehmen. Auch der Ausfall einzelner Netzwerkknoten lässt das Netzwerk nicht gesamt ausfallen, da die Pakete dann einfach über andere Knoten geleitet werden.

Die ursprüngliche Idee für ein Netzwerk, das die Kommunikation zwischen vielen Computern erlaubte, stammte von J. C. R. Licklider. Er beschrieb sein Konzept des „Intergalactic Computer Network“ in mehreren Memos. Licklider war ab 1962 an der Spitze der ARPA[1], einer Institution, die für die Vereinigten Staaten Rüstungsforschung finanziert. Dort überzeugte er seinen Nachfolger Lawrence G. Roberts von der Idee dieses Netzwerkes.

Die Grundlagen für ein Netzwerk, das mit Paketvermittlung funktioniert, lieferte Leonard Kleinrock 1961 mit seinem Papier „Information Flow in Large Communication Nets“ [12]. Dort beschrieb er die Realisierbarkeit eines solchen Netzwerkes und die Vorteile gegenüber Netzwerken, die auf Leitungsvermittlung basieren (s. o.).

Kleinrock konnte Roberts von seiner Forschung überzeugen, sodass dieser ein Konzept [20] für das ARPANET entwurf und 1967 veröffentlichte. In diesem erklärte er die Nützlichkeit eines Netzwerkes. So schlug er beispielsweise folgende Verwendungszwecke vor:

- **Lastverteilung** - Programme könnten zusammen mit den Daten auf andere Computer transferiert werden und somit die Last für Berechnungen auf mehrere Computer verteilen.
- **Nachrichtendienst** - um Nachrichten zwischen Personen auszutauschen.
- **„Program sharing“** - Daten könnten an ein Programm auf einen anderen Computer geschickt werden um dort berechnet zu werden. Das Ergebnis könnte anschließend zurückgeschickt werden.
- **„Data sharing“** - Große Datenmengen könnten auf einem anderen Computer liegen, welcher ein Programm gesendet bekommt, mit dem diese verarbeitet werden könnten. Dies sieht er insbesondere als Vorteil, wenn das Kopieren der Daten zu teuer ist.

Im Jahre 1968 wurde die Struktur und die Spezifikation des Konzeptes verfeinert und eine Ausschreibung für den Entwicklung der Paketvermittler, „Interfaces Message Processors“, kurz IMP genannt, veröffentlicht.

Den Zuschlag bekam die Bolt, Beranek and Newman company (BBN). Diese konstruierte dann die IMP in Zusammenarbeit mit Bob Kahn, der eine wichtige Rolle in der Architektur des ARPANETs spielte.

Der erste Knoten im ARPANET war das Network Measurement Center an der University of California, Los Angelos (UCLA), wo Kleinrock arbeitete. Der erste IMP wurde dort 1969 installiert und erste Rechner angeschlossen. Als zweiter Knoten kam das Stanford Research Institute (SRI) hinzu. Es wurde dann auch die erste Nachricht von der UCLA an das SRI geschickt. Sie sollte das Wort „login“ enthalten, nach den ersten zwei Buchstaben ist jedoch das System zusammen gebrochen. Nachdem das System wieder lief, konnte doch noch die gesamte Nachricht übertragen werden.

[1] heute heißt sie DARPA, für Defense Advanced Research Projects Agency

Als weitere Knoten kamen noch die University of Santa Barbara und die University of Utah hinzu, sodass das Netzwerk 1969 aus insgesamt 4 Knoten bestand.

Es wurden mehrere Anwendungen für das ARPANET entwickelt. Ray Tomlinson von BBN entwickelte 1972 eine Anwendung zum Verschicken und Empfangen von E-Mails. Sie stellte den größten Teil der Nutzung des ARPANETs dar.

Es wird oft behauptet, dass das ARPANET als Netzwerk geschaffen werden sollte, das so robust zu sein hat, dass auch während eines nuklearen Krieges weiterhin funktioniert. Leiner et. al. [14] merkten dazu an:

> It was from the RAND study that the false rumor started claiming that the ARPANET was somehow related to building a network resistant to nuclear war. This was never true of the ARPANET, only the unrelated RAND study on secure voice considered nuclear war. However, the later work on Internetting did emphasize robustness and survivability, including the capability to withstand losses of large portions of the underlying networks.

Auch wenn das ARPANET also den Ausfall großer Teile des Netzwerkes verkraftet, war es ursprünglich nicht dediziert dazu gedacht einen nuklearen Krieg stand zu halten.

1.3 ENIGMA

Die ENIGMA ist eine Chiffriermaschine, die im zweiten Weltkrieg insbesondere vom deutschen Militär genutzt wurde. Sie lief elektromechanisch je nach Modell mit drei oder vier Rotoren (auch Walzen genannt) um ihre Eingaben zu verschlüsseln. Erfunden wurde sie von Arthur Scherbius im Jahr 1917. Die ENIGMA hatte eine Tastatur, die das für Schreibmaschinen übliche QWERTZ-Layout besaß. Oberhalb der Tastatur befand sich eine Anzeigetafel mit Buchstaben unter denen sich jeweils eine Glühlampe befand. Wurde eine Taste auf der ENIGMA gedrückt, so leuchtete der verschlüsselte Buchstabe auf der Anzeigentafel auf und die Rotoren drehten sich weiter. Dadurch wurde erreicht, dass die Buchstaben nicht, wie bei monoalphabetischer Substitution, immer durch einen (anderen) gleichen Buchstaben ersetzt wurden, sondern der gleiche Buchstabe auch in verschiedene Buchstaben verschlüsselt werden konnte. [13]

Technisch wurde es so gelöst, dass die Walzen für jeden Buchstaben einen Kontakt hatten und diese je nach Walzenanordnung so die Kontakte der Buchstaben auf den Tasten auf die Kontakte für die Buchstaben auf der Anzeigetafel abbildeten. Je nach Walzenanordnung gab es also eine andere Permutation des Eingabealphabets.

An der Vorderseite ist zusätzlich noch ein Steckerbrett mit Kontakten angebracht. Bevor die Kontakte der Tasten in die erste Walze geleitet werden, passieren sie das Steckerbrett. Dort konnte durch Umstecken Verdrahtung die Zuordnung der Kontakte zu den Tasten geändert und somit ein anderer Schlüssel eingestellt werden.

Ihr Erfinder Scherbius versuchte die ENIGMA zuerst an die deutsche Marine zu verkaufen. Diese lehnte jedoch mit der Begründung ab, dass sich die

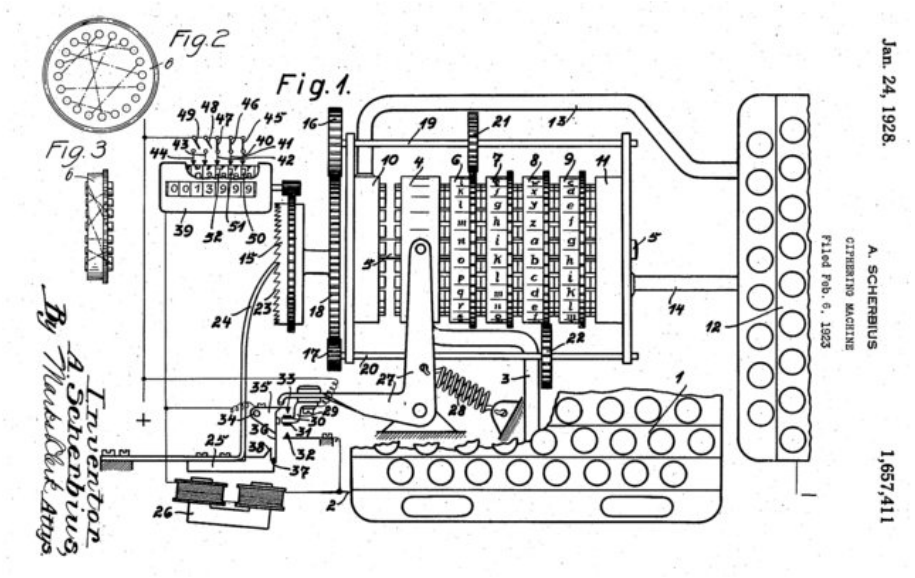


Abbildung 2: Patentzeichnung der ENIGMA. Deutlich zu sehen sind die 4 Rotoren (6, 7, 8, 9) [21]

ENIGMA für ihren niedrigen Datenverkehr nicht lohnen würden und empfahlen Scherbius beim Außenministerium nachzufragen. Dort existierte allerdings auch kein Interesse an der Maschine. [13]

Er verkaufte seine Patentrechte an die Securitas, die daraufhin 1923 die „Chiffriermaschinen Aktiengesellschaft“ gründete, um die ENIGMA auf dem zivilen Markt zu verkaufen. [13]

Beworben wurde sie mit Aussagen wie „Unangreifbar in ihrer Chiffriersicherheit“, „Jeder Entzifferungsversuch Zeitverschwendung“, „In einer halben Minute ist jeder der 277 304 461 200 Schlüssel eingestellt“ oder „Kein Teil wird zur Schlüsseländerung ausgetauscht“. [13]

Kommerziell erfolgreich war die ENIMGA jedoch auf dem zivilen Markt nie. Erst Anfang der 1920er Jahre interessierte sich das deutsche Militär für die ENIGMA. Die deutsche Wehrmacht setzte sie erst in den Jahren von 1926 bis Kriegsende 1945 ein. Das Modell „ENIGMA C“ wurde von der Reichsmarine schon 1925 zum Test produziert und eingesetzt. Mit dem Einsatz im Militär verschwand die ENIGMA auch vom zivilen Markt. [26]

Ab 1926 stellte der polnische militärische Nachrichtendienst fest, dass die deutschen Funksprüche wohl mit einem Maschinenschlüssel chiffriert wurden. Zum Knacken des Codes wurden ab 1932 drei Mathematiker eingesetzt, Rejewski, Rozicki und Zygalski. Ende 1932, nachdem dieses nahezu erreicht war, arbeitete Rejewski alleine weiter und konnte einzelne Funksprüche dechiffrieren. [26]

Das Knacken des Codes gelang jedoch nur, weil die Deutschen in der Bedienung der ENIGMA Fehler machen. So wurde festgestellt, dass die ersten 6 Buchstaben ein gewisses Muster aufwiesen. Der erste und vierte, der zweite und fünfte sowie der dritte und sechste Buchstabe bildeten Paare. Dieses lag daran, dass am Anfang eines jeden Funkspruches der Spruchschlüssel zweimal

hintereinander geschrieben wurde und mit dem jeweiligen Tagesschlüssel chiffriert wurde. Diese Schwachstelle ermöglichte es Rejewski dann, die Chiffrierung anzugreifen. [26]

Auch am Bletchley Park in Buckinghamshire, England arbeitete man an der Entschlüsselung deutscher Funksprüche. Dort entwickelten Alan Turing und Gordon Welchman die sogenannte Bombe, die dazu diente, mit der ENIGMA verschlüsselte Nachrichten zu knacken. Sie basierte auf den vorigen Arbeiten der polnischer Mathematiker, insbesondere die von Rejewski. Damit die Turing-Bombe die Nachricht dechiffrieren könnte, brauchte sie eine Angabe über ein Wort, dass sich in einem bestimmten Bereich befindet. Häufig genutzte Wörter waren „NULLNULLNULL“ oder „WETTERVORHERSAGE“. Damit konnte sie einen reduzierten Schlüsselraum nach dem richtigen Schlüssel absuchen, mit dem die Nachricht dann dechiffrieren werden konnte. [5]

Es wird geschätzt, dass die Arbeit im Bletchley Park den zweiten Weltkrieg um bis zu zwei Jahre verkürzt hat. [18]

1.4 Strategic Defense Initiative (SDI)

Die Strategic Defense Initiative war eine 1983 von Ronald Reagon gestarte Initiative zum Bau eines Abwehrschirms gegen Interkontinentalraketen der sowjetische Angriffe mit diesen zur Zeit des Kalten Krieges abwehren sollte.

Geplant waren dazu sowohl Waffen am Boden als auch Waffen im im Weltall, weshalb es auch als „Star Wars“ bezeichnet wurde. Die Forschung hatte dementsprechend einen sehr großem Umfang. So war beispielweise chemischer Laser oder ein Neuronenstrahl geplant, der im Orbit Raketen zerstören konnte. [1]

Bereits 6 Jahre nach Beginn der Initiative hatte diese bereits 16 Milliarden Dollar gekostet und wurde von vielen sehr kritisch gesehen. Bereits 1985 trat David Parnas aus dem „SDIO Panel“ aus, mit der Begründung, dass er die Arbeit dort nicht als zielführend betrachtete. Er schrieb in einem Brief [17] an James Offut, stellvertretender Leiter bei der Strategic Defense Initiative Organisation in dem er dieses genauer schilderte:

> 1. The goals stated for the Strategic Defense System cannot be attained by the class of systems that you are considering
> 2. The SDIO is not the appropriate organization to fund and administer the research it is supporting. Most of the money spent will be wasted. The panel on which you have asked me to serve, is not appropriately constituted, clearly chartered, and adequately informed. There are better ways to select and manage research

Bis heute existiert kein funktionierender Raketenschirm, der die Vereinigten Staaten vor Interkontinentalraketen schützen könnte.

2 Heutige Technologien der Rüstungsforschung in der Informatik

Die Entwicklung in der Informatik ging rasend voran. Computer wurden deutlich schneller und kleiner, Telekommunikation deutlich ausgereifter und auch

in vielen anderen Gebieten gab es erhebliche Fortschritte. Dieses wirkte sich auch auf die Rüstungsangelegenheiten von Staaten aus. Der Trend scheint sehr Richtung automatisierter oder gar komplett autonomer Systeme zu gehen.

2.1 Einsatz von Dronen

Umbemannte Dronen werden sowohl vom britischen als auch vom amerikanischen Militär eingesetzt. So besitzen die USA 200 Dronen von Typ „Predator“ und 30 Dronen vom Typ „Reaper“ (Stand 2009) und wollen 2010 eine Summe von 5,5 Milliarden Dollar in unbemannte Gefährte investieren. Auch die Briten besitzen einen „Predator“, ein anderer ist ihnen 2008 im Irak abgestürzt. [25]

Die Dronen werden hauptsächlich im Irak für die Luftaufklärung eingesetzt. Dort fliegen sie ferngesteuert über das aufzuklärende Gebiet um besonders Bomben, die an Straßen eingegraben werden, zu entdecken oder Waffenlager zu sichten. Ende 2009 wurde bekannt, dass die Dronen von irakischen Aufständischen abgehört wurden. Dies lag nach offiziellen Angaben daran, dass einer kleiner Teil der Verbindungen, insbesondere zu nahegelegenen Bodenstationen mit älterer Technik, unverschlüsselt waren. Mit neueren Bodenstationen würde nur noch verschlüsselt kommuniziert. [23]

Jedoch sind diese Dronen auch bewaffnet. Sie tragen Raketen an sich, die von der Ferne gezündet werden können. So wurden in einem aufgedeckten, ehemals geheimen Programm der CIA von ferngesteuerten Dronen ein Dutzend höherer Führer der al-Quaida getötet, darunter Abu Khabab al-Masri, der den Ruf hatte, Experte auf dem Gebiet der Massenvernichtungswaffen zu sein und Baitullah Mehsud, Führer der pakistanischen Taliban. [10]

Hier ist auch der Trend in Richtung mehr Dronen klar ersichtlich. Die American Airforce berichtete, dass sie mittlerweile mehr Dronenbediener trainiert als gewöhnliche Piloten. Während sie 2006 nur 12 Dronen fliegen lassen konnte, waren es bereits 50 im Jahr 2009. [9]

2.2 Einsatz von Kampfrobotern

Seit 2007 sind im Irak erstmals Kampfroboter des Typs „SWORDS“ (Special Weapons Observation Reconnaissance Detection System) im Einsatz. Diese ca. 60 Zentimeter breiten und 90 Zentimeter langen Roboter werden von Soldaten aus der Ferne bei einer Reichweite von bis zu 1000 Metern gesteuert. Sie könnten ein Maschinengewehr vom Typ M249 tragen - eine Waffe, die auch die Soldaten im Irak benutzen. Mit dieser kann er bis zu tausend Schuss pro Minute abgeben. Neben dem Maschinengewehr kann aber auch ein Raketenwerfer montiert werden. Der „SWORDS“ verfügt über einen Kettenantrieb mit dem er eine Geschwindigkeit von bis zu 10 km/h erreichen kann. Selbst Treppensteigen ist damit möglich. Die Betriebsdauer beträgt 4 Stunden. Mit einer Kamera kann der Soldat das Gebiet einsehen und danach Entscheidungen treffen, was der Roboter tun soll. Der „SWORDS“ basiert auf „TALON“, einem früheren Modell, das bereits bei der Entschärfung von Bomben zum Einsatz kam, jedoch nicht bewaffnet war. [22] [2]

Die Kampfroboter „SWORDS“ wurden 2008 wieder aus dem Irak abgezogen, ohne jemals einen Schuss von sich gegeben zu haben. [16]

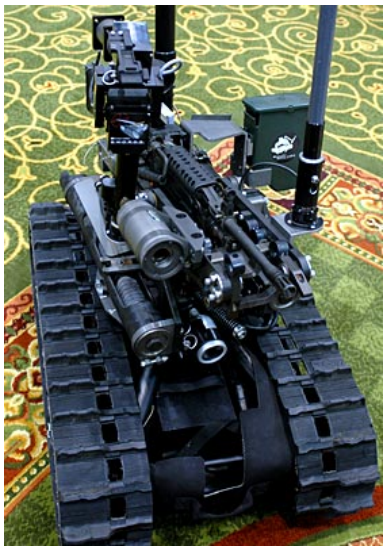


Abbildung 3: Der SWORDS-Kampfroboter mit montierten Maschinengewehr [11]

Technisch ist der Entwurf von Kampfrobotern, die in solchen Gebieten zum Einsatz kommen, schwierig. Im Jahre 2004 sollten 15 Prototypen bei einem Test der Forschungsabteilung des Pentagon 200 Kilometer durch unwegsames Gelände in der Mojawewüste fahren. Keiner der Roboter konnte diese Aufgabe lösen, alle waren nach spätestens 4 Stunden Fahrt defekt. [22]

3 Moralisch-ethische Aspekte

In diesem Abschnitt wollen wir uns Aspekten der Moral und Ethik in der Rüstungsforschung - aber auch in der Anwendung von informatikbezogenen Systemen aus der Rüstung beschäftigen.

3.1 Dual Use

Dual Use bezeichnet Technologien, die sowohl militärisch als auch zivil genutzt werden können.

Ein bekanntes Beispiel ist hierfür das Global Positioning System (GPS). Es wurde damals rein für militärische Zwecke entwickelt, wird aber heute auch zivil genutzt. Das GPS dient der Positionsbestimmung, so kann mit einem GPS-Empfänger die eigene Position auf wenige Meter genau bestimmt werden. Für das Militär ergibt sich der Vorteil, dass sie die genauen Positionen ihrer Fahrzeuge und Waffensysteme bestimmen können. Die Zivilgesellschaft nutzt das GPS hauptsächlich bei Navigationsgeräten für Autos.

Es gibt Unterschiedliche Arten von Dual Use. So gibt es Technologien, die früher für den rein militärischen Gebrauch entwickelt wurden, aber mittlerweile auch zivil genutzt wurden. Auch die umgekehrte Richtung, also zuerst für zivile Zwecke genutzt, später dann vom Militär für nützlich empfunden ist möglich.

Aus Kostengründen wird auch an Entwicklungen geforscht, die sowohl einem zivilen als auch einem militärische Zweck haben.

In einigen Fällen ist es schwierig, zu entscheiden, ob eine Technologie wirklich nur für zivile Zwecke genutzt werden kann. Folgende Aufgabenstellungen sollen dieses verdeutlichen:

1. Entwickeln Sie einen Algorithmus, um die Positionen von Krankenhäusern zu berechnen, so dass möglichst viele Menschen gut versorgt werden können.

2. Entwickeln Sie einen Algorithmus, um die Positionen von Bombenabwürfen zu berechnen, so dass möglichst viele militärische Einrichtungen zerstört werden.

