Fachhochschule Braunschweig/Wolfenbüttel
Fachbereich Wirtschaft

Elektronische Kriegsführung, Spionage und Datenschutz

Hausarbeit

eingereicht bei Diplm.-Inform. H. Märtens

von Frank Adamczak
Kriemhildstraße 29
38106 Braunschweig
Matr.-Nr. XXXXXXXX

Wolfsburg, den 20.12.2004

Inhaltsverzeichnis

Abkürzungsverzeichnis

BfV	Bundesamt für Verfassungsschutz
BND	Bundesnachrichtendienst
EADS	European Aeronautic Defence and Space Company
EloGM	Elektronische Gegenmaßnahmen
EloKa	Elektronische Kampfführung
e.V.	eingetragener Verein
Faust	Führungsausstattung taktisch
FoeBuD	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.
FOGIS	Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik
GG	Grundgesetz
HF	High Frequency
html	Hyper Text Markup Language
http	Hyper Text Transfer Protocol
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
MAD	Militärischer Abschirmdienst
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OSINT	Open Source Intelligence
pdf	Portable Document Format
php	PHP: Hypertext Preprocessor
SIGINT	Signal Intelligence
SAR-Lupe	Synthetic Aperture Radar-Lupe
VHF	Very High Frequency

1. Einleitung

Unsere Welt befindet sich in einem gesellschaftlichen und technologischen Wandel. Fortschritte in der Informations- und Kommunikationstechnik haben weitreichende Bedeutung für das tägliche Leben der gesamten Bevölkerung, insbesondere in den entwickelten Industriestaaten.
Noch nie war es so einfach, dass große Teile der Bevölkerung, am Informationszeitalter teilhaben können. Schon durch einen leicht zu beschaffenden Internetzugang ist dies heutzutage möglich.
Die „Forschungsgruppe Wahlen online“ stellte unlängst fest, dass im 3. Quartal 2004 61 Prozent der erwachsenen deutschen Bevölkerung einen Zugang zum Internet besitzen.[1]
Durch die Nutzung des Internets und anderer moderner Kommunikationstechnologien, kann in vielfältiger Weise das tägliche Leben, auf den ersten Blick, erleichtert werden. Innerhalb kürzester Zeit, ist es möglich Bücher im world wide web zu bestellen, Reisen zu buchen oder auch die moderne Form der Postkarte, die E-Mail, zu versenden. Ebenso bedarf es nur geringer finanzieller Mittel, um von allen Teilen der Erde Kommunikationsverbindungen herstellen zu können.

Dieser technologische Fortschritt erfasst nicht nur die zivilen Bereiche der Gesellschaft. Gerade die Militärs aller Staaten sind daran interessiert, technologische Errungenschaften in die Strukturen der Streitkräfte einzubinden. In der modernen Kriegsführung ist der Einsatz modernster Aufklärungs-, Kommunikations- und Kampfmittel nicht mehr wegzudenken. Auch ist der Forscherdrang, vor allem der amerikanischen Streitkräfte, in technologische Zukunftsfelder sehr ausgeprägt.

Auf den ersten Blick wird unser aller Leben durch den technologischen Fortschritt vereinfacht. Aber eine Medaille besitzt immer zwei Seiten. Die eine Seite verspricht uns Erleichterungen in allen Lebenslagen, aber die andere Seite zeigt uns ebenso die Abhängigkeiten und Risiken, die mit der zunehmenden Technisierung des Lebens verbunden sind.
In dieser Arbeit möchte ich zeigen, welche Möglichkeiten es gibt, technologische Errungenschaften im Rahmen der elektronischen Kriegsführung einzusetzen und wie die Bereiche der Spionage und des Datenschutzes vom technologischen Fortschritt in positiver und negativer Weise berührt werden.

[1] Vgl. o.V. (2004), http://www.forschungsgruppe.de/Ergebnisse/Internet-Strukturdaten/web_III_04.pdf.

2. Elektronische Kriegsführung

Mit dem Begriff der elektronischen Kriegsführung werden militärische Handlungen bezeichnet, die gegnerische elektronische Geräte, wie Computersysteme oder Systeme die Computerchips enthalten, manipulieren, kontrollieren oder zerstören sollen. In diesem Zusammenhang werden auch die Begriffe „Cyber War“, „Electronic Warfare“ oder auch „Elektronische Kampfführung“ verwendet.

Ein Problem besteht in der Abgrenzung zum „Information Warfare“, da dieses Themenfeld sich neben der Manipulation und Erlangung von Daten, auch auf die Zerstörung von Kommunikationsträgern konzentriert. Die Mittel für diese Zielerreichung sind hier z.B. Computerviren oder Würmer.

In der Literatur werden die oben genannten Terminologien in unterschiedliche Beziehungen zueinander gesetzt. Der Bundesnachrichtendienst setzt beispielsweise die elektronische Kriegsführung und Information Warfare in einen Kontext. Dies liegt darin begründet, dass nach Auffassung des BND diese beiden Instrumente der Kriegsführung die selben Ziele verfolgen.

Die Anwendung von gezielten Störmaßnahmen kann bis zu dem 1. Weltkrieg zurückverfolgt werden. In diesem Krieg versuchte die britische Royal Navy den deutschen Morseverkehr zu stören und zu manipulieren. Mit dem Aufkommen von Radar und drahtloser Kommunikation wurde der eigentliche Begriff „elektronische Kriegsführung“ geprägt.

Bei der Anwendung und Nutzung von elektronischen Technologien, stehen nicht konventionelle militärischen Ziele, wie das Nehmen von Geländeteilen oder das Zerschlagen von gegnerischen Truppenverbänden, im Vordergrund. Vielmehr wird hier die Absicht verfolgt, Kommunikationssysteme ziviler und militärischen Einrichtungen und Waffensysteme zu kontrollieren, zu manipulieren oder auch zu zerstören.[2] Als ein Schwerpunkt der elektronischen Kriegsführung kann die Außerkraftsetzung der Nutzung von militärischen Kommunikationssystemen im Vorfeld der eigentlichen konventionellen Kampfhandlungen gesehen werden. So wird diese Art der Kriegsführung vorbereitend und begleitend zum konventionellen Kampf eingesetzt.

[2] Vgl. o.V. (2004), http://de.wikipedia.org/wiki/Elektronische_Kriegsf%C3%Bchrung.

Erfolge in diesem Bereich können durch unterschiedlichste Waffensysteme erzielt werden. Gegnerische Kraftwerke werden von Flugzeugen mit Raketen beschossen. Diese Raketen enthalten Kohlefaserbündel, die sich über die elektrischen Leitungen des Kraftwerks legen und einen Kurzschluss verursachen. Somit ist das Kraftwerk zwar nicht zerstört, aber eine langfristige Stromunterbrechung wird erreicht.