Erstere beschreibt eine rein zivile Nutzung. Der gleiche Algorithmus kann jedoch, ohne dass es gleich offensichtlich ist, auch für militärische Zwecke genutzt werden, wie die zweite Aufgabenstellung zeigt.

Für einen Wissenschaftler, der aus Gewissensgründen nur zivile Forschung betreiben möchte, stellt dieses ein Problem dar. Er hat keine Sicherheit, dass das Militär seine Ergebnisse später einmal nutzt. Eine Möglichkeit, es zumindest ansatzweise zu prüfen ist, sich zu erkundigen, ob die Gelder aus denen seine Forschung finanziert wird, direkt vom Militär oder von Rüstungsfirmen stammen.

3.2 Verharmlosung

Neuere Technologien aus der Informatik, die militärisch genutzt werden, könnten zu einer Verharmlosung von Kriegen führen.

US-Verteidigungsexperte P. W. Singer, der sich sehr viel mit Militärrobotern und umbemannten Fahrzeugen bzw. Dronen beschäftigt, sagte in einem Interview [24] folgendes:

> I heard a drone pilot explain it this way: You're going to war for one hour, and then you get in the car and drive home, and within two minutes you're sitting at the dinner table talking about your kids' homework. This is a very different experience of war.

Diese Aussage zeigt deutlich die Verharmlosung von Kriegen, denn es werden stark die Vorteile der Kriegsführung aus der Ferne durch Soldaten betont und eine heile Welt beschrieben. Nicht mal ansatzweise werden grausamen Folgen eines Krieges reflektiert oder hinterfragt, ob das eigene Handeln gerechtfertigt ist.

Kriege, die nur zwischen Robotern geführt werden und bei denen keine Menschen zu schaden kommen sind Fiktion. Hohe Verluste eigener Soldaten aber auch Zivilisten führen zu einer gewissen Abschreckung, die dafür sorgen kann, dass ein Krieg nur wenige Unterstützer findet. Mit dem Einsatz vom Robotern könnte suggestiert werden, das das Führen von Kriegen weniger grausam sei, da das Risiko für die eigenen Soldaten ums Leben zu kommen geringer sei und so weniger Verluste erlitten würden.

Wird die Bereitschaft, Kriege zu führen, steigen, weil weniger Soldaten und stattdessen mehr Roboter in das betreffende Gebiet zu schicken sind? Wie werden zukünftige Kriege von Menschen wahrgenommen, wenn bei ihnen zum großen Teil nur noch Maschinen statt Menschen kämpfen?

3.3 Wahrnehmung bei ferngesteuerten Robotern

Wie in Abschnitt 2.2 bereits beschrieben, besaß der Roboter „SWORDS“ nur eine Kamera, durch die der Soldat die Umwelt des Roboters wahrnehmen kann. Seine Wahrnehmung ist im Gegensatz zu eigener Anwesenheit im Kampfgebiet stark eingeschränkt.

Zum einem ist das Bild einer Kamera, selbst wenn sie hochauflösend ist, nicht vergleichbar mit dem Bild, welches mit den eigenen Augen gesehen wird. Auch Reflexe wie das Umschauen können eingeschränkt sein. Der Soldat kann zwar über die Fernsteuerung die Kamera drehen, jedoch ist es etwas vollkommen anderes einen Knopf zu drücken oder den Kopf selbst zu bewegen.

Eine andere starke Einschränkung ist das Fehlen von Umgebungsgeräuschen. Reflex des Umschauens, sobald ein auffälliges Geräusch wahrgenommen wird, ist dadurch nicht mehr gegeben. Auch die Reaktionen anderer Menschen, die aufgrund eines solches Geräusches entstehen könnten, kann der Soldat aus der Ferne nicht richtig einschätzen. Der Einbau eines Mikrofons würde dieses zwar verbessern, nicht jedoch die gleiche Aufnahme der Geräusche wie bei eigener Anwesenheit ermöglichen. Insbesondere das dreidimensionale Hören kann nicht mit einem einfachen Mikrofon nachgebildet werden. Mehr Technik könnte dieses Problem lösen, aber selbst dann bleibt es fraglich, wie gut die Nachbildung sein kann.

Was gar nicht nachgebildet werden kann ist der Eindruck, der durch dortige Witterungsbedingungen entsteht. Wärme- oder Kältegefühl, das Gefühl auf der Haut in einer staubigen Gegend. Auch diese beinflussen den Soldaten.

Mit diesen Einschränkungen muss ein Soldat möglicherweise Entscheidungen über Leben und Tod von anderen Menschen treffen. Fraglich ist dabei, in wie weit und in welche Richtung die Einschränkungen seine Entscheidungen beinflusst. Sicher ist jedenfalls, dass der Eindruck von der Lage ein anderer ist, wenn er von der Ferne agiert anstatt direkt anwesend zu sein.

3.4 Beherrschbarkeit

Viele heutige Systeme sind sehr komplex aufgebaut. Oftmals wird Software verwendet, deren Quelltext mehrere Hunderttausend oder gar Millionen Zeilen hat. Bei dieser Komplexität steigt die Wahrscheinlichkeit, dass sich in ihr irgendwo Fehler befinden. Diese müssen nicht offensichtlich sein und sofort auftreten, sondern können auch erst bei einer unglücklichen Konstellation ihre Wirkung entfalten. Beispiele sind hier nicht nur im Bereich der Rüstung zu finden. Doch gerade dort haben Fehler meist deutlich gravierendere Folgen. Ein Schreibprogramm auf einen Computer, das abstürzt ist bei weitem nicht so schlimm wie eine Rakete, die aufgrund eines Fehlers in ihrer Elektronik nicht das gewünschte Ziel trifft, sondern stattdessen bei zivile Objekten, in denen sich Menschen befinden, explodiert.

Es stellt sich die Frage, ob man solche komplexen Technologien überhaupt noch beherrschen kann oder ob es nicht eher Glück ist, dass sie zumindest meistens funktionieren. Bei den fatalen Auswirkungen, die es haben kann, sollte doch überlegt werden, wie komplex solche Systeme gestalten werden können, damit sie noch beherrschbar bleiben. Lassen sich Kampfroboter überhaupt noch vertreten, wenn man weiß, dass sie möglicherweise nicht vollständig kontrollierbar sind? Wo ist die Grenze, also welche Systeme sind noch in dem Bereich, dass

man sagen kann, man hat sie komplett unter Kontrolle? Oder sind wir sogar schon so weit, das alle üblichen Technologien, die im Militär angewendet werden, eigentlich gar nicht mehr zu beherrschen sind?

Dieses sind alles Fragen, die sehr schwer zu klären sind. Zu einem fehlt die Möglichkeit objektiv so etwas wie Beherrschbarkeit zu messen. Zum anderen ist die Bewertung stark von den jeweiligen Wertvorstellen abhängig, also in wie weit jemand bereit ist, mögliche Risiken in Kauf zu nehmen, um die Vorteile, die er sich vom Einsatz verspricht, zu nutzen. Eine allgemeine Antwort lässt sich daher nicht finden, weshalb jeder die Fragen für sich beantworten muss.

3.5 Distanz

Gegeben durch die räumliche Distanz vom Ort des Geschehens kann auch eine inhaltliche Distanz entstehen. Kriegsführung von einem Computer aus lässt den agierenden Personen das Geschehende nicht mehr sehen, was dazu führen kann, das sie gar nicht mehr realisieren, was ihre Tätigkeiten für Auswirkungen haben.

Joseph Weizenbaum formuliert dieses Problem in einem Interview [3] auf provozierende Weise:

> „Bomberpiloten beispielsweise bombardieren mit einer B 52 aus einer Höhe von 40 000 Fuß wie in Vietnam, drücken den Knopf und diese riesigen Bomben regnen da runter. Und der Pilot ist da oben. Er hört die Explosion nicht, er sieht die Explosion nicht, er sieht kein Blut, keine abgerissenen Arme, er ist so weit entfernt, dass es mehr mit Computern zu tun hat als mit Menschen oder irgendeiner Realität."

Sicher weiß der Pilot des B-52-Bombers, welche verheerende Wirkung die Bomben haben, die er abwirft, soweit man sich dieses überhaupt vorstellen kann. Die Distanz jedoch lässt dieses leichter verdrängen. Würde man den betreffenden Bomberpiloten vorher zeigen, was sie mit den Abwurf der Bomben bewirken, wäre es sicherlich fraglich, ob diese dann noch den Knopf zum Abwurf der Bomben drücken würden.

Neuere Technologien sorgen immer mehr dafür, dass die Beteiligten sich nicht mehr Ort des Geschehens befinden. So beispielsweise die Dronen, die wir in Abschnitt 2.1 vorgestellt haben. Hier sitzen keine Piloten mehr in der Drone, sie überfliegen nicht mehr selbst das Gebiet in dem sie agieren. Dennoch können die tötlichen Raketen abgefeuert werden, von einem Stützpunkt, der möglicherweise sehr weit vom Einsatzgebiet liegt. Was nehmen die Leute, die diese Dronen bedienen überhaupt noch von ihrer Tätigkeit und der Realität dahinter wahr? Waren diese jemals in einem Krisen- oder Kriegsgebiet und haben die Grausamkeit von Kriegen erfahren?

Es stellt sich dabei die Frage, in wie weit dieses auch die Hemmschwelle allgemein herabsetzt. Zögern die Soldaten weniger mit dem Einsatz von Waffengewalt, je weiter sie entfernt sind?

Was für Konsequenzen muss dieses haben, wenn das so ist? Bei schnelleren Einsatz von Waffengewalt werden sicherlich auch mehr Zivilisten getötet. Und das muss im Krieg so weit wie möglich vermieden werden.

3.6 Vollständig autonom agierende Roboter

Juristen beraten bereits über die Zulässigkeit des Einsatzes von vollständig autonom agierenden Robotern [22]. Es gibt sicher unterschiedliche Auffassungen, was *autonom* bedeutet. Hier soll unter autonom verstanden werden, dass das System seine Entscheidungen selbstständig trifft, also beispielsweise ein Roboter, der selbstständig entscheidet, wann er schießt, wohin er fährt ohne davon von einem Menschen angeleitet zu werden. Nicht verstanden werden sollen Systeme, die ihren direkten Auftrag bekommen und dieses erledigen, ohne das manuell alles kontrolliert wird. So soll eine Rakete, dessen Ziel angegeben werden kann, aber die ihren Weg selbst findet und mögliche Abweichungen automatisch korrigiert nicht als autonom verstanden werden.

Solche vollständig autonomen Roboter werfen einige Fragen auf, nicht nur technischer Natur. Zu einem ist es fraglich, wie die Unterscheidung zwischen Kombattanten und Zivilpersonen realisiert werden kann. Dieses ist selbst für Menschen schon eine schwierige Aufgabe, da unbewusst auf sehr viel mehr geachtet wird, als nur das Tragen einer Uniform. Einem Roboter diese Feinheiten beizubringen ist nur sehr schwer, wenn nicht gar umöglich.

Eine weitere Frage ist, in wie weit künstliche Intelligenz überhaupt in der Lage ist, vernünftig autonom ihre Entscheidungen zu treffen und durchzuführen. Es wird auf dem Gebiet der künstlichen Intelligenz zwar viel geforscht, aber bis heute existiert kein System, das mit dem Menschen verglichen werden könnte.

Dürfen überhaupt Algorithmen über Leben und Tod entscheiden und möchten wir das als Gesellschaft wirklich überhaupt? Sicher kann sich auch ein Mensch in seinen Entscheidungen irren, doch kann dieser seine Fehler realisieren und danach handeln. Ob eine künstliche Intelligenz in der Lage sein wird, eigene Fehler zu erkennen und und sie in Zukunft nicht mehr zu machen, ist fraglich.

Auch stellt sich bei so einem Zwischenfall die Frage, wie darauf zu reagieren ist. Ein Soldat wird sich bei eigenem Fehlverhalten sich vor Gericht verantworten müssen. Wie will man jedoch sowas bei Robotern handhaben? Soll niemand dafür verantwortlich sein, weil das System ja autonom gehandelt habe? Sicher ist jedenfalls, dass eine Gerichtsverhandlung gegen einen Roboter, die vielleicht sogar in einer Verurteilung und Bestrafung mit einer Gefängnisstrafe endet, ziemlich absurd ist. Wer kann also in so einem Fall die Verantwortung tragen? Die Politiker, die es gebilligt haben, dass solcher Roboter im Krieg eingesetzt werden? Der Hersteller dieser Roboter bzw. direkt die Entwickler, die an der Realisierung beteiligt waren und auf dem Gebiet geforscht haben? Oder Offiziere, die den Einsatz der Roboter innerhalb eines bestimmten Gebietes angeordnet haben? Diese Frage lässt sich nicht eindeutig beantworten.

Selbst wenn die Künstliche Intelligenz irgendwann einmal so weit sein sollte, dass Roboter so etwas wie ein Gewissen haben, Reue zeigen können und alles, was zum Mensch-sein dazu gehört, ergeben sich weitere Probleme: Erlangen Roboter mit solch eine Intelligenz nicht schon den Rang eines Menschen? Denn der Einsatz von Robotern wird insbesondere von der Idee voran getrieben, die Anzahl an menschlichen Soldaten auf dem Kampffeld und deren Risiko zu minimieren. Wenn diese Roboter nun aber bereits so menschlich sind, dass die Nachteile, die sie durch das nicht Mensch-sein hatten, nicht mehr existieren, ist es dann nicht genauso problematisch sie kämpfen zu lassen, wie es bei einem richtigen Menschen ist?

Diese Probleme zeigen, dass die Menge an offenen Fragen, die der Einsatz von autonomen Kapfrobotern mitbringen würde, schier unerschöpflich zu sein scheint. Deswegen ist der Einsatz bisher strikt abzulehnen.

Literatur

[1] J. A. Adam. Star wars in transition. *IEEE Spectrum*, 26(3):32–38, March 1989.

[2] Markus Becker. US-Armee schickt bewaffnete Roboter in den Kampf. `http://www.spiegel.de/wissenschaft/mensch/0,1518,497972,00.html`, 2007.

[3] Reiner Braun and Joseph Weizenbaum. Interview mit Joseph Weizenbaum bei politik-digital.de. `http://politik-digital.de/edemocracy/cyberwar/int_sicherheit/060821_Interview_Weizenbaum.shtml`.

[4] A.W. Burks and E.S. Davidson. Introduction to "the ENIAC". *Proceedings of the IEEE*, 87(6):1028–1030, June 1999.

[5] Donald W. Davies. The bombe - a remarkable logic machine. *Cryptologia*, 23(8):108–138, 1999.

[6] W. B. Fritz. ENIAC-a problem solver. *IEEE Annals of the History of Computing*, 16(1):25–45, 1994.

[7] W. B. Fritz. The women of ENIAC. *IEEE Annals of the History of Computing*, 18(3):13–28, 1996.

[8] H. H. Goldstine and A. Goldstine. The electronic numerical integrator and computer (ENIAC). *IEEE Annals of the History of Computing*, 18(1):10–16, 1996.

[9] Edward Helmore. US now trains more drone operators than pilots. `http://www.guardian.co.uk/world/2009/aug/23/drones-air-force-robot-planes`, 2009.

[10] Mark Hosenball. The drone dilemma. `http://www.newsweek.com/id/226522`, December 2009.

[11] Lorie Jewell. Armed Robots to March into Battle. `http://www.defense.gov/transformation/articles/2004-12/ta120604c.html`, December 2006.

[12] Leonard Kleinrock. Information flow in large communication nets. *RLE Quarterly Progress Report*, July 1961.

[13] Cipher Kruh, Louis anf Deavours. The commercial enigma - beginnings of machine cryptography. *Cryptologia*, 26(1), 2002.

[14] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. A brief history of the internet. *SIGCOMM Comput. Commun. Rev.*, 39(5):22–31, 2009.

[15] C. E. McTiernan. The ENIAC patent. *IEEE Annals of the History of Computing*, 20(2):54–58, April/June 1998.

[16] Popular Mechanics. Non-answer on armed robot pullout from iraq reveals fragile bot industry. `http://www.popularmechanics.com/blogs/technology_news/4258103.html`, 2008.

[17] David Parnas. Brief an Mr. Offut, stellvertretender Leiter der SDIO. *FIfF Kommunikation*, 26(1):17–22, June 2009.

[18] Laurence Peter. How poles cracked nazi enigma secret. `http://news.bbc.co.uk/2/hi/europe/8158782.stm`, July 2009.

[19] H. Polachek. Before the ENIAC [weapons firing table calculations]. *IEEE Annals of the History of Computing*, 19(2):25–30, April/June 1997.

[20] Lawrence G. Roberts. Multiple computer networks and intercomputer communication. In *SOSP '67: Proceedings of the first ACM symposium on Operating System Principles*, pages 3.1–3.6, New York, NY, USA, 1967. ACM.

[21] Arthur Scherbius. US patent US1657411: Ciphering machine, 1928.

[22] Georg Schwarte. USA setzen bewaffnete Roboter im Irak ein. `http://www.tagesschau.de/ausland/meldung198324.html`, February 2005.

[23] Scott Shane. Officials say iraq fighters intercepted drone video. `http://www.nytimes.com/2009/12/18/world/middleeast/18drones.html`, December 2009.

[24] P. W. Singer and Marc Pitzke. "The Soldiers Call It War Porn". Interview mit Verteidigungsexperte P. W. Singer. `http://www.spiegel.de/international/world/0,1518,682852,00.html`, March 2010.

[25] Telegraph. Military killer robots "could endanger civilians". `http://www.telegraph.co.uk/news/newstopics/politics/defence/5966243/Military-killer-robots-could-endanger-civilians.html`, August 2009.

[26] Heinz Ulbricht. *Die Chiffriermaschine Enigma - Trügerische Sicherheit : Ein Beitrag zur Geschichte der Nachrichtendienste*. PhD thesis, Universität Braunschweig, 2005.

[27] U.S. Army. Photo from the archives of the ARL Technical Library. `http://ftp.arl.mil/ftp/historic-computers/`.

Bioinformatik

David Seier, Mike Lebert

Zusammenfassung

In dieser Arbeit sollen zunächst die geschichtlichen Wurzeln der Bioinformatik angerissen und eine knappe Einführung in die Relevanz dieser Schnittstellenwissenschaft aus unterschiedlichen Perspektiven gegeben werden. Ein Hauptaugenmerk wird hierbei unter Anderem auf das Humangenomprojekt gelegt. Des Weiteren werden die Unterbereiche der Bioinformatik in ihren Arbeitsaufgaben und Abgrenzungen beleuchtet, sowie in einer Ausschweifung beispielsweise die Komplexität der zu erforschenden Materie, die Funktionsweise und der molekulare Aufbau der Organismen bis zur einzelnen Zelle deutlich gemacht. Des Weiteren werden das Studium und weitere Anwendungsgebiete des Fachs erläutert und ausserdem einige Fragen über ethische Aspekte der mit dieser Forschung verbundenen Materie diskutiert.

1 Ursprung

1.1 Definition

„Die Bioinformatik (englisch bioinformatics, auch computational biology) ist eine interdisziplinäre Wissenschaft, die Probleme aus den Lebenswissenschaften mit theoretischen computergestützten Methoden löst. Sie hat zu grundlegenden Erkenntnissen der modernen Biologie und Medizin beigetragen.
...
Wesentliche Gebiete der Bioinformatik sind die Verwaltung und Integration biologischer Daten, die Sequenzanalyse, die Strukturbioinformatik, die Analyse von Daten aus Hochdurchsatzmethoden. Da Bioinformatik unentbehrlich ist, um Daten im großen Maßstab zu analysieren, bildet sie einen wesentlichen Pfeiler der Systembiologie.
...
Bioinformatik ist mittlerweile eine etablierte eigenständige Wissenschaft, die zu den Grundlagenwissenschaften der Biologie und Medizin zählt, und als solche in Deutschland an vielen Standorten studierbar ist.“ [1]

1.2 Geschichte

Die Geschichte der Bioinformatik orientiert sich an der neueren Geschichte der Biologie. Als ein erster Ursprung kann zum Beispiel die Entdeckung der Doppelhelixstruktur der Desoxyribonukleinsäure innerhalb eines jeden Lebewesens angesehen werden. Die besondere Verbindung dieser 1953 von dem Amerikaner James Watson und dem Briten Francis Crick erforschten Struktur zur Bioinformatik ist die Möglichkeit zur Digitalisierung der gewonnenen Daten. Durch

[1] `http://de.wikipedia.org/wiki/Bioinformatik`

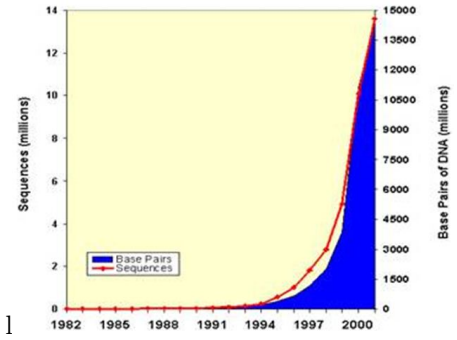


Abbildung 1: Datenzunahme in der Bioforschung

den bis dato unbekannten Aufbau der DNA-Information aus vier grundlegenden Basen (Adenin, Thymin, Cytosin, Guanin) wurde es nun möglich, die Erbinformation und den Aufbau der Proteine, aus denen jede lebende Zelle besteht, einheitlich zu beschreiben. Bereits 1955 wurde Insulin als erstes Protein sequenziert, also in Form jener genannten Basen gelesen und gespeichert (siehe auch Kap. 2.1). Ein nächster wichtiger Schritt, welcher quasi das Gegenstück auf Seite der Informatik hierzu darstellen mochte, fand drei Jahre später mit der Konstruktion des ersten integrierten Schaltkreises von Texas Instruments statt, mit dem elektronisch diskrete, digitale Zustände zunehmend effizient verarbeitet werden konnten.

Schon bald nachdem die ersten ausreichend leistungsfähigen Computer zur Verfügung standen, wurden diese von Forschern dazu genutzt, die bisher auf Handzetteln notierten, gewonnenen Sequenzierungsdaten abzuspeichern. Wegen der herausragenden Relevanz der Geninformation für die Erforschung der Organismen (siehe Kap. 1.3) nahm die Gensequenzierung im Laufe der Jahre zunehmend eine Schlüsselrolle innerhalb dieses Forschungszweiges ein. Dadurch stieg nun aber auch die Masse und Komplexität der zu händelnden Sequenzdaten, erst langsam, dann immer schneller. Ende der 1960er wurden erste Computerprogramme zur Rekombination dieser Sequenzen entwickelt, im Laufe der 70er dann schon computergestütze Sequenzierungen von Proteinketten bis hin zur Sequenzierung erster, kleinerer vollständiger Genome. Geführt von weiteren Entdeckungen der Biochemie wie der „Polymerase-Kettenreaktion“ zur Vervielfältigung von DNA-Fragmenten (1983) bis hin zum ersten vollautomatischen Sequenzier-Automaten (1986) war der Computer für eine sinnvolle Forschung in diesem Gebiet nicht mehr wegzudenken. Ohne ihn waren die immer neuen Datenmassen unterschiedlicher Proteinstrukturen schlicht nicht mehr zu bewältigen und die Analyse und der Vergleich dieser so aufwändig, dass ohne die Automation der Schaltkreise ein Ende in annehmbarer Zeit völlig außer Sicht geriet. Dieser Boom gipfelte in einem medienpräsenten Höhepunkt wie er nur mit der Mondlandung im Juli ’69 vergleichbar ist, dem Humangenomprojekt, welches sich zwischen 1990 und 2003 als öffentlich finanzierten Forscherverbund die vollständige Sequenzierung des menschlichen Genoms als Ziel setzte (siehe Kap. 1.4). Und genau wie jenes betreten des Erdtrabanten, förderte auch dieses Projekt massiv die weitere Entwicklung der betreibenden Forschung selbst. Dies war sicherlich die eigentliche Geburt der Bioinformatik wie wir sie heute

(zumindest nach Studium dieser Arbeit) kennen. [6]

1.3 Vom Gen zum Organismus: eine kurze Einführung

Also warum ist die Entschlüsselung der Gene überhaupt so wichtig? Und was genau macht diesen Vorgang so komplex, dass er einem neuen Forschungszweig den Aufschwung erbrachte, weil es ohne diesen nicht mehr geht? Um dies wirklich verstehen zu können, ist ein grober Überblick über einige Mechanismen, welche bei der Übersetzung zwischen den Basenpaaren zur fertigen Zelle wirken, unerlässlich. Genau dieser soll nun vermittelt werden.
Offenbar geht es bei der Entschlüsselung der Gene durch den Menschen um ein tieferes Verständnis des menschlichen Organismus und aller bekannten Organismen allgemein. Ein Ziel ist zum Beispiel natürlich eine umfassendere Krankheitsforschung und die damit verbundenen völlig neuen Heilmethoden, die es vermögen könnten, sogar bisher als unheilbar geltende Krankheiten quasi "an der Wurzel" den Garaus zu machen. Wunderbar wäre hier die Möglichkeit zur einfachen, direkten Übersetzung einer analysierten Sequenz in die Verhaltensweisen und die Struktur des später daraus resultierenden Gewebe, aber so einfach macht es uns die Natur natürlich nicht. „Das Klassische Konzept der Genetik und Molekularbiologie, vom Genotyp zum Phänotyp, weicht heute einem modernen Konzept dynamischer Komplexität, dem sogenannten genetisch-metabolischen Netzwerk." [7] Doch zunächst einmal das Grundlegende.
Von besonderer Wichtigkeit sind in jedem Organismus die Proteine. Sie regulieren Funktionen des Stoffwechsels, fungieren als Boten zwischen Zellen und bilden einen wichtigen Bestandteil vieler Teile der Zellen selbst. Ein menschlicher Organismus enthält etwa 35.000 verschiedene Arten von ihnen. Ausschlaggebend für ihre individuelle Funktionsweise ist ihre dreidimensionale Struktur, sie bestimmt welche Bindungen ein Protein mit anderen Molekülen eingehen kann. Proteine bestehen aus einer kettenförmig angeordneten Folge von 20 unterschiedlichen Aminosäuren. Die verschiedenen Wechselwirkungen dieser wiederum bringen diese Kette dazu, sich auf einzigartige Weise anzuordnen, zu verbiegen und zu falten. Bis zu einem gewissen Grad ist die ursprüngliche Aminosäurefolge übersetzbar in die endgültige Struktur des Proteins.
Aber schon von den heiß geliebten Genen bis zu dieser Folge ist es ein langer durchwachsener Weg.

Die aus vier verschiedenen Nukleotid genannten Bausteinen aufgebaute DNA (vergl. Kap. 1.2) ist in jeder einzelnen Zelle eines Organismus enthalten. Entscheidendes Merkmal der DNA ist nun, dass zwei dieser Bausteine jeweils komplementär ineinander übersetzbar sind (Adenin/Thymin, Cytosin/Guanin). Dies erlaubt es Teile eines DNA-Stranges zu kopieren und zu lesen. Bei Letzterem ordnen sich die Basengegenstücke nun an einem freigelegten Teil der DNA an und bilden eine neue Kette, die RNA. Diese neue, komplementäre Kette verlässt dann den Zellkern und wird dann, in einem weiteren komplizierten Vorgang in eine Kette der 20 Aminosäuren übersetzt. Drei RNA-Basen codieren hierbei eine Aminosäure. Schon bis hier sind die Übergänge jedoch alles andere als eindeutig. Die DNA enthält bei weitem mehr Nukleotide als zur Codierung der resultierenden Proteine nötig, die wichtigen Stücke müssen also erst ausgewählt werden. Die drei RNA-Basen mit je vier Möglichkeiten könnten nicht nur 20, sondern 64 verschiedene Aminosäuren codieren und bei der letztendlichen Übersetzung entstünden je nach Wahl der Startbase drei völlig unterschiedliche Aminosäure-

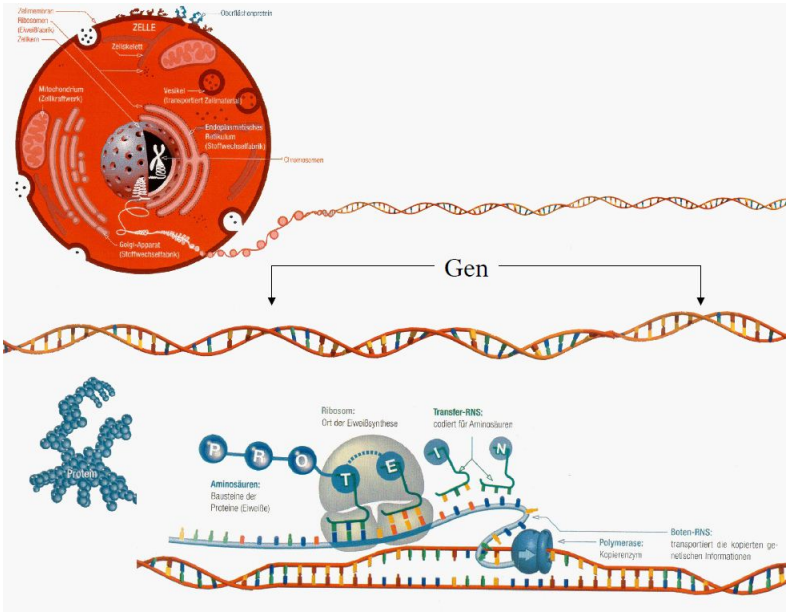


Abbildung 2: Transkription & Translation

ketten. Außerdem kann eine fertige Aminosäurekette zunächst unzählige stabile dreidimensionale Strukturen ausbilden. Bis zur fertigen Form ist wiederum biochemische Hilfe von Nöten!

Es ist zu merken, das zwischen all diesen Prozessen recht komplexe Auswahl- und Regulationsmechanismen wirken, die erst im Zusammenspiel den gewünschten Vorgang bewirken. Außerdem darf nicht vergessen werden, dass der Mensch etwa drei Milliarden Basenpaare hat, in jeder Zelle.
Trotzdem, so glauben Forscher, lohnt sich der Aufwand durchaus; Verständnis über diese Prozesse und Sequenzen bedeutet nicht weniger als Kontrolle über die Proteine, die Bausteine des Lebens. (Frei nach [7])

1.4 Das Humangenomprojekt

Das Humangenomprojekt (HGP) wurde im Jahr 1990 als öffentlicher, internationaler Forschungsverbund gegründet und dauert bis zum heutigen Tag (in Folgeprojekten) an. Es einte und koordinierte viele kleine Forschungsgruppen unterschiedlicher Größe und Struktur, welche langsam begannen, sich der Entschlüsselung des genetischen Codes des Menschen zu widmen und feststellen mussten, dass dies nach damaligem Stand der Technik nicht national in akkurater Zeit schaffbar war. Ein transnationales Forschungsnetzwerk entstand, in welchem insgesamt unter diesem Namen etwa 1000 Wissenschaftler in 40 Ländern gemeinsam mitarbeiteten (USA 62.3%, Großbrittanien 25,1%, Japan 5,5%, Frankreich 2,7%, ab 1995 Deutschland 2,5%, China 1%). Das erklärte Ziel war es nun die Abfolge aller Basenpaare der DNA in den menschlichen Chromosomen zu sequenzieren, also zu lesen und zu speichern. In den Medien war häufig von

„entschlüsseln“ die rede. Dies ist jedoch falsch, da die Entschlüsselung mit der Übersetzung der Genabschnitte in Proteine oder der Erforschung der Funktion und Bedeutung großer Bereiche von Genabschnitten mit proteinfremder Aufgabe (sowie auch völlig funktionslosen DNA-Abschnitten) gleichzusetzen ist. Diese Aufgabe dauert jedoch voraussichtlich noch für längere Zeit an.
Geleitet wurde das HGP von James Watson, welcher zusammen mit Francis Crick die DNA-Struktur erforschte (vgl. Kap. 1.2). Man versprach sich dadurch ein besseres Verständnis über den menschlichen Organismus im Allgemeinen. Insbesondere genetisch bedingte Krankheiten und Defekte sollten besser durchschaut werden können, wodurch neue Heilungsmethoden und Therapien erhofft wurden. Ursprünglich geplant war das Projekt über 20 Jahre bis 2010. Jedoch wurde der gesamte genetische Code, hauptsächlich dank massiver Entwicklung computergestützter Sequenzierungs- und Analysemethoden, bereits 2001 als vorläufige Arbeitsversion vorgestellt und in den Fachzeitschriften “Nature“ (Internationales akademisches Konsortium) und “Science“ (Privates Unternehmen Calera) veröffentlicht. 2003 gilt das Ziel dann schließlich endgültig als erreicht als 99,9 der menschlichen Erbinformation vorlagen.
Die Aufgaben der aufkeimenden Bioinformatik hierbei umfasste eine Vielzahl verschiedener Tätigkeitsfelder. Im Kern stand die eigentliche Sequenzierung (siehe Kap. 2.1), welche zu großen Teilen automatisiert werden konnte und natürlich entwickelt, initiiert und überwacht werden musste. Hierzu wurden viele schnelle, standardisierte Sequenzierungsverfahren durch Weiterentwicklung bekannter Algorithmen erforscht. Die einzelnen gelesenen Abschnitte mussten daraufhin einander zugeordnet und aneinandergereiht werden. Ein weiterer wichtiger Faktor war schließlich die Verwaltung und Speicherung der gewonnenen Daten in möglichst wenig redundanten aber indizierten Datenbanken (siehe Kap. 2.3).
Die heutige Arbeit an dem Thema ist zunächst die weitere Wiederholung der Sequenzierung zur Validierung der Daten. Nach Fachstandard ist diese Prozedur nach siebenmaliger vollständiger Wiederholung durch das Erreichen einer Genauigkeit von 99,99 % abgeschlossen. Parallel dazu läuft die eigentliche Analyse der Daten wie oben beschrieben. Über 1500 Gendefekte und/oder genetisch bedingte Krankheiten oder Anfälligkeiten auslösende Gene wurden bislang zugeordnet. ([8],[10], [5], [1])

2 Bereiche der Bioinformatik

Wenn auch nicht völlig voneinander trennbar, lässt sich die Bioinformatik heute in drei grundlegende Teilbereiche mit voneinander unterscheidbaren Aufgabengebieten und Vorgehensweisen aufteilen, welche im Folgenden jeweils kurz vorgestellt werden sollen: Die Seqenzanalyse (auch molekulare Bioinformatik), die Strukturbioinformatik (hauptsächlich Proteomik) und die Integrative Bioinformatik. [9]

2.1 Sequenzanalyse

Ihre Wurzeln hat die Bioinformatik in der Genomsequenzierung. Für diesen Bereich wurden die ersten Anwendungen entwickelt und er war lange Zeit der Inbegriff informatischer Bemühungen in molekularbiologischer Forschung. Wie in Kapitel 1.3 beschrieben, ist die wichtige dreidimensionale Anordnung der

Proteine über Umwege aus der Sequenz der Basenpaare in den Genen ableitbar. Mit diesem Wissen wurden bereits in den 70ern erste Computeralgorithmen zum Auffinden und Zuordnen von Gensequenzen entwickelt. Die Sequenzierung von Basenpaaren selbst ist ein biochemischer/biotechnologischer Prozess. Primär wird dafür heutzutage die von Frederick Sanger 1975 entwickelte Methode mit Namen Didesoxymethode verwendet. Hierzu werden DNA-Sequenzierungsgeräte unterschiedlicher Form eingesetzt. Die Sequenzierung ist jedoch nicht das eigentliche Problem der Biologie. Zunächst einmal ist das Ergebnis dieser, durch den Vorgang der Didesoxymethode bedingt, meist nicht eine lange Kette von Buchstaben, sondern unzählige kurze Folgen. Diese müssen erst wieder einander zugeordnet und digital zusammengefügt werden, um daraufhin weiter analysiert werden zu können. Erfahrung, also Kenntnis von vergleichbaren Folgen (s.u.) sowie besondere, immer wiederkehrende Zwischenfolgen helfen hierzu Programme zu entwickeln um diesen ersten Schritt zu bewältigen. Was nun folgt ist die eigentlich Analyse der Daten. Allgemein gibt es hierbei zwei verschiedene Muster. Zum einen werden bekannte, typische Merkmale dazu verwendet, in völlig unbekannten DNA- oder Proteinsequenzen neue Strukturen zu finden. Dies ist die eigentliche Sequenzanalyse. Solche typischen Merkmale können zum Beispiel bekannte Start- und Stopfolgen in DNA sein, welche bekanntermaßen den Anfang und das Ende eines gencodierenden Abschnitts markieren. Ein weiterer wichtiger Ansatz ist, bereits bekannte Strukturen in neuen, frisch gewonnenen Folgen wiederzufinden. Denn es wird allgemein angenommen, dass ähnliche Genabschnitte auch ähnliche Aminosäuren codieren. Auch das Wissen, dass drei Nukleotide genau eine Aminosäure codieren könnte man als so ein Merkmal aufführen. Wichtig ist nur, dass diese Merkmale allgemein gültig sind, bzw. zumindest innerhalb eines Organismus gewisse Gültigkeit besitzen. Früh wurden also Computer dazu verwendet, solche Merkmale und bekannten Muster in ihnen zur Verfügung gestellten Sequenzen jedweder Art zu suchen. Komplexere Algorithmen ließen es bald bereits zu, einige Genabschnitte auf diese Weise direkt zu markieren und kartographieren. Ein völlig anderer und allgemein wichtigerer Punkt ist nun der Vergleich mehrerer zugeordneter Muster, dies nennt sich Sequenz-Alignment, weil hierzu mehrere DNA, RNA oder Aminosäuresequenzen zum Beispiel untereinander angeordnet und miteinander verglichen werden. Ziel dieser Vorgehensweise ist das Auffinden von Ähnlichkeiten zwischen vergleichbaren Abschnitten verschiedener Organismen, etwa zwischen Katze und Hund. Zwei Abschnitte sind hierbei vergleichbar, wenn durch sie gleichartige oder ähnliche Zellformen, etwa die Färbung der Haut, codiert werden. Man fand heraus, dass sich durch Ähnlichkeiten und Unterschiede solcher Folgen oft Rückschlüsse auf evolutionäre Verwandtschaft und Parallelentwicklung schließen lassen. Die wichtigsten Begriffe sind die der Ähnlichkeit und der Edit-Distanz. Die Edit-Distanz ist ein Wert, der sich aus der Anzahl der einzufügenden und / oder zu ersetzenden Stellen ergibt, die benötigt werden, um zwei Folgen einander anzugleichen. Der eigentliche Schritt ist nun die Berechnung des optimalen Alignments, also derjenigen Sequenzabschnitte mit der geringsten Edit-Distanz. Auch hierbei finden Forscher inzwischen Hilfe bei einer Vielzahl bekannter Gen Anfangs- und Endsequenzen sowie weiterer charakteristischer Merkmale. ([2])
Besondere Beachtung ist hierzu dem "BLAST" Algorithmus zu geben. Das Basic Local Alignment Search Tool umfasst die weltweit wichtigsten Algorithmen und Programme zu diesem Thema. Nach Organismus, Proteinabschnitt und Muster (DNA/RNA/Aminos.) geordnet, stehen diese im Internet für Bioinformatiker

Abbildung 3: BlueGene/L

frei zur Verfügung. Eine Erweiterung und Verbesserung dieser läuft ohne Unterbrechung. [12]