In den Operationen „Desert Shield“ und „Desert Storm“ 1990 bis 1991, die den Zweck der Befreiung Kuwaits vom Irak hatten, wurden solche Angriffe erfolgreich durchgeführt. Hier kann man sehen, mit welchen relativ einfachen Mitteln, ein Teilzusammenbruch der gegnerischen Infrastruktur herbeigeführt werden kann.

Eine elegantere Methode, ist die Nutzung des Elektromagnetischen Impuls, auch EMP genannt. Er wurde erstmals bei überirdischen Atomversuchen entdeckt. Bei einer thermonuklearen Explosion entsteht für umliegende elektronische Geräte eine Überspannung, die zu einer Funktionsunfähigkeit der Selbigen führt.

2.1 Elektronische Kampfführung

Zur weiteren Erklärung der elektronischen Kriegsführung, muss ebenfalls der Begriff „elektronischen Kampfführung“ näher erläutert werden. Nach der gängigen Definition in der Bundeswehr umfasst sie alle Maßnahmen und Mittel der Fernmelde- und Elektronischen Aufklärung, sowie die des elektronischen Kampfes.[3]
Große militärische Bedeutung kommt der elektronischen Kampfführung zu. Ihr wird die Aufgabe zugeteilt, elektromagnetische Ausstrahlungen gegnerischer Kräfte aufzuklären. Weiterhin wird versucht, durch Gegenmaßnahmen diese Ausstrahlung unwirksam zu machen. Die Untersuchung der elektromagnetischen Ausstrahlung der eigenen Systeme und deren Minimierung ist eine weitere Aufgabe der elektronischen Kampfführung.[4]

[3] Vgl. o.V., http://www.streitkraeftebasis.de/C1256C290043532F/vwContentFrame/FD293B60E634E7CEC1256EA000375924.
[4] Vgl. Wehrtechnische Dienststelle für Informationstechnologie und Elektronik (2003), http://www.bwb.org/C1256DF2004FF94C/Docname/ORGANISATION_WTD81_AUFGABEN_ELOKA_ELOKA.HTM.

Folgende drei Unterscheidungen können getroffen werden:

Elektronische **Gegenmaßnahmen** (Electronic Counter Measures) stellen die erste Unterscheidung dar. Die gegnerische aktive Nutzung des gesamten elektromagnetischen Spektrums soll durch eigene aktive Maßnahmen verhindert werden.

Durch elektronische **Schutzmaßnahmen** (Electronic Protective Measures), wird der Erfolg gegnerischer aktiver Maßnahmen eingeschränkt oder sogar ganz unterbunden. Hier wird noch einmal in aktive und passive Schutzmaßnahmen unterschieden. Im aktiven Bereich werden z.B. Funkgeräte genutzt, die einen selbstständigen Frequenzsprung ermöglichen. Der passive Bereich wird vor allem durch eine gute Ausbildung des Bedienpersonals erreicht.

Eine letzte Unterscheidung, stellen elektronische **Unterstützungsmaßnahmen** (Electronic Support Measures) dar. Hier können durch den passiven Empfang von gegnerischen elektromagnetischen Strahlen, Informationen über die Gegenseite gewonnen werden.[5]

2.2 Kommando Strategische Aufklärung der Bundeswehr

In der Bundeswehr gibt es mit dem am 17. Januar 2002 gegründeten Kommando Strategische Aufklärung einen eigenen Verband zur teilstreitkraftübergreifenden Aufklärung, mit 6.300 Soldaten und 700 zivilen Mitarbeitern. Hauptaufgabe des Kommandos ist es, der politischen und militärischen Führung der Bundeswehr grundsätzliche Informationen bereitzustellen. Gerade für die Auslandseinsätze der deutschen Streitkräfte ist es nun möglich, wichtige Informationen in einer Anlaufstelle zu bündeln. Der Sitz des Kommandos befindet sich in Rheinbach bei Bonn.[6] Die vorher schon in den Streitkräften vorhandenen Kräfte zur elektronischen Kampfführung, wurden in diesem teilstreitkräfteübergreifenden Großverband zusammengefasst. Zu diesem Kommando gehören die ehemaligen ortsfesten und mobilen Aufklärungskomponenten der einzelnen Teilstreitkräfte, sowie die Satellitengestützte abbildende Aufklärung.[7]

[5] Vgl. o.V. (2004), http://de.wikipedia.org/wiki/Elektronische_Kampff%C3%Bchrung.
[6] Vgl. o.V. (2002), http://www.bundeswehr.de/forces/streitkraeftebasis/030110_strat_aufkl.php.
[7] Vgl. Lorenz, H. D. (2002), http://www.sipotec.net/IAP_Aktuell/S_02_09.html.

2.2.1 Mobile Aufklärung und Gegenmaßnahmen

Mit den mobilen Teilen der ehemaligen EloKa Truppe werden heute die Einsatzkontingente der Bundeswehr in den Einsatzländern unterstützt. Im Kosovo oder auch in Afghanistan wird das elektro-magnetische Spektrum überwacht, Radarquellen erfasst, sowie feindliche Sender geortet. Aus diesen Informationen kann ein Lagebild erstellt werden, dass der eigenen Truppe zur Verfügung gestellt wird.[8]

Als mobiles System steht im Einsatzland der Transportpanzer Fuchs als Variante Fernmeldeaufklärung und Variante Hummel zur Verfügung. Er ist seinen verschiedenen Ausstattungsversionen mit einem Störsendergerät 33, einem HF/VHF-Aufklärungsgerät, sowie einem VHF Fernmeldeaufklärungssystem ausgestattet. Mit dem Störsendergerät 33 ist es möglich auf 16 Frequenzen gleichzeitig, und das über den gesamten Frequenzbereich, Daten- und Sprachfunk zu stören. Zur Aufklärung potentieller EloGM Ziele, wird ein weiterer Fuchs Panzer mit einem HF/VHF-Aufklärungsgerät genutzt. Durch ihre Adcock-Peiler kann Truppenfunk im Bereich von 1,6 bis 512 MHz empfangen werden.[9]

Mit dem Transportpanzer Fuchs als Variante Fernmeldeaufklärung ist es unter zu Hilfenahme des VHF Fernmeldeaufklärungssystem möglich, Daten- und Sprachfunk abzuhören. Wie bei der Variante Hummel, ist auch hier ein Adcock-Peiler vorhanden, der den selben Bereich des taktischen Truppenfunks erreichen kann.[10]
Eine Überprüfung der aufgefangen Daten auf ihren taktischen Inhalt und eine Störung der Kommunikation des Gegners wird mit diesem System gewährleistet.