2.2 Strukturbioinformatik

Mit den Informationen, die mit den aus dem vorherigen Kapitel bekannten Techniken gewonnen werden konnten, vervollständigen sich nun zum Beispiel Bruchstücke von DNA zu vollständigen Genen und kurze Aminosäurefolgen zu ganzen Proteinen bis zu vollständigen Zellen. Die Frage, welche sich dem Bioinformatiker als nächstes aufdrängt, ist natürlich die der Funktion dieser Eiweiße innerhalb eines Organismus. Wie in Kapitel 1.3 beschrieben, ist die endgültige Form des fertigen Proteins von zentraler Bedeutung für seine spätere Funktion. Beides zu erforschen, zu simulieren und vorherzusagen ist die zweite zentrale Aufgabe der Bioinformatik. Insbesondere die spätere Funktion des Proteins zu beschreiben steht dem komplexen Problem gegenüber, dass die Proteine innerhalb einer Zelle in unzähligen Wechselwirkungen miteinander stehen und auch durch äußere Einwirkungen beeinflusst werden, welche zur genauen Vorhersage des Lebenszyklus eines Proteins vollständig mit einbezogen werden müssten. Das ist schwierig. Die Forschung auf dem Gebiet der Simulation einzelner Proteinfaltungen schreitet aber rasant voran. Als Beispiel für den Nutzen dessen sei etwa genannt, dass die genaue Kenntnis über die Form der Proteine von Krankheitserregern es ermöglicht, entsprechende Moleküle zu konstruieren die diese schlichtweg deaktivieren. Krankheiten wie Krebs und Aids könnten so (wie teilweise auch schon geschehen) deutlich gemindert, wenn letztendlich nicht sogar geheilt werden.
Um also die vielen Möglichkeiten einer Proteinfaltung, oder die Bindungsmöglichkeiten und Funktionen eines fertigen Proteins simulieren zu können, ist massiver Rechenaufwand von Nöten. Um dies zu verdeutlichen sei hier das Forschungszentrum Jülich, in Jülich (Nordrhein-Westfalen), aufgeführt. Dort wird im Institute for Advance Simulation IAS unter anderem zur Simulierung und Visualisierung von Proteinstrukturen ein BlueGene/P Supercomputer verwendet. Diese auf dem 2004 von IBM entwickelten BlueGene/L aufbauende Serie wurde dort 2007 eingeführt und im Mai 2009 weiter aufgerüstet und rechnet aktuell mittels 294.912 hochparallelen 850 MHz Prozessoren mit einer Spitzenleistung von 1 Petaflop. Damit ist er aktuell der schnellste Rechner Europas und der drittschnellste der Welt. [4]

2.3 Integrative Bioinformatik

Ein weiterer wichtiger Teil ist die Speicherung und Verwaltung der gewonnenen Daten. Was zunächst überschaubar klingt, erlangt seine Schwierigkeit durch die besonders großen Datenmengen, die die Erforschung von Organismen auf molekularer Basis mit sich bringt, sowie die aktuell große Anzahl an redundanten biologischen Datenbanken mit teils jeweils eigener Nomenklatur. Eine mangelhafte Kontrolle dieser Daten bedeutet redundante und somit überflüssige oder sogar falsche Forschung. Das Ziel der Integrativen Bioinformatik ist die Indizierung und Zuordnung der Daten. Ein digitales Netzwerk soll erstellt werden, indem Sequenzen logisch indiziert sind, DNA-Stränge mit Genabschnitten kartographiert sind, diese Gene wiederum den zugehörigen Proteinen zugewiesen sind und typische Proteinfaltungen sowie endgültige dreidimensionale Strukturen dieser beigefügt, in ihren Funktionsweisen und Eigenschaften beschrieben und schließlich ihre Rollen in Musterorganismen deutlich gemacht wurden. In dieser Aufgabe steht die Bioinformatik jedoch noch ganz am Anfang. Ein wichtiges Werkzeug hierfür ist natürlich das Internet. Metasuchmaschinen liefern bereits sinnvolle Ergebnisse zu fachspezifischen Anfragen über gespeicherten Strukturen oder frei zugängliche Algorithmen für die weitere Erforschung dieser über eine Vielzahl von internationalen Datenbanken hinweg. Einige Algorithmen und Programme bedienen sich sogar eigenständig dieser Schnittstelle, um zum Beispiel aktuelle, bekannte Strukturen in ihre Suche mit einzubeziehen (siehe Kap. 2.1). Private Dienstleister entwickeln neue Zugangstechniken, Strukturierungsmechanismen und Suchalgorithmen, um diese dann Forschungsunternehmen weltweit zur kostenpflichtigen Nutzung anzubieten (siehe zum Beispiel [2]). Bei der Entwicklung dieser ist es selbsterklärend unumgänglich Wissen sowohl im Bereich der Biochemie zu haben, da auf dessen Forschung die Entwicklung der integrativen Programme abzielt und sich an ihr orientiert, als auch auf dem Gebiet der Informatik zu besitzen, da diese erst die nötigen Werkzeuge und das Know-How liefert, die benötigt werden, um diese Programme überhaupt entwickeln zu können. Der Bioinformatiker ist also wie hierfür gemacht.

3 Studium Bioinformatik

3.1 Warum Bioinformatik studieren?

Wie in Kap. 2 deutlich geworden sein sollte, hat sich die Bioinformatik zu einem unverzichtbaren Feld der modernen Forschung in den Bereichen Biologie, Biochemie, Bio- und Medizintechnologie entwickelt. Eine große Nachfrage an Absolventen mit fundierten Kenntnissen auf beiden Seiten dieser Schnittstellenwissenschaft besteht nicht nur auf akademischer Seite vieler Forschungseinrichtungen weltweit, sondern auch im industriellen Umfeld. Denn die Werkzeuge und Vorgehensweisen der Bioinformatik unterstützen nicht nur die Forschung, sondern auch bereits viele private Unternehmen. Die Aufgabenbereiche die diese Unternehmen kommerziell decken sind vielfältig. So entwickelt beispielsweise die Hamburger *emplics AG* zusammen mit der Norderstedter *c.a.r.u.s. Information Technology AG* gebrauchsfertige Hochleistungscomputer, auf denen die wichtigsten Anwendungen der Bioinformatik inklusive entsprechendem Linux

[2] `http://www.integrativebioinformatics.com/`

Betriebssystem bereits vorinstalliert sind. Diese sind in vielen Fällen direkt im Forschungsfeld einsetzbar, wodurch viel Zeit gespart werden kann.
Wie in Kap. 2.3 erkennbar, haben sich inzwischen durch neuartige biologische / biochemische Experimente große Datenmengen aufgestaut. Bis zum heutigen Tag kann, gerade im Bereich der Sequenzierung, von einer wahren Datensammelwut gesprochen werden. Diese Daten nutzbar zu machen ist zu größten Teilen Aufgabe des Bioinformatikers. Damit versprechen sich Experten einen enormen Zuwachs an biologischem und biochemischem Wissen. Außerdem entsteht hieran ein immer größer werdendes ökonomisches Interesse wie zum Beispiel im medizinisch-pharmazeutischen Bereich. [3]

3.2 Das Studium der Bioinformatik am Beispiel der Universität Hamburg

Seit Juli 2002 ist das Zentrum für Bioinformatik, das ZBH, Teil der Universität Hamburg. Durch ihn wird der spezielle Anspruch der Interdisziplinarität erfüllt, der Voraussetzung für Lehre und Forschung auf diesem Gebiet ist.
Seit dem Wintersemester 2006/07 wird hier die Bioinformatik als zweijähriger Masterstudiengang angeboten. Zugangsvoraussetzung hierzu ist der Abschluss in einem lebenswissenschaftlichen oder informatisch-orientierten Fach. Im Laufe des Studiums besteht die Möglichkeit, sich auf eines der Themen *Genominformatik*, *Strukturelle Bioinformatik* oder *Chemieinformatik / Wirkstoffdesign* zu spezialisieren welche folgende Inhalte vermitteln sollen:

- Die **Genominformatik** beschäftigt sich mit der Nutzbarmachung und Analyse der heutzutage im industriellen Maßstab produzierten Sequenzen kompletter Genome, welche riesige Mengen Daten verschiedenster Art mit sich bringen. Hier behandelte Projekte beschäftigen sich mit der Suche nach Mustern in Sequenzen oder neuen Methoden zur Analyse dieser.

- Das Feld der **Strukturellen Bioinformatik** erstreckt sich über die Simulationsmethoden der Physik und Proteinbiochemie zur Beantwortung spezieller Fragestellungen an Proteinstrukturen mit bestimmten Eigenschaften. Aktuelle Projekte sind etwa die Klassifizierung von Proteinen, die digitale Modellierung von Proteinen oder die Vorhersage ihrer Struktur anhand ihrer Aminosäuresequenz.

- **Cheimieinformatik / Wirkstoffdesign** behandelt schließlich die Weiter- und Neuentwicklung von Methoden zur digitalen Modellierung von Molekülen aller Art. Dies geht von der Visualisierung über die Analyse bis zur Vorhersage von Moleküleigenschaften. Aktuelle Projekte behandeln das zweidimensionale digitale Zeichnen von molekularen Strukturen oder die Modellierung riesiger Makromoleküle.

Das Studium gliedert sich in zwei Abschnitte. Zunächst werden Grundlagen von im bisherigen Studium nicht behandelten Basisdisziplinen sowie die Grundlagen der Bioinformatik selbst vermittelt. Dies wird anhand einer Angleichungsphase (1. Fachsemester) und einer Bioinformatik-Grundausbildung (5 Pflichtmodule 1./2. Semester) erreicht. Danach steht eine "forschungsorientierte,

[3] `http://www.zbh.uni-hamburg.de/study/occupational_image/index.php`

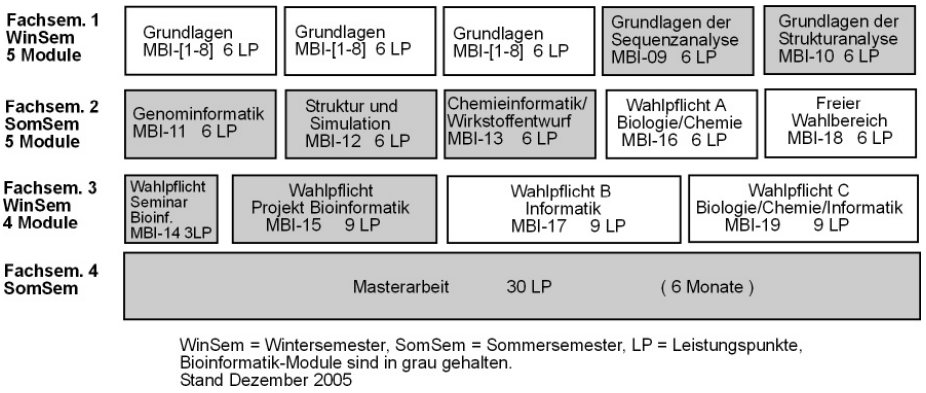


Abbildung 4: Aufbau des Studienganges

fachübergreifende Ausbildung in Bioinformatik im Vordergrund"[11] die überwiegend über Wahlpflichtmodule vermittelt wird (ab dem 2. Semester).

3.3 Berufsbild

Das mögliche Aufgabenspektrum eines Bioinformatikers ist vielseitig. Absolventen können neben der Genomforschung zum Beispiel in der Arzneimittelforschung arbeiten. Auch in den Bereichen Zell- und Molekularbiologie sind Bioinformatiker unverzichtbar. Mögliche Arbeitgeber sind Pharma-, Pflanzenschutz- oder Biotechnologieunternehmen.
Ein wichtiger Faktor ist, ob sich ein Bioinformatiker eher in die naturwissenschaftliche oder die mathematisch/informatische Richtung spezialisieren will. Die bisher genannten Bereiche der Entwicklung und Simulation sind eher zweiterem zuzuordnen. Denn zur Entwicklung komplexer Algorithmen zum Thema wird häufig nur eine grundlegende Ausbildung im naturwissenschaftlichen Bereich und eine tiefergehende, umfangreichere Kenntnis informatischer Methoden benötigt. Andersherum ist ein Gewicht bei der Biologie/Biochemie meist eine bessere Voraussetzung, um aktiv die naturwissenschaftliche Forschung voranzutreiben und dabei bioinformatische Methoden “nur“ anzuwenden. Diese Spezialisierung scheint sich jedoch häufig erst einige Zeit nach dem Studium herauszubilden.
Weitere mögliche Aufgabenbereiche sind „die Simulation und Steuerung chemischer Prozesse, die biomedizinische Wissensverarbeitung, die Erstellung und Pflege von Reaktions- und Stoffdatenbanken, die computergestützte Synthese, die Auswertung von Daten mit Methoden der Mustererkennung und künstlicher Intelligenz oder die Robotik zur Automatisierung chemischer und biologischer Analysen und Synthesen“. [4] Des Weiteren benötigen unzählige Forschungsinstitue allgemeine IT-Experten die die Sprache der Wissenschaft verstehen können. „Auch in der Automatisierungstechnik, der Luft- und Raumfahrt-Industrie und in der Mikroelektronik-Industrie sind die Experten gefragt. Nicht zuletzt Unternehmensberatungen stellen die strukturiert denkenden Männer und Frauen mit den harten und den Soft Skills ein - denn sie suchen Mitarbeiter aus den naturwissenschaftlichen und technischen Fächern.“ Wie hiersaus bereits erkenn-

[4] `http://it.monster.de/2143_DE_p1.asp`

bar sein sollte, herrscht sowohl in der Forschung als auch in der Wirtschaft ein wahrer Mangel an interdisziplinären Schnittstellenexperten wie dem Bioinformatiker.

4 Aktuelle und zukünftige Anwendungsmöglichkeiten

4.1 Allgemeines

Wie nun bereits mehrmalig erwähnt, ist eines der großen Ziele der Bioinformatik Informationen über Krankheitsursachen aus der menschlichen DNA zu gewinnen und somit eine Früherkennung und Heilung dieser Krankheiten voranzutreiben oder überhaupt erst zu ermöglichen. Doch wo im bisherigen Teil dieser Arbeit der Forschungsaspekt und Wissensgewinn im Vordergrund stand, soll hier daran erinnert werden, dass am Ende eher die Umsetzung dieses Wissens in vermarktungsfähige Medikamente und in der Praxis anwendbare Methoden wichtig ist. Damit hat die Bioinformatik auch einen bedeutenden Einfluss auf den Verlauf der fachbezogenen Wirtschaft und Finanzwelt. Mit der Entschlüsselung der Daten aus dem HGP (Kap. 1.4) durch die Zuweisung der Funktion und den Aufbau der menschlichen Gene und Genprodukte schreitet genau dieser Teil voran. Schon die daraus resultierte Erkenntnis, dass die Anzahl der menschlichen Gene viel geringer ist als ursprünglich angenommen hat bereits beträchtlichen Einfluss. Denn wie bereits in Kap. 1.3 deutlich gemacht, konnte nun nicht mehr ignoriert werden, dass die alte Schule der Molekularbiologie neu überdacht werden muss. Es wurde deutlich, dass mit "Abschluss" der humanen Genomsequenzierung, von deren Ergebnissen sich unzählige Pharmakonzerne herausragende Vorteile versprachen oder gar darin die Zukunft der modernen Pharmazie und Medizin im Ganzen sahen, die eigentliche Arbeit erst begann. Diese Arbeit und Hoffnung liegt nun auf den Schultern der Bioinformatiker, denn sie sind heutzutage der Motor der molekularbiologischen Forschung. Natürlich darf nicht vergessen werden, das allgemeinhin mathematische Modelle erst mit Überprüfung durch experimentelle Ergebnisse, oder Bestätigung Selbiger, an heuristischer Relevanz erlangen. Dies ist weiterhin Aufgabe der Biochemie, wenn auch mit Unterstützung durch Automatisierung und Standardisierung. Die Bioinformatik beschreibt und erklärt mit ihren Analysen und Vorhersagen die, für sich selbst, nichtssagenden Experimentergebnisse der Naturforscher und verhilft diesen zu besseren, zielgerichteteren Experimenten.

4.2 Genchips

Neben den erwähnten Anwendungen gewinnt vor allem der Bereich der Biosensorik und sogenannter Genchips durch die fortschreitende Entwicklung in der Bioinformatik immer mehr an Bedeutung. Unter Microarrays versteht man molekularbiologische Untersuchungssysteme, die parallele Analyse von mehreren tausend Einzelnachweisen erlauben, wobei für die Analyse eine nur sehr geringe Menge des Probenmaterials nötig ist. Dieses Anwendungsgebiet hat sich seit den 90er Jahren als wichtiger Bestandteil in der Forschung für die Bereiche Pharmazie, Medizin, Biochemie, Genetik und Molekularbiologie durchgesetzt. Durch dieses Anwendungsgebiet der automatisierten Auswertung von Ergebnissen ist

r 

Abbildung 5: Ampli-Chip CYP450

es möglich, eine hohe Anzahl an Tests pro Zeiteinheit mit vergleichsweise geringen Probenmengen vorzunehmen und so Kosten extrem zu senken. Bisher gelangte man in der Forschung nur durch aufwendige Laborversuche mit hohem Zeit- und Kostenfaktor zu ähnlichen Ergebnissen, die mit wiederum aufwendigen Verfahren ausgewertet werden mussten. Konkret bestehen Biochips aus einem Trägermaterial, auf dem sich eine große Zahl biologischer oder biochemischer Nachweise oder Tests auf engstem Raum befinden. Die Informationen werden hier nicht durch elektrische Signale, sondern durch biologische Moleküle vermittelt. Biochip ist ein Sammelbegriff für eine Vielzahl unterschiedlichster Testmethoden und technischer Verfahren. So gibt es heute je nach Einsatzzweck viele verschiedene Arten von Genchips. Eine besondere Rolle spielen hierbei, auch im Hinblick auf die Bedeutung in der Bioinformatik und der DNA-Analyse, die DNA-Microarrays. Sie finden zunehmend Anwendung in der Genomanalyse, der Diagnostik und bei Untersuchungen in der differenziellen Genexpression, also der Art der Ausprägung von Genen zum letztendlichen Phänotyp. Genchips bzw. DNA-Microarrays sind eine Methode um die unterschiedliche Genexpression in Zellen verschiedener Gewebe bzw. unter verschiedenen Einflüssen zu bestimmen. Das Wissen wann welche Gene in der Zelle exprimiert werden, trägt entscheidend zum Verständnis von metabolischen Netzwerken und der Herstellung von Arzneimitteln bei. Nachdem die Bioinformatik zunächst Möglichkeiten zur Genomentschlüsselung und deren Verständnismodell bereitgestellt hat, entwickeln nun die einzelnen Forschungsbereiche der Bioinformatik, wie zum Beispiel die Genchips, weitere Methoden und Modelle zum Umgang mit der neu gewonnen Datenflut. Entscheidend sind hierbei die automatisierte Auswertung und auch die automatisierte Gewinnung von Messergebnissen durch Genchips. Man geht davon aus, dass der Genchip die Gentechnologie dramatisch beeinflussen wird, so wie seinerzeit der Computer-Chip die Elektronikindustrie revolutionierte. Der Genchip macht eine völlig neue Art der Genanalyse möglich und wird in künftigen Anwendungen dank Massenproduktion als preiswertes Hilfsmittel unverzichtbar sein.

Was zunächst noch experimentelle Forschung war, soll künftig als Massenprodukt zur Verfügung stehen, um zum Bespiel Tests auf Erbkrankheiten zu ermöglichen, die ohne größeren Aufwand in jedem Krankenhaus oder jeder Apo-

theke zur Verfügung stehen. So könnte unter anderem rechtzeitig geprüft werden, ob eine genetische Veranlagung für Brustkrebs oder Herz- und Kreislaufleiden vorliegt. Der weltweit erste Gen-Chip für die klinische Anwendung ist in Europa 2004 zugelassen worden. Der Ampli-Chip CYP450 der Firmen Roche und Affymetrix soll Ärzten helfen, die Arzneimittel ihrer Patienten individueller als bisher dosieren zu können. Durch diesen Chip werden zwei Gene für das Stoffwechselenzym Cytochrom P450 analysiert, welches im Stoffwechsel des Menschen für den unterschiedlich schnellen Abbau vieler Medikamente zuständig ist untersucht. Durch die genaue Kenntnis dieses Stoffwechselvorganges kann nun der Mediziner bereits bei der Dosierung der entsprechenden Medikamente auf den einzelnen Patienten eingehen. Damit ist die Zukunftsvision der personalisierten Medizin nicht nur in greifbare Nähe gerückt, sondern wurde als erster Schritt bereits zur Marktreife gebracht und umgesetzt.