2.2.2 SAR-Lupe

Zu den weiteren Aufgaben des Kommandos strategische Aufklärung gehört die Satellitengestützte Aufklärung, die der Bundeswehr erstmals eine eigene raumgestützte abbildende Aufklärung ermöglicht.[11] Die SAR-Lupe ist ein Satellitengestütztes Aufklärungssystem. Es besteht aus fünf baugleichen Kleinsatelliten und einem Bodensegment. Mit diesem System wird der Bundeswehr ein System zur Verfügung gestellt, das es ihr ermöglicht, jederzeit und unabhängig von Dritten Informationen zur strategischen Aufklärung zu

[8] Vgl. Schuldt F. (2003), http://www.streitkraeftebasis.de/C1256C290043532F/vwContentFrame/5EB0F4856E3BA144C1256EA000252BCB.
[9] Vgl. o.V. (2001), http://www.sipotec.net/Neu_Ausr/Waffensysteme/hummel_beschr.html.
[10] Vgl. o.V. (2001), http://www.sipotec.net/Neu_Ausr/Waffensysteme/fuchsfmaufkl_beschr.html.
[11] Vgl. Lorenz, H. D. (2002), http://www.sipotec.net/IAP_Aktuell/S_02_09.html.

beschaffen. Die volle Einsatzbereitschaft wird im Jahre 2007 hergestellt sein, denn zu diesem Zeitpunkt wird der letzte Satellit in die Umlaufbahn geschossen. Bis 2015 ist es dann möglich, aus einer Höhe von 500 km hochauflösende Aufklärungsbilder zu erstellen. Die einzelnen Satelliten werden über drei Bahneben im Weltall verteilt. Die einzelnen Satelliten werden mit ihren Parabolantennen auf das Aufklärungsobjekt gerichtet. So ist es nun möglich im interessanten Aufklärungsgebiet 30 Bilder pro Tag zu schießen und dies mit einer Auflösung im höchsten Bereich von 5,5 mal 5,5 km und im hohen Bereich von 60 mal 8 km. Ein weiterer Vorteil des Systems ist, dass die Bilder zu jeder Tages- und Nachtzeit, sowie bei jeder Wetterlage erstellt werden können. Mit der erforderlichen Aufnahme, Verarbeitung und Weiterleitung der erhaltenen Daten, wird das Bodensegment betraut.

Durch die mittelständische OHB System AG mit Sitz im Bremer Technologiepark, wird die Betriebsüberwachung und Wartung des SAR-Lupe Systems gewährleistet. Sie ist als industrieller Systemführer der Hauptauftragnehmer für das SAR-Lupe System und führt weiterhin ein nationales, sowie internationales Industrieteam, dass sich mit der Erstellung der Satelliten und dem Bodensegment befasst.

Für Europa schließt die Inbetriebnahme des deutschen strategischen Satellitenaufklärungssystem eine Lücke, da im europäischen Aufklärungsverbund eine solche strategische Aufklärungs-komponente bis jetzt noch fehlt.[12]
Ab 2007 ist es möglich der europäischen politischen und militärischen Führung ein Instrument der Aufklärung zur Verfügung zu stellen, das es ihr ermöglicht, von den USA unabhängig, eigene strategische Aufklärung zu betrieben. Aus der jüngeren Geschichte zeigt sich, dass das amerikanische Militär nur temporär mit seinen Verbündeten zusammenarbeitet, obwohl ein großer Teil der europäischen Staaten mit der USA in der NATO militärisch vereint ist. So gibt das US-amerikanische Militär nur für klar umrissene Teileinsätze, und dies auch nur für eine bestimmte Zeit, ihre eigenen Aufklärungsergebnisse an die eigenen Verbündeten weiter.
Mit einem eigenen europäischen Sattelitenaufklärungssystem kann Europa sich ein weiteres Stück Unabhängigkeit von der amerikanischen Technologieüberlegenheit sichern. Diese Maßnahmen sollten nicht als Schaffung eines Gegenpols gegenüber den USA gelten, sondern als Stärkung des europäischen Partners in der Weltpolitik angesehen werden.

[12] Vgl. o.V. (2003), http://www.ohb-system.de/dt/pdf/sar-lupe-broschure.pdf.

2.3 US-Streitkräfte erobern den Cyberspace

Für die USA ist der internationale Terrorismus eine Bedrohung der existierenden Ordnung. Global denkend und lokal handelnd, ist nur ein Kennzeichen der im 21. Jahrhundert handelnden Terroristen. Für sie ist der Globus eine einzige Aktionsfläche. Anschläge werden aus der Anonymität der Zivilgesellschaft, in der sich Terroristen verstecken, geführt.[13]
In einem Beispiel griff eine pakistanische Hackergruppe eine US-Verwaltung an und drohte bei einer Nichteinstellung der Angriffe in Afghanistan, geheime Regierungsdaten an Terroristenführer Bin Laden zu liefern.[14]

Im Bereich der amerikanischen Sicherheitspolitik gehören Angriffe aus dem Cyberspace zu einer wahrscheinlichen Möglichkeit, die ein „elektronisches Pearl Harbor" auslösen können. Seit zehn Jahren ist mit solchen Angriffen, laut einigen amerikanischen Sicherheitspolitikern, zu rechnen.
Es gibt verschiede Varianten die Gesellschaft in den USA zu treffen oder die amerikanische Infrastruktur lahm zu legen. Flugsicherungssysteme können ausgeschaltet, Denial-of-Service-Attacken gegen verschiedene Server gestartet oder wie im oben genannten Beispiel Regierungseinrichtungen gehackt werden. Eine klare Trennung zwischen militärischen und zivilen Zielen ist nicht mehr ohne weiteres möglich. Aufgrund von gemeinsam genutzten Kommunikationsverbindungen, wie Telefonleitungen oder auch das Internet, kann es zu weltweiten Auswirkungen kommen.
Zu den Urhebern solcher Angriffe zählen nach Meinung der US-Geheimdienste islamische Terroristen, die chinesische Volksbefreiungsarmee, das Militär von Kuba oder auch die Regionalmacht Indien.

Der Ursprung all dieser strategischen Analysen ist in den Vereinigten Staaten von Amerika selbst zu suchen. Seit Anfang der 1990er erforschen und erproben amerikanische Militärs unter größter Geheimhaltung elektronische Waffen und mögliche Varianten eines Hackerkriegs. Bis 1996 wurden lediglich defensive Maßnahmen zum Schutz der eigenen Dateninfrastruktur erforscht. Seit 1996 trat nun auch ein offensives Konzept des Cyberkrieges in den Vordergrund, das sich mit aktiven „Computer-Netzwerkattacken" beschäftigte.[15]

[13] Vgl. Palm, G./Rötzer, F. (2002), S. 10ff.
[14] Vgl. Hutter, R. (2002), http://www.bpb.de/publikationen/NVN0CA,2,0,CyberTerror:_Risiken_im_Informationszeitalter.html.
[15] Vgl. Bendrath, R. (2001), http://www.heise.de/tp/r4/artikel/7/7892/1.html.

2.3.1 Joint Information Operations Center

In den amerikanischen Streitkräften beschäftigen sich nicht weniger als 29 Abteilungen mit dem Thema der offensiven Cyberangriffe. Das Joint Information Operations Center mit Sitzt in San Antonio in Texas nimmt z.B. Aufgaben der Computerkriegführung, psychologische Operationen, Aufklärung und elektronische Kriegsführung war. In dieser Organisation arbeiten ca. 150 Soldaten der US-Streitkräfte, sowie Militärgesandte dreier verbündeter Staaten.
Als Unterstützungs- und Forschungsabteilung arbeitet sie weiterhin auch eng mit der NSA und der Air Intelligence Agency zusammen.[16]

2.3.2 Informationskrieg

Mit dem Wandel einer postindustriellen Gesellschaft zu einer Informationsgesellschaft, werden große Transformationsvorgänge ausgelöst. Die Ressourcen Mensch und Maschine werden von der Ressource Information zunehmend abgelöst. Im militärischen Bereich bedeutet das auch eine Abwendung von alten Militärkonzepten mit Massen von Soldaten und Panzern. Militärische Ziele, wie die Zerschlagung des Gegners, treten in den Hintergrund, dafür ist jetzt eine Fokussierung auf Informationsverarbeitungssysteme zu beobachten.
In den amerikanischen Streitkräften ist der Informationskrieg ein übergreifendes Konzept. Er soll durch die Kontrolle der gegnerischen Informationswege eine Informationsüberlegenheit schaffen. Für die Zielerreichung werden psychologische Maßnahmen mit Flugblättern, konventionelle Angriffe auf Kommunikationszentralen und –leitungen oder auch elektronische Angriffe genutzt.

Einige Schwierigkeiten bestehen aber bei den elektronischen Angriffen. Als erstes müssen gegnerische Kommunikationsstrukturen erst einmal erkannt und in ihrer Bedeutung für den Gegner eingeordnet werden, da eine technische Infrastruktur eben nur einen Teilaspekt im Gesamtkontext einer Gesellschaft darstellt. Cyberangriffe gelten als riskant, da Auswirkungseffekte auf zivile Einrichtungen und Infrastrukturen, wie oben schon einmal beschrieben, nicht ausgeschlossen werden können und Präzedenzfälle geschaffen werden, die mit dem internationalen Recht nicht vereinbar sind.

[16] Vgl. Bendrath, R. (2001), http://www.fogis.de/fogis-ap3.PDF.

2.3.3 Die Waffen des Cyberkrieges

Durch den technologischen Fortschritt, erweitert sich das Repertoire an Waffen für den Cyberkrieg ständig. Mit passiven Abhörattacken, zu denen Netzwerkmonitorring und Entschlüsselung gehört, oder aktive Netzwerkattacken die aktive Systemeinbrüche beinhalten, sind diese nur ein Teil Anwendungsmöglichkeiten. Viele dieser Maßnahmen sind nicht neu, werden jetzt aber auch in militärische Strukturen eingebunden. Durch die oben genannten aktiven Netzwerkattacken wird in gegnerische Computersysteme eingebrochen und auch nach Bedarf mit einem „boshaften Code“ verseucht. Hier sind mit Viren, Würmern, trojanischen Pferden oder diversen Skripten nur einige Beispiele zu nennen, die es ermöglichen Computersysteme zu manipulieren. Es muss aber auch die militärische Einsatzfähigkeit betrachtet werden, denn Viren und Würmer sind in ihrer Ausbreitung kaum zu begrenzen und laufen dementsprechend dem Konzept von chirurgischen Präzisionsangriffen entgegen. Somit wären eingebaute Hintertüren in Softwareprodukten eine elegantere Möglichkeit, um in fremde Computersysteme einzudringen, zumal auch diese Zugriffe nicht bemerkt werden sollen.

Die US-Luftwaffe entwickelt ebenfalls Infowar-Systeme. Ein Ziel ist es beispielsweise gegnerische Luftabwehrstellungen zu manipulieren. Im Jahre 2002 wurde dieses System erstmals unter zu Hilfenahme der Flugzeugtypen RC-135 Rivet Joint und der EC-130 Compass Call getestet. Im Gegensatz zur herkömmlichen Ausschaltung von Luftabwehrstellungen mit Raketen, wird hier ein neuer Weg beschritten. Der Angriff läuft über das Computernetz des gegnerischen Systems. Es bestehen zwei Alternativen. Die erste Alternative ist die Ausschaltung des Netzes und die damit verbundene Wirkungslosigkeit der Abwehrstellung. Eine zweite Alternative manipuliert das Computersystem. Somit können falsche Ziele eingegeben oder auch irreführende Informationen in das Netz eingespeist werden. Dieses System ist noch in der Erprobung, stellt aber nach Meinung der US-Luftwaffe eine vielversprechende Alternative dar. Ziel der Entwicklung wird es sein, dass gegnerische Radaranlagen so manipuliert werden, dass Luftabwehrstellungen keine Boden-Luft-Raketen mehr abschießen. Übungen mit diesem System werden in den Flugverbotszonen des Iraks durchgeführt. Dabei können simulierte oder auch echte Beschussübungen durchgeführt werden. In diesen Zonen des Iraks sammelte die US-Luftwaffe wertvolle Informationen über die elektronischen Signaturen und Sendebereiche der irakischen Systeme.

Ebenfalls von Interesse ist die schon einsatzfähige Möglichkeit, den Inhalt gegnerischer Radarschirme zu sehen. Hiefür werden Satelliten der NSA genutzt, die dann mit amerikanischen

Aufklärungsflugzeugen eine Kommunikationsverbindung herstellen. Daraus kann ein großer Nutzen gezogen werden. Zum Einen erkennt man selber, ob das gegnerische System das eigene Flugzeug erfasst hat und somit ein Ausweichen stattfinden kann. Zum Anderen wird erkannt, dass das eigene Flugzeug noch nicht aufgefasst wurde und somit ein Angriff auf die Radarstellung stattfinden kann.