4.3 Ergänzung

Die Genomforschung ist jedoch nur eines der Themengebiete, in dem die Interdisziplinarität von Bioinformatikern unerlässlich wird. Auch zum Beispiel in den Neurowissenschaften, mit ihren neuronalen Netzen, der KI-Forschung und autonomen Systemen ist dies gefordert. Dies wiederum beleuchtet einen völlig neuen, bisher eher vernachlässigten Aspekt der hier nur kurz erwähnt werden soll:

Auch die Informatik und Mathematik lernt von der Biochemie. Wie in jedem anderen Bereich von Wirtschaft und Wissenschaft auch, dient die Natur für die Informatik als ein Vorbild und Inspiration zur Entwicklung neuer Anwendungen und Methoden. Wie erwähnt, gilt dies unter anderem gerade für die Entwicklung von KI und autonomen Systemen wie Robotern. Und natürlich ist diese Inspiration besonders dort einflussreich, wo die Forschungsbereiche eng zusammenarbeiten. Die Bioinformatik ist, und das sei hier ganz besonders hervorgehoben, also nicht mehr bloß ein Forschungszweig, der Biologen, Biochemiker und andere Naturwissenschaftler mit neuen Methoden und Werkzeugen unterstützt. Vielmehr ist sie als interdisziplinäre Schnittstelle zu sehen, welche durch ihre Grenzforschung ein "Erkenntnisfeedback" an alle beteiligten Wissenschaften zurückgibt und diese fördert. Sie ist eine eigenständige Wissenschaft mit eigenen Methoden und Werkzeugen. Die Ergebnisse die während der Forschung zwischen Biologie, Biochemie, Physik, Informatik und Mathematik hiermit entstehen, lassen sich nicht mehr einer dieser Wissenschaften zuordnen. Denn erst das Zusammenspiel dieser machte diese Ergebnisse überhaupt erst möglich.

5 Ethik

Durch die Förderung der menschlichen Genomforschung und auch weiterer Aspekte wie der Künstlichen Intelligenz durch die Bioinformatik sind Fragen über ethische Konflikte nicht völlig ungerechtfertigt.
Die Kosten für die Sequenzierung eines kompletten, menschlichen Genoms sind durch Optimierung oben genannter Methoden und der Möglichkeit zur teilweise vollständigen Automatisierung in den letzten Jahren rapide gefallen und fallen weiter. Wo dies zur Zeit des Humangenomprojekts, also sogar noch am Anfang dieses Jahrtausends, noch mit enormen Aufwand und Kosten verbun-

den war, wird es laut aktueller Entwicklungen schon bald möglich sein, anhand einer DNA-Probe eines beliebigen Menschen, ähnlich etwa eines Vaterschaftstests, kostengünstig ein vollständiges Bild seiner Gene zu bekommen. Bekanntlich können aus diesen Genen Informationen gewonnen werden, die zum Beispiel für einen möglichen zukünftigen Arbeitgeber sehr interessant sein dürften. Es drängen sich nun bereits recht entscheidende Fragen auf, wie etwa folgende:

- Wie weit darf es legal/normal sein, dass ein Arbeitgeber von Bewerbern genetische Informationen erlangt?
- Wie weit darf es ein Standard sein, dass genetische Informationen über Personen vom Staat gespeichert werden?
- Wie weit dürfen diese Daten für die Öffentlichkeit oder verschiedene Staatsorgane einsehbar sein?
- Wenn diese Daten so leicht zu beschaffen sind, wie weit kann dann der Einzelne überhaupt noch über deren Verteilung entscheiden?

Auch die Veränderung von DNA und Proteinen, sowie die aufkeimende Möglichkeit zur Erzeugung und Modellierung wirft grundlegende neue Fragen auf, wie etwa:

- Wie viel ist Leben überhaupt noch wert in einer Welt in der Menschen ihre Körper grundlegend verändern können?
- Wie viel ist Leben überhaupt noch wert in einer Welt in der Menschen neues Leben formen und erschaffen können?
- Darf das Kind der Zukunft eine optimierte Version der Gene seiner Eltern erhalten?
- Wo führt zum Beispiel die Minderung oder Auslöschung von Krankheiten wie Krebs oder Aids möglicherweise hin, wenn man etwa das schwankende Gleichgewicht der Weltbevölkerung betrachtet? [3]

Literatur

[1] Ordnung in die datenflut. *Life Science Nord*, 2009.

[2] Uta Bohnebeck. Sequenzvergleiche in der bioinformatik. *FIfF*, Januar 2003.

[3] Klaus Fuchs-Kittowski. Bioinformatik: eine interdisziplinäre wissenschaft. *FIfF*, Januar 2003.

[4] Institute for Advanced Simulation FZ Jülich. http://www.fzjuelich.de.

[5] Lisa Gannet. http://plato.stanford.edu/entries/human-genome/.

[6] Schweitz Institut Bioinformatik. http://www.isb-sib.ch/.

[7] Sigrid Schmitz. Schmökern im buch des lebens. *FIfF*, Januar 2003.

[8] Gholamali Tariverdian Werner Buselmaier. *Humangenetik für Biologen.* Springer, 2005.

[9] Wikipedia. Bioinformatik.

[10] Wikipedia. Humangenomprojekt.

[11] Hamburg Zentrum Bioinformatik. versch. flyermaterial.

[12] Saarbrücken Zentrum Bioinformatik. http://zbi-www.bioinf.uni-sb.de.

Datensammelwut

Jurek Frunzke, Daniel Gleim und Hendrik Pfeifer

Zusammenfassung

Bei unserem Thema Datensammelwut haben wir uns auf das Sammeln von personenbezogenen Daten konzentriert. Dazu haben wir zunächst einmal die Frage geklärt, was eigentlich Daten sind und wie diese gesammelt werden können. Speziell nehmen wir hierzu die Rolle von Google unter die Lupe. Danach richten wir unser Augenmerk auf den Nutzen der gesammelten Daten, die Gefahren, die daraus entstehen können und den Datenschutz, der dadurch nötig wird.

Detailliert befassen wir uns dann mit Institutionen die den Datenschutz ermöglichen, erkämpfen oder durchzusetzen versuchen. Abgeschlossen wird unser Text mit einigen Beispielen, wo der Datenschutz versagt hat und was die Folgen waren, sowie mit einer kritischen Betrachtung des ELENA Verfahrens.

1 Was sind *Daten*? [1][2]

1.1 Personenbezogene Daten

Personenbezogene Daten sind alle Angaben über eine Person, die entweder bestimmt oder bestimmbar ist. Bestimmt ist eine Person, wenn durch eine Aussage eindeutig hervorgeht, um welche Person es sich handelt. Bei der Aussage „Hans Mustermann hat blaue Augen“ wäre jedem klar, welche Person hier gemeint ist. Eine Person ist bestimmbar, wenn aus der Aussage ableitbar ist, um welche Person es sich handelt. „Der amtierende Bürgermeister von Hamburg ist homosexuell“ jeder sollte wissen, dass damit Ole von Beust gemeint ist. Es lässt sich jedoch auch durch andere Eigenschaften eine Person eindeutig identifizieren. „Die Fahrerin des Autos mit dem Kennzeichen HH-XX-1234 arbeitet bei der Hamburger Sparkasse“ auch hier wäre die Person, die gemeint ist, ebenso bestimmbar wie im ersten Beispiel, obwohl es schwieriger ist, diese Person zu bestimmen.

Der Begriff „Personenbezogene Daten“ stammt aus dem Datenschutzrecht. In Deutschland werden jedoch nur personenbezogene Daten von natürlichen Personen geschützt. Als eine natürliche Person wird jeder Mensch bezeichnet, der rechtsfähig ist. In Deutschland ist man nach Vollendung der Geburt rechtsfähig. Das Komplement der natürlichen Person, ist die juristische Person. Eine juristische Person ist ein Zusammenschluss von Personen, der gesetzlich anerkannt ist und somit auch rechtsfähig ist.

1.2 Rechner Daten

Rechner Daten sind alle Daten, die der Rechner von sich preisgibt. Als Beispiele wären hier zu nennen die Browser-Informationen, Verbindungsdetails, Display-

und Layout-Einstellungen, Script-Eigenschaften, System-Eigenschaften und lokale Information.

Jeder Browser teilt der angewählten Seite mit, über welchen Provider der User gerade surft, dadurch lässt sich dessen Standort bestimmen. Hinzu kommen über 100 Details zu den bereits erwähnten Einstellungen.

Der Browser tut dies um die Seite optimal anzeigen zu können. Wenn der User ein Display der Größe 11 Zoll hat und die Grafikeinstellung von 800*600, so wird die gewünschte Seite auch genau so angezeigt. Entsprechend verhält es sich auch beispielsweise mit den Scripteigenschaften, wie JavaScript. Das Ziel von Datensammlern ist es nun, personenbezogene Daten und Rechner Daten zu verknüpfen, sodass ein umfangreiches Profil von jedem Surfer erstellt werden kann.

1.3 Wie werden Daten gesammelt?

Daten können nicht nur von einem Browser gesammelt werden. Zwei weitere und einfache Möglichkeiten sind das Einsetzen von Cookies und Speichern von Formular-Daten.

1.3.1 Cookies

Ein Cookie ist in der Regel eine Textdatei, die erzeugt wird, weil eine Webseite, auf die der Benutzer zugreifen will, eine Cookie Information sendet beziehungsweise empfangen will. In der Textdatei ist der Inhalt frei wählbar, das heißt die Webseite bestimmt ob über das Cookie lediglich eine Identifizierung stattfindet, oder welche Informationen gespeichert werden sollen.

Cookies sind also dann von Nutzen, wenn der Benutzer regelmäßig ein und dieselbe Webseite besucht, auf der er bestimmte Einstellungen vornehmen kann und diese speichern möchte, wie zum Beispiel in einem Forum sein Login. Ein Cookie ermöglicht jedoch auch das Speichern von Informationen während einer Sitzung. Wenn der Benutzer also auf der Seite eines Onlineshops etwas bestellt, werden seine relevanten Daten zur Lieferung in einem Cookie gespeichert, sodass er diese nicht jedes mal neu eingeben muss, wenn er eine Seite zurück geht, oder vielleicht noch etwas dazu bestellen will.

Ein Cookie ist also eigentlich sehr sinnvoll und erleichtert dem Benutzer den Umgang mit einigen Webseiten. Leider kann durch einen Cookie auch versucht werden, einen Benutzer im Internet zu verfolgen. Es ist nämlich für viele Seiten von Interesse, auf welchen anderen Seiten der Nutzer war, um eine möglichst personalisierte Darstellung der Seite zu gewährleisten. Dieses Profil wird vor allem in der Werbe-Industrie genutzt.

1.3.2 Formulardaten

Jeder Surfer hat wahrscheinlich im Internet schon seine persönlichen Daten, wie seine Anschrift oder sogar die Bankverbindung, in ein Formular einer Webseite geschrieben. Es ist ein Leichtes, diese Daten nun auf dem Server der Webseite zu speichern. Selbst wenn der Benutzer nicht zustimmt, wird dies oft gemacht, da es sehr schwierig ist nachzuweisen, wer überhaupt Zugriff auf Daten hat und vor allem woher.

1.4 Google

Je größer ein Dienstleister im Internet ist, desto öfter kommt er auch an Daten, die alle zusammengefasst eine umfangreiche Datenbank ergeben. Im Fall von Google ist diese Datenbank sogar einer der Grundsteine des Unternehmenserfolgs, da der Suchalgorithmus von Google auch die Suchanfragen der anderen Benutzer und die vorherigen Seiten des momentanen Nutzers in die Berechnung mit einfließen lässt.

Google muss in diesem Zusammenhang erwähnt werden, weil heutzutage fast jeder Internetbenutzer in irgendeiner Art und Weise die Dienste von Google nutzt. Google speichert zu jeder Suchanfrage den Länder-Code, die Suchanfrage, die IP Adresse, die Sprache, die Anzahl der Ergebnisse und die Klicks auf die Links in der Suchanfrage. Dazu kommen natürlich auch die zahlreichen Informationen von Google Mail, YouTube, Google Maps und allen anderen Diensten des Unternehmens.

Solange es Google finanziell gut geht, sind all diese Informationen sicher und es ist im Interesse eines Jeden, dass dies auch so bleibt.

1.5 Nutzen von gesammelten Daten

Der Nutzen von Daten, die gesammelt und gespeichert worden sind, entsteht vor allem durch die Personalisierung. Durch die Personalisierung können Webseiten besser für den Benutzer angezeigt werden, da der Benutzer zum Beispiel Einstellungen speichern kann oder er nicht immer wieder seine Kennung eingeben muss. Google nutzt, wie bereits erwähnt, diese Daten sogar zur Optimierung der Suchergebnisse.

Es sind aber auch die Rechnerdaten von Interesse, denn durch ihre Auswertung wissen die Betreiber zum Beispiel, welcher Browser vorzugsweise benutzt wird oder aus welchem Land die Benutzer überwiegend kommen oder aber auch ob die Benutzer per Handy oder Computer surfen.

Den größten Nutzen hat jedoch die Werbeindustrie. Sie kann gezielte Werbung schalten und so die Kosten senken bzw. die Effektivität der Werbung um ein Vielfaches erhöhen. Für den Benutzer kann dies auf einigen Seiten sehr lästig sein, jedoch ist im Endeffekt auch niemand gezwungen, aufgrund der Werbung etwas zu kaufen.

1.6 Gefahren

In der heutigen Zeit wird versucht, alles zu digitalisieren. Durch die immer wachsenden Rechnerkapazitäten - auch im Bezug auf die Menge an Speicherplatz - werden überall Daten gesammelt und gespeichert.

Die eigentliche Gefahr ist der Kontrollverlust des Benutzers über die Daten. Dieser weiß oftmals gar nicht, wer überhaupt seine Daten hat und woher er diese bezogen hat. Oftmals bekommt der Benutzer es nämlich nicht mit, wenn seine Daten missbraucht werden. Ein gutes Beispiel ist in Deutschland die Schufa. Jeder Vertrag, der abgeschlossen wird, sei es ein Kaufvertrag oder ein Kreditvertrag etc. wird der Schufa gemeldet. Die Schufa speichert diese Daten und verkauft diese an Dritte, die zum Beispiel die Kreditwürdigkeit einer Person prüfen wollen. Ein bekanntes Phänomen ist, dass oft falsche Daten gespeichert

werden. Es kommt zu Verwechselungen oder ein Unternehmen vergisst der Schufa mitzuteilen, dass die nicht bezahlte Rechnung nur ein Missverständnis war.

Durch unter anderem diesen Zwang zur Veröffentlichung entsteht der „Gläserne Bürger“. In der Theorie ist der „Gläserne Bürger“ ein Bürger über den jeder Mensch alles weiß oder herausfinden kann. Das ist natürlich in der Realität noch nicht der Fall, doch vor allem Datenschützer warnen vor der Entwicklung, die nämlich genau darauf zuführt.

2 Datenschutz [3][4]

2.1 Bedeutung des Datenschutzes

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, weil Datenverarbeitung, -erfassung, -haltung, -weitergabe und -analyse immer einfacher werden. Technische Entwicklungen wie z.B. Internet, E-Mail, Mobiltelefonie, Videoüberwachung und elektronische Zahlungsmethoden bieten neue Möglichkeiten zur Datenerfassung.

Sowohl staatliche Stellen als auch private Unternehmen haben Interesse an personenbezogenen Informationen. So z.B. Sicherheitsbehörden, die durch Rasterfahndung und Telekommunikationsüberwachung die Verbrechensbekämpfung verbessern wollen. Unternehmen versprechen sich von Mitarbeiterüberwachung höhere Effizienz und die Zahlungsfähigkeit von Kunden kann über die Schufa ermittelt werden.

Durch die weltweite Vernetzung über das Internet, nehmen die Gefahren hinsichtlich des Schutzes personenbezogener Daten laufend zu. Die Verlagerung (z.B. Outsourcing, Offshoring) von IT-Aufgaben in Regionen, in denen deutsche und europäische Gesetzte nicht durchsetzbar sind, macht guten Datenschutz praktisch oft unmöglich.

2.2 Geschichte des Datenschutzes

1890 entwickelten Samuel D. Waren und Louis D. Brandeis das sogenannte „Right to Privacy“ wonach jedem Individuum das Recht zusteht, selbst zu bestimmen inwieweit seine Gedanken Meinungen und Gefühle, mithin personenbezogene Informationen Anderen mitgeteilt werden dürfen.

Ausgangspunkt der weltweiten Debatte um den Datenschutz waren 1960 die Pläne der US-Regierung unter John F. Kennedy, ein nationales Datenzentrum zur Verbesserung des staatlichen Informationswesens einzurichten. Über diese Debatte wurde auch in Europa berichtet und dann wurde Ende der 1960er Jahre in Deutschland in der Wissenschaft das Wort „Datenschutz“ geschaffen.

Daraufhin verabschiedete Hessen 1970 als erstes Bundesland der BRD ein Datenschutzgesetz, im Jahr 1977 folgte das Bundesdatenschutzgesetz. Schwerpunkte waren die Bestimmung von Datenschutzbeauftragten und die Vorrangstellung des Schutzes personenbezogener Daten.

Ein Meilenstein in der Geschichte des Datenschutzes war 1983 die Prägung des Begriffs des „Informationellen Selbstbestimmungsrechts“ - das Recht des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Anlass war eine geplante Volkszählung.

2.3 Datenschutz in Europa

Mit der Datenschutzrichtlinie 95/46/EG (1995) haben das Europäische Parlament und der Europäische Rat Mindeststandards für den Datenschutz der Mitgliedsstaaten festgelegt. Die Richtlinie ist zum Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten. Sie gilt nicht für die Bereiche Außen- und Sicherheitspolitik (GASP) und die der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS).

Geregelt wird auch die Übermittlung von personenbezogenen Daten an Drittstaaten die nicht in der EU sind. Die Übermittlung ist nur dann zulässig, wenn der Drittstaat ein „angemessenes Schutzniveau“ gewährleistet. Die Europäische Kommission und die sogenannte Artikel-29-Datenschutzgruppe entscheiden, welche Länder dieses Schutzniveau gewährleisten, momentan sind dies z.B. Schweiz, Kanada, Argentinien und speziell bei der Übermittlung von Fluggastdatensätzen der US-Zoll und die Grenzschutzbehörde(CBP).

Die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG ist eine 2002 erlassene Richtlinie der europäischen Gemeinschaft, die verbindliche Mindestvorgaben für den Datenschutz in der Telekommunikation setzt. Sie ergänzt die Datenschutzrichtlinie 95/46/EG. Die Richtlinie soll beispielsweise das Mithören von Telefongesprächen und das Abfangen von E-Mails verbieten, außerdem enthält die Richtlinie Vorgaben zu Einzelgebührennachweisen, zu den Möglichkeiten der Anzeige und Unterdrückung von Telefonnummern, zu automatischen Anrufweiterschaltungen und bezüglich gebührenfreier und widerruflicher Aufnahme in Teilnehmerverzeichnisse. Die Richtlinie muss von den einzelnen Mitgliedsstaaten in nationales Recht umgesetzt werden, Deutschland z.B. gelang die fristgerechte Umsetzung nicht und daraufhin leitete die Europäische Kommission eine Vertragsverletzungsverfahren gegen Deutschland ein. Mitte 2004 schaffte es Deutschland, mit dem Telekommunikationsgesetz die Richtlinie umzusetzen.

2.4 Datenschutz in den USA

Der Datenschutz ist in den Vereinigten Staaten kaum rechtlich durch Gesetze oder andere Vorschriften geregelt. Der Zugriff auf private Daten ist in vielen Fällen gesellschaftlich akzeptiert z.B. eine Bonitätsprüfung vor der Anmietung einer Wohnung oder vor der Vereinbarung eines Arbeitsverhältnisses. Die persönlichen Daten von Kindern unter 13 Jahren werden durch den „Childrens Online Privacy Protaction Act“ seit 2002 geschützt und auch im Bereich der Krankenversicherung werden Daten geschützt.

„Safe Harbor“ ist eine besondere Datenschutz-Vereinbarung zwischen der EU und den USA, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln. Grundsätzlich ist es durch die EU Richtlinie verboten, da die USA keine umfassenden gesetzlichen Regelungen kennen, die den Standards entsprechen. Damit der Datenverkehr zwischen den USA und der EU nicht zum erliegen kommt, wurde zwischen 1998 und 2000 „Safe Harbor“ entwickelt. US-Unternehmen können dem „Safe Harbor“ beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die „Safe Harbor Principles“ zu beachten. Bislang sind mehr als 1000 Unternehmen dem „Safe-Harbor-Abkommen“ beigetreten, darunter Microsoft, General Motors, Amazon, Google, Hewlett-Packard und Facebook.