2.4 Neue Techniken im Krieg der Zukunft

Wie sieht die Gestaltung zukünftiger Kriege aus?
Es ist davon auszugehen, dass bestehende Technologien weiter verbessert werden und die sich noch im Entwicklungsstadium befindlichen Hightech - Kriegstechnologien in den nächsten Jahren ihren praktischen Einsatzstaus erhalten. Das Potential des Cyber War scheint noch lange nicht ausgeschöpft zu sein. Man befindet sich vielmehr noch am Anfang der Entwicklung und Nutzung.
Wenn man den Krieg in Afghanistan im Jahre 2001 und den Irakkrieg 2003 betrachtet, sieht man eine mögliche Option für die Zukunft. Ein schneller Aufmarsch der Truppen mit modernster Ausrüstung und ein vorbereitender und begleitender Einsatz von Cyber War Techniken kennzeichneten diese zwei Kriege.

2.4.1 Drohnen

Als sehr nützlich haben sich Drohnen für Echtzeitaufklärung erwiesen. Die „Global Hawk“ von Northrop Grumman aus den USA stellt für die U.S.-Streitkräfte ein sehr modernes Aufklärungssystem zur Verfügung. Sie kann bis zu 35 Stunden in der Luft operieren und schafft es in 24 Stunden ein Gebiet von 40.000 Quadratmeilen zu scannen. Eigenständige Lagekontrolle, Navigation und Systemkontrolle, zeichnen dieses System aus. Von der Bodenstation werden nur noch Flugmanöver oder neue Flugkurse autorisiert. Angriffe gegen die Drohne werden selbstständig ausgewertet und Gegenmaßnahmen selbstständig eingeleitet. Mit modernsten Sensoren, kann dieses auch als „Unmanned Aerial Vehicle“ bezeichnete Aufklärungssystem Echtzeitüberwachung betreiben. Dazu sind modernste elektronische Optiken eingebaut. Mit diesen Kameras werden Bilder im sichtbaren, sowie im infraroten Frequenzspektrum aufgenommen. Durch das eingebaute Radarsystem können zu jeder Tageszeit und bei jeden Wetterbedingung bewegliche Ziele, wie Bodenfahrzeuge, ausgemacht werden. Die Heimatbasis erhält diese Daten dann in Echtzeit durch eine Funkverbindung oder Satellitenübertragung.

Dieses erfolgreiche System wird in Kooperation mit der EADS für europäische Zwecke unter dem Namen „Euro Hawk“ weiterentwickelt und soll die europäische Aufklärungskomponente erweitern und verbessern. All diesen Vorteilen stehen auch noch technische Schwierigkeiten und steigende Systemkosten gegenüber. Von sieben Prototypen sind drei abgestürzt. Der veranschlagte Preis für eine „Global Hawk“ stieg von 15 auf 70 Millionen Dollar. Im Rahmen der schon angelaufen Serienfertigung, werden Produktqualität und der Systempreis deutlich gesenkt.[17]

2.4.2 Die Infanterie der Zukunft

Die Bundeswehr verfolgt seit Anfang der neunziger Jahre ein Programm zur Modernisierung der Ausrüstung ihrer Infanterie. Seit dem Jahr 2004 werden erste Komponenten der Ausrüstung an die Truppe ausgegeben.
Mit diesem Programm wird der Zweck verfolgt, Soldaten im Einsatz umfassend und mit bestmöglicher Ausrüstung auszustatten. Da im überwiegenden Fall die bisherige Ausrüstung nicht aufeinander abgestimmt war, wurden neue Lösungsmöglichkeiten für einen integrierten Systemansatz verfolgt. Im Vordergrund steht Kommunikation, Orientierung und Bewaffnung.

Im Mittelpunkt steht eine zehn Mann starke Infanteriegruppe. Jeder dieser Soldaten erhält Teile der aus ca. 20 Komponenten bestehenden Ausrüstung. Im Bereich der Kleidung und Schutzausstattung gibt es einen einheitlichen Standard. Die einzelnen Komponenten der Ausstattung werden auf die Gruppe verteilt. Die Ausrüstung die gerade nicht benötigt wird, verbleibt auf dem Gefechtsfahrzeug. Durch bewährte Komponenten die auf dem freien Markt zu kaufen sind und durch Neuentwicklungen, konnte eine flexible und modulare Ausrüstung erstellt werden. Ein großer Vorteil ist auch die Gewichtsreduzierung der Ausrüstung von ca. 47 kg auf 30 kg, je Soldat.
Für jede Klimasituation wird die Kleidung, von der Funktionsunterwäsche bis zum Kampfstiefel, angepasst. Im Folgenden wird aber das Augenmerk auf die technischen Komponenten gelegt.

Eine Revolution stellt die Elektronikausrüstung dar, sämtliche elektronische Gegenstände werden entweder an oder in der Trageweste getragen. Im Rücken der Weste befindet sich ein UHF-Funkgerät, auf der Brust ist ein „Personal Data Assistand“ angebracht. Mit ihm kann die eigene Position ermittelt werden und auch die der Kameraden, um Verluste durch „friendly fire“ zu minimieren. Ebenso dürfen ein digitaler Kompass integriert in einem Messfernglas und ein

[17] Lange, S. (2003), http://www.swp-berlin.org/common/get_document.php?id=865.

Headset nicht fehlen. Mit dem Informationssystem „Faust“ wird das Zusammenspiel der verbundenen Waffen verbessert. Zu den weiteren Ausrüstungsgegenständen gehören noch eine Restlichtverstärkerbrille, Restlichtverstärkerrohr sowie ein Wärmebildzielgerät. Diese können einzeln oder auch in Verbindung mit den Handfeuerwaffen genutzt werden. Aber auch hier gibt es Neuerungen, wie eine Nahbereichsverteidigungswaffe MP 7 oder mögliche Zusatzausstattungen für das deutsche Standardgewehr G36 z.B. mit einem Laserlichtmodul oder ein Abschussgerät für Granatpatronen.[18] Die Drohne Aladin, die eine Flügelspannweite von nur 42 cm misst, gehört ebenso zur zukünftigen Ausrüstung. Sie wurde schon erfolgreich in Afghanistan durch deutsche Truppen getestet.[19]

Da das Programm „Infanterist der Zukunft“ modular aufgebaut ist, werden ständig Neuerungen in das System integriert, die vor allem den technischen, sowie waffentechnischen Bereich beinhalten. Somit schwanken die Kosten für eine Infanteriegruppe von zehn Mann zwischen 250.000 bis 270.000 Euro. Mit dem neuen Ausrüstungskonzept schafft die Bundeswehr die Möglichkeit schon in den heutigen Einsätzen den Infanteristen mit modernster Technik auszustatten. Dies ermöglicht ihm seine Überlebens-, sowie Durchhaltefähigkeit entscheidend zu erhöhen. Aber es ist darauf zu achten, dass man keiner Technikgläubigkeit verfällt, da die Nutzung moderne Technologien auch immer eine gewisse Fehler- und Ausfallanfälligkeit besitzt, die unter Umständen das Leben des Soldaten kosten kann.

2.4 Fazit

Die großen Schlachten mit Hunderttausenden von Soldaten sind vorbei. In der Zukunft werden Kriege lokal und zeitlich begrenzt geführt. In diesen Einsätzen werden die neuesten Waffen- und Aufklärungssysteme in Verbindung mit Soldaten, deren Ausrüstung einen hohen technischen Standard aufzeigen, eingesetzt. Ebenfalls problematisch ist die Situation, dass man in diesen neuen Konflikten zunehmend auf Kräfte trifft, die sich der asymmetrischen Kriegsführung bedienen. Hier kämpft ein Gegner, der sich nicht an internationales Kriegsrecht hält, sondern die zivilisierte Welt dort treffen will, wo sie am meisten verwundbar ist und das zu jeder Zeit und an jedem Ort. Unsere hochkomplexe und technisierte Infrastruktur bietet daher ein hochinteressantes und vor allem ein lohnendes Ziel für Angriffe und Anschläge dieser Kräfte.
Damit sind Gegenmaßnahmen konventioneller Art mit Panzer- und Infanteriedivisionen nur von begrenztem Nutzen, da man regulären Truppen nur noch selten, und dann höchstens am Anfang

[18] Vgl. Bocklet, W. (2004), http://www.soldat-und-technik.de/08-2004/idz.pdf.
[19] Vgl. Weckbach-Mara, F. (2003), http://www.wams.de/data/2003/06/22/122831.html?prx=1.

von Kampfhandlungen, gegenüber steht. Mit dieser Problematik sehen sich auch die alliierten Truppen in Afghanistan und im Irak konfrontiert. Nachdem der reguläre Gegner besiegt und die Kampfhandlungen für offiziell beendet erklärt wurden, war der Krieg dennoch nicht zu Ende. Noch heute kämpft man gegen irakische Aufständische und Einheiten der afghanischen Taliban mehr oder minder erfolgreich.

Als Schlussfolgerung ziehen hier die westlichen Staaten, dass mehr in militärische Zukunftstechnologien investiert werden muss. Konflikte frühzeitig zu beenden und das möglichst ohne eigene menschliche Verluste ist das Hauptziel. Inwieweit die Waffen- und Informationsüberlegenheit des Westens und vor allem der Vereinigten Staaten von Amerika zu einem Absinken der Hemmschwelle für kriegerische Konfliktlösungen führt, wird die Zukunft zeigen.

3. Spionage

Der französische Philosoph Francis Bacon (1561-1621) sagte einmal „Wissen ist Macht“. Mit der Bedeutung dieser Aussage kann das Tätigkeitsfeld von Geheimdiensten seit der Antike umschrieben werden. [20]

Spionage im weiten Sinne ist die Beschaffung von Informationen und Daten aus Quellen anderer Nationen, Organisationen oder Unternehmen. Es wird auch von dem zweitältesten Gewerbe der Welt gesprochen. In jeder Regierungsform, ob demokratisch oder diktatorisch geprägt, wird Spionage betrieben. Zu Zeiten des „Kalten Krieges“ war das Wissen der potentiellen Gegner jenseits des „Eisernen Vorhangs“ von großem Interesse. Vor allem benötigten die jeweiligen Geheimdienste Informationen über technologische Entwicklungen und den Stand der Nukleartechnologie der gegnerischen Seite.
Heutzutage hat sich der Aufgabenbereich der Geheimdienste auf ein weiteres Feld fokussiert. Mit dem Ausspionieren von Wirtschaftsgeheimnissen durch staatliche Nachrichtendienste und Konkurrenzunternehmen, wird der Versuch unternommen, die eigene Wirtschaft zu stärken und fremde Technologievorsprünge in die eigene Wirtschaftsstruktur schnell und günstig zu integrieren.[21]

[20] Vgl. Krieger, W. (2003), S. 7.
[21] Vgl. o.V. (2004), http://de.wikipedia.org/wiki/Spionage.

Durch Wirtschaftsspionage in Deutschland entsteht laut einer Studie der Universität Lüneburg ein Schaden von ca. 50 Mrd. Euro pro Jahr. Professor Egbert Kahle, Autor der Studie verdeutlichte, dass besonders kleine und innovative Unternehmen von diesem Problem betroffen sind. Gerade diese Unternehmen sind durch innovative Produkte und zukunftsweisende Kleinserienfertigungen stark gefährdet.
Laut Professor Kahle geht die größte Gefahr von den eigenen Mitarbeitern, Konkurrenzunternehmen und Kooperationspartnern aus. In vielen Unternehmen gibt es beispielsweise keine Vorstellung über die Verwundbarkeit des eigenen EDV-Systems. Der unkontrollierte Wissensabfluss durch ein nicht vorhandenes Wissenserfassungssystem oder durch nachrichtendienstliche Aktivitäten kann nur mit firmeninternen Sicherheitsbeauftragten oder Sicherheitsapparaten präventiv verhindert werden.
Zwei Drittel der an der Studie beteiligten Unternehmen waren schon einmal das Opfer von Spionagetätigkeiten. Somit lauten die Schlussfolgerungen für dieses Problemfeld, dass mehr finanzielle Mittel für Sicherheitsvorkehrungen aufgewendet werden müssen und das der Kampf gegen Wirtschaftsspionage als Managementaufgabe verstanden werden muss.[22]

3.1 Nachrichtendienste in Deutschland

In der Bundesrepublik Deutschland gibt es drei Nachrichtendienste. Dies sind der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und der Militärischer Abschirmdienst.
Alle drei Organisationen sind Teil der Staats- und Rechtsordnung der Bundesrepublik Deutschland und unterstützen sich gegenseitig durch ihre aufsichtsführenden Behörden. Informationsbeschaffung und Auswertung sind ein gemeinsames Bindeglied aller drei Organisationen. Im folgenden soll lediglich auf den Bundesnachrichtendienst eingegangen werden, da er die klassischen nachrichtendienstlichen Tätigkeiten durchführt.

3.1.1 Bundesnachrichtendienst

Der BND wurde auf Weisung der Bundesregierung am 1. April 1956 gegründet. Sein Sitz ist in Pullach. Fach- und Dienstaufsicht erfolgt durch das Bundeskanzleramt. Eine Kontrolle der Tätigkeiten wird z.B. durch das Parlament, den Bundesrechnungshof oder durch den Bundesbeauftragten für Datenschutz gewährleistet.

[22] Vgl. o.V. (2004), http://www.n24.de/wirtschaft/wirtschaftspolitik/index.php/a2004101314345731686.