In den USA gibt es keine umfassende unabhängige Datenschutzaufsicht, lediglich die im Bereich Handel tätige Federal Trade Comission (FTC), die sich gelegentlich auch mit Datenschutzproblemen befasst. Die FTC schreitet jedoch nur ein, wenn ein Unternehmen seine selbst gesetzten Datenschutzrichtlinien nicht einhält. Besitzt ein Unternehmen keine Datenschutzrichtlinien kann die FTC auch nicht eingreifen.

In den Vereinigten Staaten gibt es auch keinerlei rechtliche Vorgaben über die Aufbewahrungsdauer gesammelter personenbezogener Daten. Es gibt des Weiteren kein Recht auf Auskunft gegenüber Behörden oder Unternehmen, welche Daten zur eigenen Person gespeichert sind. Ausnahme ist der „Freedom of Information Act“, der jedem US-Bürger das Recht gibt, Zugang zu Dokumenten der Exekutive (Der Regierung) zu erlangen.

3 Vereine, Gruppen und Institutionen

3.1 Hamburger Datenschutzgesellschaft [5][6]

Die *HDG* ist ein e.V. mit dem Ziel, den Ideenaustausch zum Thema Datenschutz zu ermöglichen und zu beschleunigen und die Bürger zu sensibilisieren, für ihr Recht auf Intimsphäre einzutreten.

Vor diesem Hintergrund bildet die *HDG* ein Forum, das die Möglichkeit bieten soll, Themen und Diskussionen aus verschiedenen Blickwinkeln zu betrachten, um so auch diejenigen zu erreichen, die nicht zum Kreis der ca. 100 Mitglieder gehören.

Des Weiteren finden in unregelmäßigen Abständen Veranstaltungen zu aktuellen Themen statt, zuletzt am 25. Juni 2009 zum Thema: „Nutzung der E-Mail-Funktion und des Internets durch Arbeitnehmer: Risiken und zweckmäßige Gestaltungsvarianten“

3.2 Deutsche Vereinigung für Datenschutz [7]

Ähnlich wie bei der *HDG* ist das Hauptziel der *DVD* die Aufklärung der Bürger. Auch sie tritt als e.V. auf und zusätzlich zu Öffentlichkeits- und Medienarbeit gibt sie seit 1978 die Zeitschrift Datenschutz Nachrichten (DANA) heraus.

In dieser Zeitschrift und auch auf der Homepage der *DVD* wird eine immer wieder ergänzte „Schwarze Liste“ publiziert, auf der andere Homepages aufgeführt sind, deren Nutzung der *DVD* nach bedenklich ist, da sie aus Sicht der *DVD* mangelhaften Datenschutz gewährleisten.

3.3 Humanistische Union [8]

Die *HU* ist die älteste Bürgerrechtsorganisation Deutschlands und als solche befasst auch sie sich mit dem Datenschutz. Gegründet 1961 in München zählt sie heutzutage etwa 1200 Mitglieder und tritt in vielen Bereichen gleichzeitig auf.

Wie auch die *DVD* ist die *HU* an der Verleihung der „Big Brother Awards“ beteiligt, Negativpreisen, die jährlich in mehreren Ländern an Behörden, Unternehmen, Organisationen und Personen vergeben werden, die in besonderer Weise und nachhaltig die Privatsphäre von Personen beeinträchtigen oder Dritten persönliche Daten zugänglich gemacht haben oder machen.

3.4 Konferenz der Datenschutzbeauftragten des Bundes und der Länder [9][10]

Die Konferenz ist ein Zusammenschluss aus den 16 Datenschutzbeauftragten der einzelnen Länder und zusätzlich dem der Bundesrepublik.

Seit 1978 finden Treffen in unterschiedlichen Städten statt, bei denen Stellungnahmen und Entschließungen diskutiert und später bekannt gegeben werden. Am 17. März 2010 fand die 79. Konferenz statt, unter anderem zu den Themen „Vorratsdatenspeicherung“, „Körperscanner“ und „gesetzlichen Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung“.

Auf der Homepage der Konferenz, kann man zu jedem Thema die Beschlüsse und Stellungnahmen nachlesen. Auch wenn ihre Entscheidungen nicht rechtlich bindend sind, sondern nur einen Kommentar darstellen können, so gelten die Mitteilungen der Konferenz dennoch als recht hoch angesehen, aufgrund der hohen fachlichen Kompetenz ihrer Teilnehmer.

3.5 Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI) [11][12]

Der Bundesbeauftragte für Datenschutz (und seit 1. Januar 2006 auch der für Informationsfreiheit) bildet eine unabhängige Kontrollinstanz der deutschen öffentlichen Stellen und der Bundesbehörden, sowie der Telekommunikations- und Postdienst-Unternehmen.

Zusätzlich gehört es zu seinen Aufgaben, selbige zu beraten und regelmäßige Sicherheitsüberprüfungen durchzuführen. Die Kontrolle des Datenschutzes in der allgemeinen Privatwirtschaft gehört nicht zu seinem Tätigkeitsbereich, sondern wird von den einzelnen Datenschutzbeauftragten der jeweiligen Bundesländer durchgeführt.

Es besteht keine Fachaufsicht, was bedeutet, er kann die Art und Weise seiner Aufgabenerfüllung frei wählen. Allerdings verfasst er alle 2 Jahre einen Tätigkeitsbericht, in welchem er Stellung nimmt zu den wesentlichen Entwicklungen zum Thema Datenschutz.

Gewählt wird der *BfDI* auf Vorschlag der Bundesregierung vom Bundestag und seine Amtszeit umfasst 5 Jahre, wobei eine Wiederwahl möglich ist. Zusätzlich zu diesen Aufgaben, ist der *BfDI* Mitglied in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und in der Artikel-29-Datenschutzgruppe.

Seit Dezember 2003 wird das Amt von Peter Schaar bekleidet, welcher von 1994-99 bereits Stellvertretender BfD war. Er wurde im November 2008 wiedergewählt, weshalb sich seine Amtszeit noch bis 2013 verlängert hat.

3.6 Europäischer Datenschutzbeauftragter [13][14]

Der EDPS (European Data Protection Supervisor) ist in seiner Funktion und Tätigkeit dem BfDI recht ähnlich. Er ist eine unabhängige und weisungsfreie Kontrollinstanz der EU-Organe und EU-Institutionen. Zu diesem Zweck hält er Informations- und Zugangsrechte zu diesen inne.

Entgegen zu denen des BfDI, gelten die Anordnungen des EDPS als verbindlich und er hat Eingriffsrechte gegenüber den Gemeinschaftsorganen und Gemeinschaftseinrichtungen. Das bedeutet, er kann Verantwortliche ermahnen

oder verwarnen, des Weiteren sogar unzulässige Datenverarbeitung verbieten oder aber auch rechtswidrig gespeicherte Daten löschen lassen. Dies gilt jedoch nur bei den Europäischen Organisationen, den nationalen Datenschutzbehörden ist der EDPS nicht überstellt oder ihnen gegenüber weisungsberechtigt.

3.7 Artikel-29-Datenschutzgruppe [15][16]

Die Artikel-29-Datenschutzgruppe oder um sie bei ihrer amtlichen Bezeichnung zu nennen, die 'Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten', befasst sich mit dem Datenschutz in Europa. Hierbei stellt sie ein unabhängiges Beratungsgremium der Europäischen Gemeinschaft dar, bestehend aus je einem Vertreter der jeweiligen nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und einem - nicht stimmberechtigten - Vertreter der Europäischen Kommission.

Die Gruppe trifft sich in der Regel fünf Mal pro Jahr in Brüssel zu zweitägigen Sitzungen und wird in ihrer Arbeit durch Untergruppen unterstützt. Bis Ende 2006 wurden fast 130 Entschließungen verabschiedet. Diese sind aber wie bei den meisten anderen Institutionen im Bereich Datenschutz nicht bindend, somit hat selbst die Artikel-29-Datenschutzgruppe vornehmlich beratende Funktion.

Zuletzt wurden Stellungnamen bekannt zu Themen wie Videoüberwachung, Arbeitnehmerdatenschutz, Datenschutz im Internet oder dem Einsatz biometrischer Verfahren, 2003 stimmte die Gruppe gegen die Übermittlung von Passagierdaten an die USA - die Kommission der EU beschloss diese trotzdem. 2005 stimmte die Gruppe gegen die Vorratsdatenspeicherung, noch im selben Jahr wurde sie vom EU Parlament beschlossen.

3.8 Zusammenfassung

Man sieht also, dass es jede Menge Gruppen, Vereine und Institutionen gibt, die sich mit dem brisanten Thema *Datenschutz* befassen.

Selbst wenn es sich bei allen aufgeführten größtenteils um beratende Einrichtungen handelt, so sollte man doch meinen, der Datenschutz würde in der Regel funktionieren, oder zumindest das Bewusstsein der Verantwortlichen sei sensibilisiert genug um mit personenbezogenen Daten verantwortungsvoll umzugehen.

Die folgende Zusammenstellung einiger ausgewählter Vorfälle soll deutlich machen, dass dem absolut nicht so ist und zeigen, dass die bereits vorhandenen Massen an gesammelten Daten, für niemanden mehr kontrollierbar sind.

4 Fallbeispiele von Datenschutz(-pannen)

4.1 TNS Infratest [17][18]

TNS Infratest ist eine Tochtergesellschaft vom zweitgrößten Marktforschungsunternehmen der Welt, *Taylor Nelson Sofres*. Mit 14.000 Mitarbeitern in über 70 Ländern ist *TNS Infratest* fest etabliert und unter anderem in Deutschland bekannt durch die Wahlberichtserstattung für die ARD durch die Umfrage „Wenn am kommenden Sonntag Bundestagswahl “.

Im Juli 2008 wurden dem Chaos Computer Club anonym Login-Daten zugespielt inklusive dazugehöriger URL auf der die Beteiligten persönliche Daten wie Name, Adresse, Geburt, aber auch Anzahl und Art der Wertgegenstände im Haus einsehen konnten. In der URL auf die man nach dem Login geleitet wurde, war am Ende die Kundennummer der betroffenen Person zu sehen - unverschlüsselt. Daher probierten die CCCler nun andere fortlaufende Kundennummern und gerieten mit jeder neuen Nummer auf eine neue Kundendatei. Innerhalb dieser konnten sie nicht nur einsehen, was die Person für Daten angegeben hatte, sondern konnten diese auch noch verändern. Auf diese Art wurden über 40.000 verschiedene Kundennummern getestet und zu jeder gab es über 50 personenbezogene Daten, fein geordnet, veränderbar und für mindestens alle der 40.000 „frei“ zugänglich.

Laut *TNS* handelte es sich bei den aufgerufenen Kundennummern um sog. „Mystery Shopper“, Leute die anonym bei Geschäften einkaufen und sie so auf Kundenfreundlichkeit und Kompetenz testen. Allerdings räumte *TNS* weiter ein, dass es lediglich 100 dieser *Mystery Shopper* gäbe, Wikipedia dagegen berichteten später von immerhin 4000.

Erst im späteren Verlauf stellte sich heraus, dass Leute die bei einem Umfragebogen die Frage „Könnten sich sich einen Job als Mystery Shopper vorstellen?“ mit JA beantworteten, ebenfalls alle in die entsprechende Datenbank mit aufgenommen wurden.

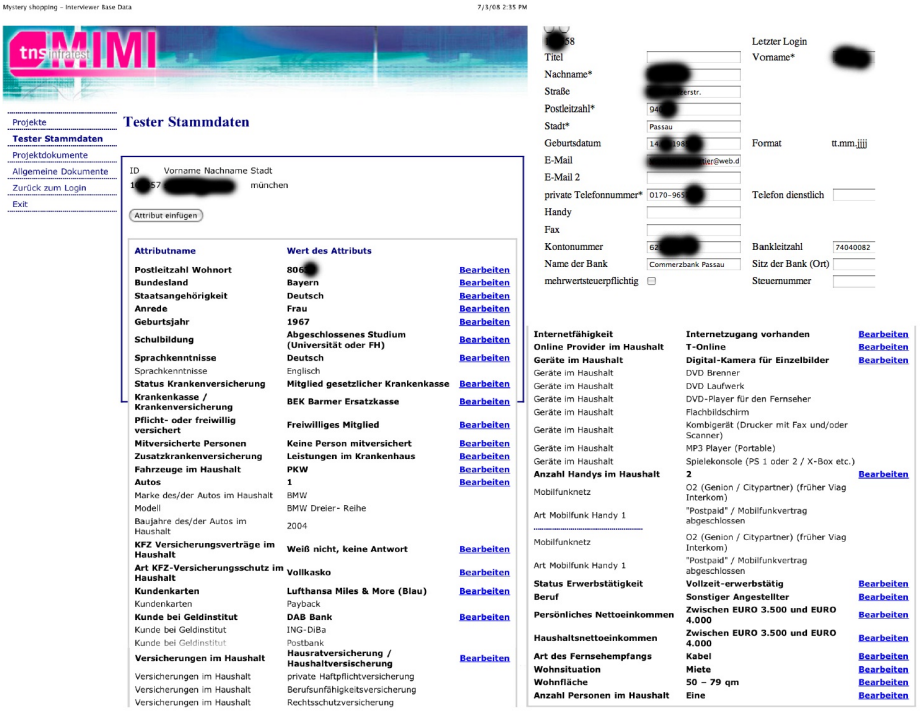


Abbildung 1: Ein Screenshot vom CCC, von den einseh- und veränderbaren Kundendaten

4.2 Libri [19][20]

Ein weiterer, ähnlicher Fall wie der bei *TNS* ereignete sich am 28. Oktober 2009 bei *libri*, einem der größten deutschen online Marktplätze für Bücher und verwandte Produkte. *libri* arbeitet u.a. als Dienstleister für rund 1000 lokale Buchhändler aber auch für Online-Shops wie z.B. *shop.spiegel.de*.

Bei *libri* standen für unbekannt lange Zeiträume über 500.000 Buchbestellungen und dazugehörige Kundendaten aus den vergangenen 16 Monaten als PDF-Rechnung im Internet. Somit waren Adressen, bestellte Bücher und dazugehöriger Preis der Kunden frei einsehbar für alle, die die Sicherheitslücke einmal entdeckt hatten, denn anders als bei *TNS* brauchte man bei *libri* sich nicht einmal in einen abgesonderten Bereich einloggen.

Die so einsehbaren Daten waren, wie man sich vorstellen kann, in hohem Maße persönlichkeitsrelevant, denn aus einer Bestellung von einem Buch mit aussagekräftigen Titeln wie z.B. „Leben mit Depressionen“ lassen sich leicht Rückschlüsse über den Käufer ziehen.

Die Kunden erhielten ihre Rechnung per E-Mail zugeschickt, in der ein Link zu der Ihnen zugehörigen PDF Datei mitgeteilt wurde. In diesem Link war wie bei *TNS* auch die Kundennummer unverschlüsselt enthalten.

Erschwerend hinzu kam, dass zusätzlich auch der Zugang zu Online-Shops, die von *libri* verwaltet wurden, mit einem einfachen Trick ermöglicht wurde. Dies galt sogar für bereits für von den Erstellern gelöschte Angebotssteiten. *libri* wies den Erstellern von Online-Shops fortlaufende Nummern als Initial-Benutzernamen zu, ebenso dazugehörige Initial-Passwörter, bestehend aus der selben Nummer. In diesen Online-Shops konnten zusätzlich zu den oben erwähnten Daten nun auch Kundenlisten abgefragt werden, in denen ergänzend Emailadressen vorhanden waren, oder aber auch der gesamte Shop selber umgestaltet und auch das Passwort geändert werden.

Erschreckend an diesem Fall sind zwei Dinge:

Zum einen die Tatsache, dass die Online-Buchhändler es anscheinend nicht für nötig hielten, ihre automatisch gesetzten Login-Daten, die ja offensichtlich nicht sicher waren, zu ändern.

Zum anderen aber fast noch schlimmer, dass *libri* am 7. Mai 2009 vom TÜV Süd das sog. „Safer-Shopping-Zertifikat“ verliehen bekommen hatte. Der TÜV versuchte dies zu entschuldigen mit der Begründung, *libri* sei bereits 2008 getestet worden und danach erst sei die fehlerhafte Software eingesetzt worden. Warum dann allerdings vor der tatsächlichen Verleihung des Zertifikats keine erneute Überprüfung stattfand konnte man nicht erklären.

4.3 Her Majesty's Revenue and Customs [21][22][23]

Dem britischen „Finanzamt“ *HMRC* gelang es die Dimension der bei *TNS* oder *libri* Betroffenen um ein Vielfaches zu übertreffen.

HMRC ist die zentrale Behörde für sämtliche Steuerangelegenheiten, somit auch Umsatzsteuer bei Unternehmen oder Einkommenssteuerangelegenheiten von Privatpersonen.

Am 18. Oktober 2007 „verlor“ *HMRC* 2 CDs mit Daten von über 25 Millionen Briten. Hierbei handelte es sich um Namen, Adressen, Geburtsgaten, nationale Versicherungsnummern und teilweise Informationen zur Bankverbindung von

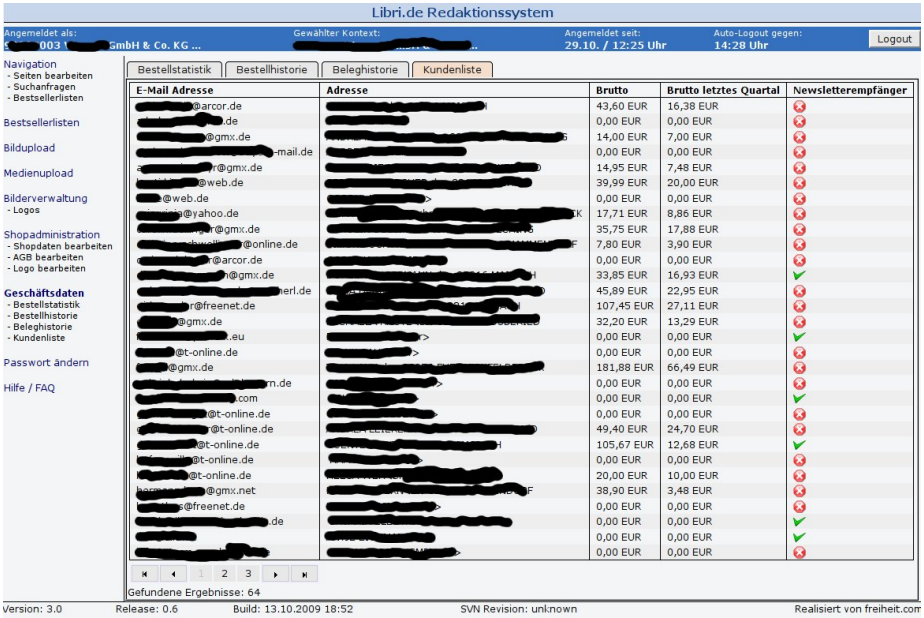


Abbildung 2: Eine Kundenliste aus einem Online-Shop bei libri

insgesamt 7,25 Millionen Familien, nämlich diejenigen, die Sozialhilfe wegen ihrer unter 16 Jahre alten Kinder beantragt hatten.

Die CDs wurden mit der normalen Post verschickt, ohne Beachtung der eigentlich vorgesehenen Sicherheitsmaßnahmen und sind bis heute verschwunden.

4.4 Studie: „Verlorene Daten“ [24][25]

Eine Studie des Ponemon Institute 2009 zeigt, dass „verlorene“ Daten keine Einzelfälle sind. In der Studie wurden 950 ehemalige Mitarbeiter von Firmen befragt, die in den vergangenen zwölf Monaten kündigten oder entlassen wurden. 82% von ihnen gaben an, beim Verlassen des Unternehmens nicht kontrolliert worden zu sein. 60% nahmen bewusst unerlaubt vertrauliche Daten mit, wie z.B. Adresslisten von Kunden oder andere Informationen, die bei einer neuen Arbeitsstelle nützlich sein könnten und immerhin 24% hatten auch nach der Beendigung des Arbeitsverhältnisses noch Zugriff auf das Unternehmensnetzwerk, teilweise über einen Monat lang.

4.5 Datenmissbrauchsfälle [26]

Das Verschwinden von Daten ist nicht das einzige Problem, das entsteht wenn man solche riesigen Mengen an Informationen sammelt und verarbeitet. Diese Beispielfälle sollen zeigen, zu welchem Missbrauch und Fehlern die bereits existierenden Datenbanken und Auswertungen führen können.

Ein 67 jähriger Unternehmer wird fast verhaftet [27]

Am 15. Dezember 2006 wird ein 67 jähriger Unternehmer in seiner Wohnung von der Polizei aufgesucht, wegen dem Verdacht Kinderpornografie über das Internet bestellt zu haben. Der Verdacht entstand, weil von seinem MasterCard Konto entsprechende Beträge abgebucht wurden.

Der 67 jährige nutzte allerdings laut eigener Aussage nicht einmal das Internet. Erst auf seine wiederholte Nachfrage offenbarte die Polizei ihm den Verdachtsgrund, also die Abbuchungen von seinem Konto. Dadurch erinnerte er sich an Vorfälle die eineinhalb Jahre zurücklagen, nämlich unbekannte Abbuchungen von Dollarbeträgen von seinem Konto und rief bei seiner Kundenbetreuung an. Auf seine dringende Bitte hin sendete eine Angestellte ihm interne Informationspapiere und Kopien seiner zahlreichen Beschwerden.

Die Polizei brach daraufhin die Durchsuchung ab, bedenklich allerdings bleibt, dass hätte der Unternehmer sich nicht an die entsprechenden Vorfälle erinnert, die Polizei seinen Computer mit allen Kundendaten beschlagnahmt hätte. Das wäre in der Vorweihnachtszeit, wo über 300 Bestellungen täglich verschickt wurden, so der Unternehmer, sein Ruin gewesen.

Eine Googleabfrage führt zur Hausdurchsuchung [28]

Im Mai 2007 drangen BKA-Ermittler in die Wohnung eines mutmaßlich militanten G8-Gegners ein, mit der Begründung, er sei an einem zuvor verübten Brandanschlag auf das Berliner Unternehmen Dussmann beteiligt gewesen. Das einzige Indiz für diese Annahme jedoch war, dass er im Internet nach „Dussmann“ recherchiert haben soll, was allerdings auch eines der größten Bücherkaufhäuser der Stadt ist.

Eine Bankkundin bekommt eine Rechnung über Reinigungskosten [29]

Im Februar 2008 wurde einer Frau eine Rechnung über entstandene Reinigungskosten zugestellt, die ihre Tochter verursacht haben sollte. Die Frau war einige Tage zuvor mit ihrer Tochter in das Foyer der Filiale gegangen um Geld abzuheben, wobei die Tochter allem Anschein nach Hundekot am Schuh hatte und so die Filiale verschmutzte.

Daraufhin wurden von der Bank die Videoaufzeichnungen ausgewertet und verglichen mit den Kundendaten zu dem entsprechenden Zeitpunkt und die Betroffene Frau angeschrieben. Dieses Vorgehen jedoch ist nur bei Strafverfolgung erlaubt, weswegen die Bank auch auf ihrer Gegendarstellung bestand, es habe sich um eine mutwillige Sachbeschädigung gehandelt, weil sich das Kind in der Ecke erleichtert habe und es sich somit nicht um Hundekot gehandelt habe.

Ein Provider liefert falsche Daten ans BKA [30]

Ein Internetanbieter wurde am 29. August 2007 per Fax vom BKA aufgefordert, die Kundendaten einer bestimmten IP-Adresse zu übermitteln, die zu dem Zeitpunkt im Internet in einer Tauschbörse aktiv war und eine beachtliche Menge Kinderpornografie zum Download anbot. Der Mitarbeiter schickte das Fax zurück, auf welchem er schnell handschriftlich die verlangten Daten notiert hatte.

Für den benannten Kunden hatte die Auskunft weitreichende Folgen: Hausdurchsuchung, Beschlagnahme des Heim-PCs und des Firmennotebooks und

Vernehmungen, von dem Ansehensverlust im Familien- und Bekanntenkreis ganz zu schweigen. Der Betroffene war jedoch nicht der tatsächliche Nutzer der IP-Adresse. Der Datenschutzbeauftragte des Providers formulierte später: „Die Prozesse bei der Überprüfung von IP-Adressen liefen nicht optimal. Die operative Einheit hat sich vertan."

Dieser Vorfall führte dazu, dass die zuständigen Mitarbeiter ab sofort durch Controller verstärkt wurden, die alle Arbeitsschritte in der Abteilung überprüfen und außerdem jede Abfrage durch Screenshots dokumentiert wurde, was bis zu dem Zeitpunkt nicht der Fall gewesen ist.

5 ELENA [31]

Der *El*ektronische *E*ntgeld*na*chweis betrifft seit Anfang 2010 alle Arbeitnehmer. ELENA soll dazu dienen, die bisher vom Arbeitgeber auf Papier erstellten Gehaltsbescheinigungen in Verfahren der Sozialbehörden elektronisch im sogenannten *M*ultifunktionalen *V*erdienst *D*aten*s*atz zur Verfügung zu stellen. „Es handelt sich bei den gespeicherten Daten daher um Einkommensdaten und um weitere Angaben, die für die Prüfung notwendig sind, ob ein Anspruch auf die Sozialleistung besteht oder nicht." Soweit die offizielle Darstellung in Kurzform. Welche Daten genau gespeichert werden, verrät eine 57 Seiten lange PDF Datei. Stark zusammenfassend sind zu nennen: Name, Geburtsangaben, Anschrift, Arbeitgeberdaten, von der Arbeitgeberanschrift abweichender Beschäftigungsort, Fehlzeiten, Steuerpflichtiger sonstiger Bezug, Steuerfreie Bezüge, Ausbildung, Zusatzdaten, Nebenbeschäftigung Arbeitslose, Heimarbeiter, Kündigung/Entlassung, Fehler.

ELENA soll durch diese Digitalisierung eine Ersparnis von 85 Mio. Euro bringen, wie genau allerdings diese Berechnung erfolgt ist und welche neu entstehenden Aufwände wie z.B. Serververwaltung und Energiekosten berücksichtigt wurden ist nirgends einzusehen. Die öffentlich bekannt gemachten Zahlen jedenfalls weisen deutliche Lücken auf.

Ebenso ist die Speicherung der Daten an sich fraglich, denn die Behauptung, dass Angaben über z.B. Kündigung, Abmahnungen, Streikteilnahmen und eventuelle Entlassungsgründe bei der Beurteilung von Sozialleistungen sinnvoll sind, scheint nicht nur dem *BfDI* Peter Schaar etwas aus der Luft gegriffen zu sein.

Datenschützer sehen in dem „ursprünglich sinnvollen Projekt" nun nur noch eine aberwitzige Datensammelwut, also die Umkehrung ins absolute Gegenteil. Ihrer Ansicht nach, fehlt das angemessene Verhältnis der gesammelten Daten zum tatsächlichen Nutzen und sie befürchten, dass ein Großteil wohl nie gebraucht wird.

Ein letzter Punkt allerdings bleibt positiv zu erwähnen, denn bei der Sicherheit der gesammelten Daten scheinen dieses Mal deutliche Fortschritte gemacht worden zu sein, zum einen weil mit dem *BfDI* eng zusammengearbeitet wird und er mit zusätzlichen Kontrollbefugnissen ausgestattet wurde, zum anderen auch weil es Studenten der FH Bonn in einem mehrwöchigen Test trotz Insiderwissen weder durch Angriffe von außen noch von innen gelang, auf Personenbezogene Daten zuzugreifen. Dies liegt an der Art der seperaten Speicherung von Synonymen einerseits und dazugehöriger Datensätze andererseits und daran, dass die Daten nur mit den Antragsstellern in Verbindung gebracht werden können, wenn der entsprechende Betroffene dem Sachbearbeiter die Befugnis erteilt. (s.

Abb. 3)

Das erste Mal soll ELENA allerdings erst im Januar 2012 zur Beurteilung dienen, bis dahin werden vorerst nur Daten gespeichert.

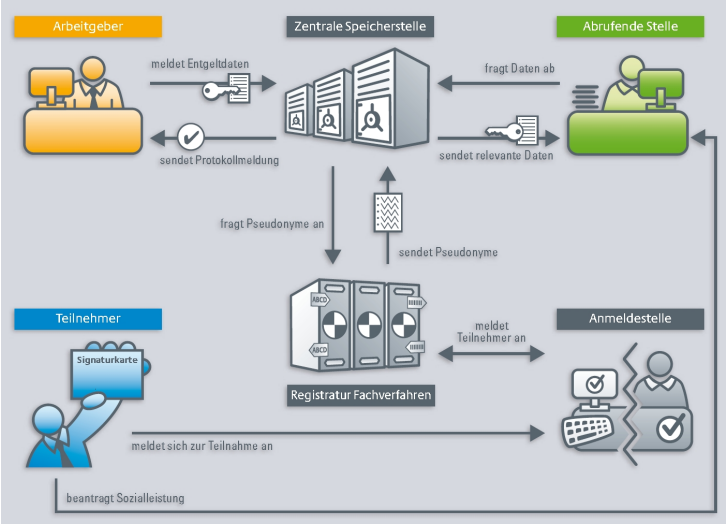


Abbildung 3: Das Elena Verfahren bei einer Datenabfrage

Literatur

[1] http://de.wikipedia.org/wiki/Daten.

[2] http://de.wikipedia.org/wiki/Personenbezogene_Daten.

[3] http://de.wikipedia.org/wiki/Datenschutz.

[4] http://de.wikipedia.org/wiki/Bundesdatenschutzgesetz.

[5] http://de.wikipedia.org/wiki/Hamburger_Datenschutzgesellschaft.

[6] http://www.hamdg.de/.

[7] http://de.wikipedia.org/wiki/Deutsche_Vereinigung_f%C3%BCr_Datenschutz.

[8] http://de.wikipedia.org/wiki/Humanistische_Union.

[9] http://www.sachsen-anhalt.de/LPSA/index.php?id=18664.

[10] http://de.wikipedia.org/wiki/Konferenz_der_Datenschutzbeauftragten_des_Bundes_und_der_L%C3%A4nder.

[11] http://www.bfdi.bund.de/cln_134/DE/Dienststelle/dienststelle_node.html.

[12] http://de.wikipedia.org/wiki/Bundesbeauftragter_f%C3%BCr_den_Datenschutz_und_die_Informationsfreiheit.

[13] http://de.wikipedia.org/wiki/Datenschutzbeauftragter_der_Europ%C3%A4ischen_Kommission.

[14] http://www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=de.

[15] http://www.bfdi.bund.de/cln_134/DE/EuropaUndInternationales/Art29Gruppe/Art29Gruppe_node.html.

[16] http://de.wikipedia.org/wiki/Artikel-29-Datenschutzgruppe.

[17] http://ds.ccc.de/vorab/Sicherheitsleck_Infratest.pdf.

[18] http://www.spiegel.de/netzwelt/web/0,1518,565412,00.html.

[19] http://www.netzpolitik.org/2009/exklusiv-die-libri-shops-der-anderen/#more-9400.

[20] http://www.netzpolitik.org/2009/exklusiv-die-buecher-der-anderen/.

[21] http://www.heise.de/newsticker/meldung/Millionen-Briten-von-Datenpanne-betroffen-197858.html.

[22] http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm.

[23] http://news.bbc.co.uk/2/hi/business/7103940.stm.

[24] http://www.zdnet.de/news/wirtschaft_sicherheit_security_studie_warnt_vor_datendiebstaehlen_durch_ex_mitarbeiter_story-39001024-41000865-1.htm.

[25] http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Data%20Loss%20Risks%20During%20Downsizing%20FINAL%201.pdf.

[26] http://www.daten-speicherung.de/wiki/index.php/F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern.

[27] http://www.faz.net/s/RubCD175863466D41BB9A6A93D460B81174/Doc~E213402745D034DD2985EC4BEB52EEB38~ATpl~Ecommon~Scontent.html.

[28] http://www.taz.de/index.php?id=archivseite&dig=2007/05/15/a0059.

[29] http://www.stuttgarter-nachrichten.de/stn/page/detail.php/1628468.

[30] http://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/.

[31] http://www.bfdi.bund.de/cln_134/DE/Schwerpunkte/JobcardVerfahren/Jobcard_node.html.

Informatik und Utopie

Pavel Lapin

Zusammenfassung

In dieser Arbeit geht es um die modernen Entwicklungsgebiete in der Forschung, auf die von der Gesellschaft große Hoffnung auf besseres Leben gesetzt werden und die die großen Änderungen mit sich bringen können. Diese Änderungen können einen globaler Charakter annehmen und zu einer neuen Ordnung auf der Erde führen, bei der der Mensch nicht mehr die überstehende Spezie ist. Die Vorschläge für die Gegenmaßnahmen bieten meist keine Lösungen oder sind einfach nur absurd. Im Rahmen dieser Arbeit wird versucht, den Umgang mit dem Thema „Fortschritt“ zu sensibilisieren.

1 Einleitung

Das griechische Wort ‘Utopia’ bedeutet übersetzt eine „Nicht-Örtlichkeit“, ein Ort, der nicht existiert. Utopie ist eine Wunschvorstellung von der Welt, die gewünscht, aber nicht existent ist. Utopien beschreiben den Aufbau dieser Welt, ohne auf die Gründe einzugehen, warum das Gewünschte noch nicht realisiert oder gar nicht realisierbar ist.

Die moderne Bedeutung vom Wort ist durch den 1516 erschienenen Roman „De optimo rei publicae statu deque nova insula Utopia“ („Vom besten Zustand des Staates oder von der neuen Insel Utopia“) des englischen Staatsmanns Thomas Morus geprägt. Im Roman wird durch die Beschreibung der Inselordnung eine gesellschaftliche Kritik ausgeübt[10]. Im modernen Wortgebrauch ist dieser Kritikaspekt meistens dabei. Man hat gelernt, dass es keine Utopien ohne Anti-Utopien gibt. Jede Änderung bringt etwas Neues und Unbekanntes mit sich, was weitere Probleme verursachen kann.

Der rasante technologische Fortschritt führt dazu, dass viele Neuerungen positiv aufgenommen werden und die Träume nach mehr entstehen lassen. Was gestern als nicht realisierbar angesehen wurde, ist heute Realität oder hat theoretische Untermauerung für die Verwirklichung erhalten. Man erlebt den Umbruch im Glauben, was alles möglich und unmöglich ist. Die Euphorien diesbezüglich werden aber auch durch kritische Stimmen begleitet. Am anderen Ende entstehen immer wieder Schreckszenarien, die die Menschheit zum Verzicht auf alle technische Errungenschaften und zum Rückkehr in die vor-technologische Zeit bewegen sollen.

2 Fortschritt

Der Mensch entwickelt im Laufe seiner Existenz immer neue Technologien und die Entwicklungsgeschwindigkeit nimmt mit der Zeit immer wieder zu. Das 20.

Jahrhundert war ein Jahrhundert des rasanten Fortschritts. Es sind zahlreiche Erfindungen gemacht worden, die den Alltag und die Tätigkeiten enorm erleichtern, was tiefgehende Änderungen in der Gesellschaft mit sich gebracht hat. Heutzutage erreichen die Technologien den Stand, der nicht nur auf eine Erleichterung und einen Ersatz des Menschen in einfacheren Arbeitsbereichen abzielen.

In den letzten Jahrzehnten ist eine Schwerpunktverlageng der Wissenschaft deutlich sichtbar geworden. Die klassifizierende und erkenntnisorientierte Tätigkeit ist durch Eingriff und Modellierung in den Hintergrund gedrängt worden. Es reicht nicht mehr, Prozesse zu betrachten und sie zu beschreiben. Man will diese Prozesse aktiv steuern, um ein gewünschtes Ergebnis zu bekommen, die Prozesse aus dem ursprünglichen Kontext rauszunehmen und vom Anfang an nachzubilden. Das dabei gewonnene Wissen soll bei der Modellierung neuer Prozesse, die noch nicht existieren aber gewünscht sind, eingesetzt werden[1].

Die Entwicklungstendenzen werden zwiespältig angesehen. Einerseits ruft jede neue Entdeckung beinahe euphorische Stimmungen in der Wissenschaftswelt und eine Mehrzahl von Meldungen, wofür sie eingesetzt und was alles dadurch ermöglicht werden kann. Andererseits hört man aber auch mahnende Stimmen, was den leichtsinnigen Umgang und fehlendes Wissen über die möglichen Folgen angeht.

Unter der Tatsache, dass die Entwicklungszyklen immer kürzer werden, bleibt der Gesellschaft wenig und oft sogar keine Zeit über die Neuerung nachzudenken. Zum Teil kann man auch darüber sprechen, dass die Gesellschaft nicht mehr genug kritischer Aufmerksamkeit dem Fortschritt schenkt. Man ist daran gewöhnt, dass jeden Tag etwas Neues entwickelt wird und hat Resistenz dagegen entwickelt[1]. Andererseits werden auch hohe Erwartungen an die Wissenschaft gestellt. Die Gesellschaft wirkt manchmal ungeduldig und gierig nach neuen Erfindungen. Oft kann man Stimmen hören, dass Pharmakonzerne immer noch keine Arzneien für einige Krankheiten entwickelt haben und die Testphasen für neuen Medikamente verkürzt werden sollen, die Roboter sind im Alltag immer noch eher ein Spielzeug und die Rechner können immer noch nicht bestimmte Aufgaben übernehmen, abgesehen von den veralteten Schnittstellen zwischen dem Menschen und einer Maschine.

Nichts desto trotz werden mehrere Lebensbereiche soweit durch die Maschinen verwaltet, so dass es merkbar nur in Fällen wird, wenn ein Ausfall stattfindet und ein Ersatz nicht bzw. nicht mehr vorhanden ist. Die Abhängigkeit ist bereits sehr groß und wird mit der Zeit nur immer größer.

In kleinen Schritten ist die Entwicklungsstufe vorstellbar, wo die Maschinen entwickelt werden, die alles besser als Mensch machen können. Es stellt sich die Frage, welche Rolle bleibt dem Menschen übelassen. Bleibt der Mensch ein Entscheidungsträger und die Maschinen werden nur zur Hilfe da sein oder entwickelt sich eine Abhängigkeit von besserer Leistung, so dass auch die Entscheidungsrolle nach und nach an die Maschinen abgegeben wird[1].

Dass diese Stufe erreicht wird, ist für viele Wissenschaftler ohne Zweifel. Die Frage ist nur wann. Die Fortschrittskurve nimmt mit der Zeit exponentiell zu. Man spricht bereits davon, dass eine technologische Singularität - ein Zeitpunkt ab dem, die Kurve beinahe vertikal verläuft, möglich ist. Die Situation davor wird mit dem Begriff "Bootstrap"beschildert. Man versteht darunter einen Zustand, in dem die Technologien soweit fortgeschritten sind, dass der Durchbruch ansteht, aber entscheidende Komponente noch fehlt. Wenn sie da ist, überholen

sich die neuen Technologien mit einer sehr hohen Geschwindigkeit.

Die größten Hoffnungen setzt man heute auf die Genetik, Nanotechnologien, künstliche Intelligenz und Robotik. Es sind bereits große Erfolge zu verzeichnen und die Vorraussetzungen für technologische Singularität in der Bereichen am ehesten zu erwarten.

2.1 Nanotechnologie

Unter dem Sammelbegriff „Nanotechnologie“ versteht man interdisziplinäre Grundlagenforschung und die angewandten Wissenschaften, die sich mit sich mit der Sammlung von theoretischen Studien, praktischen Methoden der Untersuchung, Analyse und Synthese, sowie Methoden der Herstellung und Verwendung von Produkten, die eine bestimmten atomaren Struktur besitzen oder durch kontrollierte Manipulation einzelner Atome und Moleküle hergestellt werden, beschäftigen[9].

Vom Technischen Komitee ISO/TC 229 wird folgender Rahmen für die Nanotechnologie gestellt:

- Es handelt sich um Wissen und Prozesse für die Objekte, die in der Regel das Ausmaß von 1 nm bis 100 nm in einer (oder mehreren) Dimension nicht überschreiten und durch das Size-Phänomen neue Eigenschaften zunehmend auftreten, die zu neuen Möglichkeiten und neuen Anwendungen führen.