Mit dem BND als einzigen Auslandsnachrichtendienst betreibt die Bundesrepublik Deutschland zivile und militärische Auslandsaufklärung. Inlandsaufklärung bleibt ihm untersagt. Informationserfassungstätigkeiten über das Ausland können dennoch auch im Inland erfolgen. Ebenso besitzt der Bundesnachrichtendienst keine polizeilichen Exekutivbefugnisse. Mit geheimgehaltenen Informationen, die nur mit spezifischen nachrichtendienstlichen Möglichkeiten gewonnen werden können, unterstützt der Bundesnachrichtendienst den Informationsbedarf der Bundesregierung. Hierzu zählen beispielsweise Kenntnisse über illegale Migration, organisierte Kriminalität, internationaler Terrorismus und die Gefahren des Information Warfare.
Um die zugewiesenen Aufgaben erfüllen zu können, bedient sich der BND vier verschiedener Methoden:

HUMINT - Human Intelligence:
Die Gewinnung von geheimen Informationen durch Unterstützung menschlicher Quellen fällt in diesen Bereich. Auch im Zeitalter moderner Aufklärungstechniken, stellt diese Aufklärungsvariante mit Spionen die klassische Form der Informationsbeschaffung dar. Human Intelligence wird auch unter dem Begriff „operative Aufklärung“ geführt. Er stellt die klassische Spionagearbeit mit menschlichen Kundschaftern dar. Gesprächsaufklärung durch eigene Mitarbeiter im Ausland und angeworbene Agenten ist nur ein Teil dieses großen Bereiches.

SIGINT - Signal Intelligence:
Mit Hilfe von technischen Mitteln werden Informationen aus internationalen Kommunikationsströmen herausgefiltert. Hierzu sind in ganz Deutschland Abhörstationen installiert, mit denen der Kommunikationsverkehr abgehört werden kann.

IMINT - Imagery Intelligence:
Dieser Bereich befasst sich mit der Erfassung und Auswertung von Satellitenbildern. Also mit der Reproduktion von Zielobjekten, die beispielsweise durch elektronische oder optische Mittel erzeugt werden. Im Zuge des technologischen Fortschritts unterliegt dieser Bereich einer ständigen Verbesserung und Weiterentwicklung. Wurde am Anfang des Letzten Jahrhunderts noch fotooptische Aufklärung betrieben, so ist heute eine Aufklärung über optronische Sensoren Standard. Sie erlauben eine zeit- und wetterunabhängige Aufklärung der gesamten Erdoberfläche.[23]

[23] Vgl. Lux, C./Peske T. (2002), S. 91.

OSINT - Open Source Intelligence:

Anders ausgedrückt ist mit Open Source Intelligence auch offene Informationsgewinnung gemeint. Zu ihr zählen die Beschaffung von Daten aus frei verfügbaren Informationsquellen, wie Printmedien oder Fernsehübertragungen. Durch diese Informationen können wertvolle Grundlageninformationen, die das Lagebild vervollständigen, beschafft werden. Es ist hinzuzufügen, dass mit OSINT eine preiswerte und gefahrlose Aufklärungsvariante zur Verfügung steht, mit der weltweit Informationen abgeschöpft werden können.

3.2 Wirtschaftsspionage

Wie oben schon beschrieben, nimmt die Wirtschaftsspionage einen breiten Raum im Spionagegeschäft ein. Mit dieser Art der Informationsgewinnung beschäftigen sich Konkurrenten und staatliche Nachrichtendienste. Sie gliedert sich in Konkurrenz- und nachrichtendienstlich geführte Spionage auf.

3.2.1 Konkurrenzspionage

Der Bereich der Konkurrenzspionage ist vielschichtig, da sich Spionageaktivitäten nicht nur auf direkte Mitbewerber der Unternehmen bezieht, sondern vielmehr auf das gesamte Wettbewerbsumfeld. Hierzu zählen auch Lieferanten und Abnehmer des eigenen Unternehmens. Hier steht die Spionage durch private Organisationen im Vordergrund.[24] Die Hintergründe für diese Art der Informationsbeschaffung sind mannigfaltig. Sie reichen von der Gewinnung von Kenntnissen über neue Produktionstechnologien und Produktionsabläufen, bis hin zu Informationen, die für eine Übernahme durch Mitbewerber entscheidend sind. Erschwerend kommt hinzu, das weder feste Strukturen noch Organisationen offen als Akteure in Erscheinung treten.

Als wichtiger Unsicherheitsfaktor für den Informationsabfluss aus einem Unternehmen, gelten die eigenen Mitarbeiter, externes Personal von Reinigungs- und Wartungsunternehmen, sowie Unternehmensberatungen.[25]

Diesen Angriffen sieht sich jedes Unternehmen potentiell ausgesetzt. Verschiedene Methoden sind für eine Informationserlangung hilfreich. Mit der Offenen Beschaffung durch frei zugängliche Fachliteratur, Werbeprospekten und Vorträgen und deren systematische Auswertung

[24] Vgl. Lux, C./Peske T. (2002), S. 30.
[25] Vgl. Lux, C./Peske T. (2002), S. 50.

ist es möglich, eine legale Informationsbasis zu schaffen. Weiterhin eignet sich zur Informationsgewinnung, die Überwachung von Post-, Daten- und Telefonverkehr des interessanten Unternehmens.
Mit Fachgesprächen bei Kongressen und Tagungen, ist es ebenso möglich wichtige Informationen von Mitbewerbern zu erlangen.[26]

3.2.2 Nachrichtendienstlich geführte Spionage

Aus dem allgemeinen Verständnis heraus wird diese Art der Spionage durch staatliche Organisationen betrieben. Im Vordergrund stehen hier die staatlichen Nachrichtendienste der einzelnen Nationalstaaten, sowie temporär angeworbene Privatpersonen und auch Staatsdiener, die in verschiedenen Botschaften ihren Dienst versehen.
Um die Frage zu beantworten, inwieweit Deutschland Wirtschaftsspionage durch eigene Nachrichtendienste betreibt, kann nur spekuliert werden. Von offizieller Seite gibt es Aussagen, die eine Wirtschaftsspionage durch eine fehlende rechtliche Legitimation verhindert. Auch in der Fachliteratur geht man davon aus, dass Anschuldigungen über deutsche Wirtschaftsspionage nur das Ziel der Verbreitung von Fehlinformationen hat.

Im Gegensatz zu Deutschland, betreibt die NSA als Inlandsnachrichtendienst der USA gezielte Wirtschaftsspionage. Als eine Grundlage hierfür gilt die „Anweisung zur Nationensicherheit NSD-67 Intelligence Capabilities 1992-2005“ von dem ehemaligen amerikanischen Präsidenten George Bush aus dem Jahre 1992. Als ein wichtiges Hilfsmittel zur Erreichung dieses amerikanischen Zieles, gehört ECHELON. Es ist ein weltweites Überwachungsnetzwerk, das eine 100% Abhörbarkeit der weltweiten Kommunikation zum Ziel hat. Schon 1992 konnten laut Aussage eines ehemaligen NSA Direktors pro Stunde zwei Millionen Nachrichten abgefangen werden.[27]Neben den USA beteiligen sich an diesem System auch Groß Britannien, Kanada, Neuseeland, Australien, sowie einige drittbeteiligte Länder, die aber nur eingeschränkt Informationen erhalten und somit keine vollständige Analyse und Auswertung der Daten vornehmen können.[28] Auf eine genaue technische Erklärung von ECHELON soll hier verzichtet werden, da dies den vorhanden Rahmen sprengen würde.