- Es handelt sich um die Eigenschaften von Objekten und Materialien im Nanometerbereich, die sich von denen der freien Atome oder Moleküle unterscheiden, sowie Volumeneigenschaften der Materie aus diesen Atomen oder Molekülen. Die Oberflächeneingenschaften und quantenphysikalische Effekte prägen solche Materialien und erlauben Vorrichtungen und Systeme zu realisieren, die derartige Eigenschaften bei den anderen Materialien aufs neu schaffen.

Der praktische Aspekt der Nanotechnologie befasst sich mit der Herstellung von Geräten und Komponenten, die für die Erstellung, Bearbeitung und Manipulation von Atomen, Molekülen und Nanoteilchen erforderlich sind. Es wird davon ausgegangen, dass ein Objekt nicht unbedingt mindestens eine lineare Ausdehnung von weniger als 100 Nanometern haben muss. Es können auch Mikroobjekte sein, dessen atomare Struktur mit einer Auflösung auf der Ebene von einzelnen Atomen steuerbar ist oder die mit der Nanostruktur erzeugt sind. Im weiteren Sinne umfasst der Begriff „Nanotechnologie“ auch Methoden der Diagnose, Charakterisierung und Untersuchung solcher Objekte[9].

Nanotechnologien unterscheiden sich qualitativ von den traditionellen Disziplinen, da die üblichen makroskopischen Technologien in solchem Ausmass nicht mehr wirken und die mikroskopischen Phänomene, die zu schwach in einer makroskopischen Größenordnung sind, viel bedeutender werden, wie z.B. die Eigenschaften und Wechselwirkungen der einzelnen Atome und Moleküle, Aggregatzustände von Molekülen, Quanteneffekte.

Erste Erwähnung von Methoden, die später Nanotechnologie genannt werden, findet man in dem Vortrag „There's Plenty of Room at the Bottom“ („Ganz unten ist eine Menge Platz“) von Richard Feynman, den er 1959 auf dem jährlichen Treffen der Physikergesellschaft gehalten hat. Richard Feynman hat es für möglich erklärt, einzelne Atome mechanisch mithilfe eines in der geeigneten

Grösse zu entwickelnden Mechanismus zu bewegen. Die Existenz von solchem Mechanismus und der Bewegungsprozess selbst widersprechen nicht den derzeit bekannten physikalischen Gesetzen. Ausserdem wurde das Konstruktionsprinzip für so einen Mechanismus vorgeschlagen. Man sollte als erstes einen Mechanismus konstruieren, der eine verkleinerte Kopie von sich selbst nachbauen kann. Diese Kopie soll den Vorgang wiederholen können, so dass noch eine kleinere Kopie erstellt wird, die das gleiche wie das Original macht. Bei jedem Schritt sollten Anpassungen an dem Mechanismus vorgenommen werden, die die schwindende Wirkung von den makroobjekttypischen Eigenschaften und die zunehmenden Microobjekteffekte berücksichtigt. Im letzten Schritt soll dieser Mechanismus sich selbst aus einzelnen Atomen nachbauen. Die in jedem Schritt erstellten Mechanismen sind im Stand, eine unbegrenzte Anzahl von Kopien anzufertigen. In Gegenrichtung gesehen, könnten solche Mechanismen auch Makroobjekte aus einzelnen Atomen zusammenbauen. Später werden solche Mechanismen als Nanoroboter oder Superassembler genannt. Sie sollen der Massenproduktion einen neuen Charakter geben und Ressourcen- und Energieverbrauch immens optimieren. Es wäre für die Produktion nur soviel Material verbraucht, wie es in der Endkonstruktion verbaut ist. Produktionsabfälle und Wirkungsgrad wären somit gesteigert[8].

Nanotechnologie und molekulare Technologie bleiben aber auch nach 60 Jahren noch ein relativ neues und wenig studiertes Thema. Die großen Entdeckungen, die in diesem Bereich prognostiziert wurden, sind noch nicht gemacht worden. Der Traum von Nanorobotern bleibt bis heute eine der modernen Utopien. Keiner konnte das Prinzip und die potenzielle Möglichkeit solcher Nanoroboter widerlegen. Es ist aber auch bis heute nicht gelungen, einen solchen Roboter herzustellen.

Dennoch liefern die Studien bereits praktische Ergebnisse. 1990 gelang es den IBM Forschern mit 35 Xenon-Atomen den Firmennamen zu schreiben. Die Physiker der Stanford Universität konnten mit Elektronenwellen die Anfangsbuchstaben der Einrichtung „S“ und „U“ formen[7]. Es existieren bereits erste Nanorotore und Nanomotore. Auf dem Weg zum ersten Nanorobot oder Superassembler steht nur noch ein Problem, das sich mit dem Bootstrap-Begriff beschreiben lässt. Es sollte der erste derartige Mechanismus geschaffen werden, damit die Weiterentwicklung voranschreitet.

2.2 Genetik

Die Genen sind strukturelle und funktionelle Einheiten der Vererbung, welche für die Steuerung der Eigenschaften und der Entwicklung verantwortlich sind. Die Genen sind den Mutationen ausgesetzt, die spontan oder durch den äusseren Einfluss auftreten können. Die genetische Variation, die dadurch entsteht, stellt ein wichtiger Faktor für die Evolution dar[6].

Der Mensch ist heutzutage durch die natürliche Evolution die Spitze der Schöpfung auf der Erde. Durch die Erfolge in der Genetik ist es schon heute möglich das Erbgut anzupassen, um Lebewesen mit den gewünschten Parameter zu züchten. Das menschliches Genom ist im Rahmen des Humangenomprojektes April 2003 entschlüsselt worden. In Folgeprojekten wird die Rolle von einzelnen Genen erforscht[5].

Bei Pflanzen und Haustieren versucht sich der Mensch schon heute als Wegweiser der Evolution. Künftig ist es sehr wahrscheinlich, dass der Mensch auch

eigene Entwicklung mit der Genmanipulation beeinflussen wird. Krankheitsresistenz, Körper- und Krafteigenschaften, Aussehen, Charakter und Intelligenz könnten dann schon bei der Geburtsplanung auf Wunsch oder auch auf Vorschrift berücksichtigt werden.

Die Folgen für die Gesellschaft werden kolossal sein. Betrachtet einerseits alle Lebewesen ausser dem Menschen, so eröffnen sich wirtschaftlich gesehen beinahe unbegrenzte Möglichkeiten, was Landwirtschaft und Produktion angeht. Pflanzen und Nutztiere, die krankheits-, witterungs- und schädlingsresistent sind, mit wenigen Nährstoffen auskommen und im voraus vordefinierte Eigenschaften besitzen, können ein Traum von der Welt ohne Hunger wahr sein lassen.

„Geplante“ Menschen können bessere Leistungen durch die Anpassung des Körpers bei physisch geprägten Arbeiten besser und schneller erledigen. Gesteigerte Intelligenz führt schneller zu weiteren Neuentwicklung und Entdeckungen in der Wissenschaft. Durch die vorgegebenen Gesundheit- und Älterungssparameter steigert die Lebenserwartung und Lebensqualität.

Die grössten Sorgen, die mit den Genmanipulationen heute verbunden sind, bestehen darin, dass man Angst vor möglichen Folgen der Manipulation hat. Es ist bis heute nicht genug erforscht, ob der Verzehr von genetisch manipulierten Lebensmitteln gesundheitliche oder mit Erbgut verbundene Schäden für den Organismus anrichten kann. Soziale Folgen durch fehlerhafte Massenmanipulationen am Menschen können zu einer Katastrophe und Tragödie führen.

Man könnte aber auch annehmen, dass anfangs Schwierigkeiten und auch Fehler auftreten können, die mit der immer wachsender Erfahrung auf dem Gebiet vermindert werden. Es bleibt doch die Frage offen, wie das Versuchsfeld aussehen, wenn es um die Manipulationen am menschlichen Erbgut gehen sollte. Aus vielen Gründen, die vor allen moralischen Charakter tragen, ist es heutzutage strengst nicht zulässig. Können solche Manipulationen so gut simuliert werden, dass man auf Korrektheit der Berechnung mit vollster Sicherheit aufbauen kann? Oder sollen die Moralvorstellungen der Gesellschaft angepasst werden, um solche Experimente mit Gemeinschaftswohlvorhaben zu rechtfertigen? Vielleicht und eher wahrscheinlich werden genetische Manipulationen am Menschen bereits geheim geführt.

Die Forderung nach dem Verbot der gentechnischen Forschung ist der Forderung nach dem Verbot oder Aufhalten des Fortschrittes gleichzusetzen. Solche Forderungen entsprechen nicht der menschlichen Natur und dem Drang nach dem Neuen. Jeder künstlicher Eingriff führt nur dazu, dass die Forschung aus dem Blick der Gesellschaft verschwindet und geheim weitergeführt wird. Die mit der Forschung verbundenen Diskussionen finden nicht statt, was das Verantwortungsgefühl und die Klarheit in der Einschätzung von Tragweiten bei den Forschern nicht steigert.

2.3 Künstliche Intelligenz

Die moderne Gesellschaft definiert sich als eine Informationsgesellschaft und es ist fast nicht mehr möglich, ein Mitglied davon zu sein, ohne den Gebrauch von den Entwicklungen zu machen. Die Mechanismen werden immer komplizierter und ihre Beherrschung stellt selbst für einen gebildeten hochqualifizierten Menschen große Anforderung vor allem der intellektuellen Natur. Es werden gleichzeitig Anforderungen nach einerseits intelligenten und andererseits leicht

bedienbaren Systemen gestellt. Eine mögliche Lösung dafür versprechen sich die Lösungen, die sich auf dem Nutzen von künstlicher Intelligenz basieren.

Unter Intelligenz versteht man die Fähigkeit eines Wesens oder einer Maschine, einen bestimmten messbaren Erfolgsgrad bei der Suche nach einer Lösung unter den zahlreichen Möglichkeiten. Dabei unterscheidet man zwischen dem Wissen und der Intelligenz. Wissen ist eine vom Wesen akkumulierte Information. Intelligenz impliziert eine Fähigkeit, eine Voraussage über die Umgebung zu erschliessen und die Fähigkeit, auf jede Voraussage eine Reaktion abzubilden, die zum Ziel führen würde.

Der Begriff der künstlichen Intelligenz wird auch verschieden gedeutet. Man geht heute davon aus, dass die künstliche Intelligenz erst dann als Intelligenz anzusehen ist, wenn eine Maschine die Aufgaben übernimmt, die ein Mensch nicht lösen kann und das nicht durch Operationsgeschwindigkeit der Maschine, sondern durch die Anwendung einer neuartigen Methode erreich wird[3].

Die Frage, ob eine Maschine denken kann, ist eng mit Frage, wie man feststellt, ob eine Maschine denken kann, verbunden. Zum ersten Mal wurden diese Fragen von Alan Turing in seinem Artikel "Computing machinery and intelligence"gestellt. Turing meint, dass ein Kriterium eine Imitation sein kann. Wenn die Maschine die Fragen eines Menschen so gut beantwortet, dass wir nicht feststellen können, ob wir als Dialogpartner eine Maschine oder einen anderen Menschen haben, dann sollen wir anerkennen, dass es eine den denkende Maschine ist. Es gibt keine rationale Gründe, warum eine Maschine nicht bestimmte Aufgaben erledigen könnte. Basierend auf dem Prinzip der vollständigen Induktion kann man zeigen, dass eine Maschine Aufgaben beliebiger Komplexität lösen kann[4]. Wie bei der vollständigen Induktion ist die erste Frage, wo soll man anfangen. Sollte man als erstes dem Rechner Lösung von abstrakten Aufgaben beibringen? Oder fängt man wie bei einem Kind mit dem Erkunden der Umwelt an, in dem man Gegenstände zeigt und sie benennt? Weitere Jahrzehnte hat man versucht, beide Methoden auszuprobieren.

Die Rechner sind inzwischen viel schneller und Algorithmen sind ausgeklügelter geworden. Es scheitert aber immer noch an den beiden Bestandteilen. Die modernen Rechner besitzen eine Rechenleistung, die mit der Gehirnleistung von Insekten vergleichbar wäre. Das Gehirn eines Menschen enthält etwa 100 Milliarden Neuronen, jeder von denen etwa 5000 Synapsen hat. Man schätzt, dass ein Rechner eine Leistung von 100 Tops und Speichern im Umfang von 100 Tb haben muss, um menschliche Gehirntätigkeit zu simulieren. Diese Stufe soll in 15 bis 20 Jahren erreicht werden[3].

Doch allein die Rechenleistung ist nicht ausreichend. Jeder Rechner braucht ein passendes Programm. In diesem Softwarebereich sieht man heute die grössten Schwierigkeiten, die noch zu lösen sind. Es gibt zwar Fortschritte bei der Nachbildung der im Gehirn ablaufenden Prozesse, wie neuronale Netze. Ein Problem bleibt das Gehirn an sich. Es ist nicht ausreichend erforscht. Ein weiteres Problem ist die Softwareentwicklung selbst. Für ein neues Betriebssystem eines Rechners werden heute mehrere Jahre Entwicklungszeit gebraucht. Die Entwicklung von künstlicher Intelligenz ist eine Aufgabe anderer Ordnung. Man gehe davon aus, dass zwischen 10 und 20 Jahren nach der Entwicklung eines passenden Rechners vergehen werden, bis erste Programme entwickelt werden[3].

Wenn die künstliche Intelligenz auf dem Niveau der menschlichen sein wird, so stellt sich die Frage, ob die menschliche Intelligenz ein Endstadium im Intelligenzmass darstellt und die Intelligenz beschränkt ist. Wenn nicht, was sehr wahr-

scheinlich ist, dann könnten man vorstellen, dass der Mensch oder die künstliche Intelligenz, die zu Eigenentwicklung und Weiterforschung ja fähig sein soll, eine neue Art der Intelligenz entwickeln, die die menschliche übersteigt. Wenn diese Superintelligenz einst existiert, kann eine Kettenreaktion ausgelöst werden, so dass die neuen Intelligenzformen sich mit immer steigender Geschwindigkeit überholen.

Wird der Mensch die Kontrolle über die künstliche Intelligenz behalten können? Und über die mögliche Superintelligenz? Werden die sich auf künstlicher Intelligenz basierenden Systeme freundlich zur Menschheit sein oder wird eine Konkurrenz um Ressourcen mit anschliessendem Konflikt entstehen? Die Antworten auf diese Fragen fallen für den Menschen meist negativ aus. Wie bei der Genetik, wird vorgeschlagen, weitere Forschungen auf dem Gebiet zu stoppen. Eine Lösung wäre es nicht. Wenn solche Intelligenzformen einmal existieren, dann werden wie immer die Natur und die Evolution gewinnen. Die Menschen werden von Maschinen abgelöst.

3 Posthumanismus

Mit dem Fortschritt ändert sich nicht nur die uns umgebene Welt. Der Mensch an sich ist in den Prozess mit einbezogen. Eine Wandlung erlebt die Wahrnehmung sich selbst und seiner Rollen und Fähigkeiten. Diese Neudefinition von sich selbst bezeichnet man als Transhumanismus. Am Ziel der Weiterentwicklung sollen die Änderungen sehr groß sein und werden im Konzept des Posthumanismus gefasst.

3.1 Transhumanismus

Der Mensch hat sich immer als nicht ideal empfunden und war bestrebt über sich hinauszuwachsen. Im Humanismus sind Verbesserungsvorschläge eine ideeller Natur. Man muss seinen Geist entwickelt. Durch die Erziehung sollen immer bessere Menschen aufwachsen, die dann die Umwelt entsprechend verbessern.

Transhumanismus stellt die natürliche Evolution der menschlichen Spezies in Vordergrund. Der Mensch ist ist nicht Spitze der Evolution und hat Potenzial sich selbst zu etwas anderem weiterzuentwickeln. Die Entwicklung kann der Mensch selbst anstossen und regulieren. Der Organismus und die Intelligenz sind im Visier der Transhumanisten. Grundlegende menschliche Grenzen in beiden Bereichen sollen und können überwunden werden. Man soll dabei aktiv die Errungenschaften des Fortschritts eingesetzt werden. Die Älterungsprozesse sollen verlangsamt, Krankheitsresistenzen aufgebaut, Prothetik aktiv eingesetzt und die geistige Kapazitäten gesteigert werden[2].

Transhumanismus stellt an sich einen Umbruch im Denken dar, was der Mensch ist. Es sind zwar viele von den Technologien noch nicht soweit fortgeschritten, um eine Lösung darzustellen, sollte der Mensch aber so eine Lösung einsetzten, sobald sie verfügbar ist.

3.2 Posthumanismus

Posthumanismus geht noch weiter und beschreibt das Konzept einer Fortentwicklung des Menschen. Die Technlogien sind in dem Konzept soweit fortgeschritten, dass der Mensch sich dem seinem eigenem Körper entledigen kann

und weiter als reines Bewusstsein existieren. Das Entledigen soll durch das sogenannte Üploading"geschiehen. Dabei werden alle Parameter eines Individuums erfasst und in digitale Form übertragen. Man unterscheidet dabei zwischen dem destruktiven und nicht-destruktiven Uploading. Bei dem destruktiven Uploading wird der Körper bei dem Ablesen von Daten zestört. Der Mensch existiert nur als Maschine, Programm o. ä. Bei dem nicht-destruktiven Uploading bleibt der Mensch in seiner ursprünglichen Form weiterleben und seine Abbildung führt ein Koexistenz in der Form, die dafür mögliche sein wird[1].

Durch das Uploading sollte der Traum vom ewigen Leben wahr werden. Uploading würde aber auch grundlegend die Vorstellung über die existierende Welt ändern. Der eingefangene Geist könnte sich durch Kommunikationskanäle sekundenschnell bewegen. Es könnten weitere Kopien angefertigt werden und die rechtliche Auffassung von einer Person in Frage stellen. Was nutzen dann den "hochgeladenen"Menschen die nicht "hochgeladenen". Würde eine Zweiklassengesellschaft mit der daraus resultierenden Konkurrenz um Ressourcen entwickeln? Braucht man die Menschen dann immer noch? Bleiben die "hochgeladenenïmmer noch Menschen?

4 Fazit

Der weitere Fortschritt bringt mit sich neben den Vorteilen viele Fragen und Gefahren. Man träumt von einem sorglosen Leben, wo keiner arbeiten muss, weil alles von Nanorobotern erstellt wird, und weiss man nicht, wie man dann die Menschen beschäftigt. Man will sich selbst gegen Krankheitserreger durch gentechnischen Eingriffe schützen und ist sich den möglichen Tragweiten nicht klar. Von der künstlichen Intelligenz verspricht man sich ausgeklügelte Systeme und Hilfe bei der Forschung und geht bewusst das Risiko ein, dass solche Systeme uns überlegen sein können.

Die Utopien können schnell zu Anti-Utopien werden. Im technologische Bereich ist es bereits mit Atomenergie passiert. Gentechnik wird von vielen als kritisch eingestuft und bestimmte Forschungen bleiben verboten. Informations- und Nanotechnologien werden durch indirekte Verbindung mit dem Menschen als unkritisch eingestuft, können aber auch zu katastrophalen Szenarios führen.

In der Tatsache, dass der Fortschritt nicht zu stoppen ist, benötige man in einigen Bereichen bereits heute die (interdisziplinären) Diskussionen, wie man bestimmte Probleme in Zukunft vorbeugt und mit den unabwehrbaren negativen Folgen umgeht.

Literatur

[1] http://www.wired.com/wired/archive/8.04/joy.html

[2] http://www.transhumanism.org/index.php/WTA/more/162/

[3] http://www.aiplayground.org/artikel/agi/

[4] http://loebner.net/Prizef/TuringArticle.html

[5] http://de.wikipedia.org/wiki/Humangenomprojekt

[6] http://de.wikipedia.org/wiki/Gen

[7] http://www.g-o.de/wissen-aktuell-9447-2009-02-02.html

[8] http://www.its.caltech.edu/ feynman/plenty.html

[9] http://de.wikipedia.org/wiki/Nanotechnologie

[10] http://de.wikipedia.org/wiki/Utopie