[26] Vgl. o.V., http://www.kdm-portal.com/sp_heute.html.
[27] Vgl. Raven, K., http://kai.iks-jena.de/miniwahr/echelon1.html.
[28] Vgl. Becker, K. u.a. (2003), http://www.bpb.de/publikationen/U3P11A,0,0,5_4_Echelon.html#art0.

3.3 Fazit

Wie schon in der Einleitung beschrieben, ist Spionage in all ihren Variationen keine neue Erscheinung. Durch den ständigen technologischen Fortschritt ist eine Informationsgewinnung durch Spionage schneller und effizienter möglich. Als großes Problem stellt sich die Verlagerung der Aktivitäten einiger staatlichen Nachrichtendienste auf den Bereich der Wirtschaftsspionage dar. Die Nutzung dieser Technologien zur Abwendung von Bedrohungen, beispielsweise durch den internationalen Terrorismus und die Gefahren der organisierten Kriminalität, ist wünschenswert und nachvollziehbar. Leider sind die Systeme der Überwachung auch ohne Probleme zum Ausspionieren der eigenen Bevölkerung und befreundeter Staaten geeignet. Gerade das Verhalten der Vereinigten Staaten von Amerika zeigt uns, dass auch befreundete Staaten in den Fokus der US-amerikanischen Geheimdienste geraten. Hier muss auf internationaler Ebene eine befriedigende Lösung gefunden werden, da solche Konfliktpotentiale sehr ernst genommen werden müssen.

Für den einzelnen Bürger und Wirtschaftsunternehmen bedeutet dies eine zunehmende Verunsicherung und Bedrohung. Inwieweit die eigene Kommunikation per Telefon oder E-Mail abgehört oder das eigene Unternehmen ausspioniert wird, ist nicht nachvollziehbar. Eine weltweite Sensibilisierung der Bevölkerung für dieses Bedrohungsszenario muss eine sinnvolle Konsequenz sein.

4. Datenschutz

Der Bereich des Datensatzes ist vielfältig und kaum überschaubar. Ein Wirkungszusammenhang zwischen Spionage, der Gewinnung der Informationsüberlegenheit im Rahmen des Informationskrieges und dem Bereich des Datenschutzes ist zu erkennen. Die Verschaffung von Vorteilen durch Erlangung von Informationen, beinhaltet in beiden Bereichen potentielle Verletzungen von Datenschutzrechten des Einzelnen oder von Unternehmen.

Im Allgemeinen umfasst der Datenschutz Rechte, die es dem einzelnen Bürger ermöglichen, seine personenbezogenen Daten vor Dritten zu schützen. Dieses Recht auf informationelle Selbstbestimmung gilt für die Bundesrepublik Deutschland seit dem 15. Dezember 1983. An diesem Tag entschied das Bundesverfassungsgericht im sogenannten „Volkszählungsurteil“, dass die informationelle Selbstbestimmung als ein Teil der Persönlichkeitsrechte und der Menschenwürde zu gelten hat. Auslöser für das Urteil war eine für 1983 angestrebte

Volkszählung die eine zusätzliche Datenerhebung für statistische Zwecke beinhalten sollte. Aufggrund einer Verfassungsbeschwerde und der darauffolgenden mündlichen Verhandlung wurde dieses Urteil erlassen.[29]

In der Bundesrepublik Deutschland wird das Datenschutzrecht in allgemeinen Datenschutzgesetzen des Bundes, der Länder und in Sondergesetzen geregelt. So gilt, dass die Artikel 1 Abs.1 GG und Artikel 2 Abs. 1 GG, die das allgemeine Recht auf Unantastbarkeit der Menschenwürde und das Recht auf freie Persönlichkeitsentfaltung beinhalten, als Grundlage für geltende Datenschutzgesetze gesehen werden können. Die Neufassung des Bundesdatenschutzgesetzes vom 14. Januar 2003 ist nur ein Gesetz auf Bundesebene. In ihr sind Richtlinien niedergeschrieben, die den Umgang mit personenbezogenen Daten des Einzelnen regeln.[30]
Weitere Gesetze, wie das Teledienstdatenschutzgesetz oder die Telekommunikations-Überwachungsverordnung regeln den Umgang und Zugriff auf personenbezogene Daten im Bereich der Telekommunikationswirtschaft.

Im Folgenden sollen nun Probleme im Spannungsfeld des Datenschutzes aufgezeigt werden, mit denen der Bürger tagtäglich in Berührung kommen kann.

4.1 Big Brother Awards

Eingriffe in die Privatsphäre und Datenschutzverletzungen der Bürger sind kein deutsches Phänomen. Aufgrund dieser Problematik haben sich in weltweit 16 Länder Interessengruppen zusammengeschlossen, die jährlich nationale Big Brother Awards verleihen.
In der Bundesrepublik Deutschland versteht sich Big Brother Awards.de als Diskussionsforum, um mißbräulichen Umgang mit Technik und Informationen darzustellen. So sollen Eingriffe in die Privatsphäre und den Datenschutz in das öffentliche Bewusstsein gerückt werden.
Als Schirmherr der Awards organisieren die Mitglieder der FoeBuD e. V. seit dem Jahre 2000 die jährliche Verleihung an Organisationen, Unternehmen und Personen in unterschiedlichen Kategorien, die im hohen Maße die Privatsphäre verletzt oder persönliche Daten an Dritte weitergegeben haben.[31]

[29] Vgl. o.V. (2004), http://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil.
[30] Vgl. o.V., (2003), http://www.datenschutz-portal.de/Dokumente/Neufassung%20des%20Bundesdatenschutzgesetzes.doc.
[31] Vgl. o.V. (2004), http://www.bigbrotherawards.de/.

4.1.1 Kategorie Wirtschaft und Verbraucherschutz

Für das Jahr 2004 erhält die Tchibo direct GmbH in der oben genannten Kategorie eine Big Brother Award. Grund der Verleihung war die Weitergabe ihrer Kundendaten an die Vermarktungsfirma Arvato / AZ Direct.

Als problematisch stellt sich hier der Anspruch und die Wirklichkeit des Datenschutzesgedankens dar. Auf Prospekt- und Internetseiten, wird der vertrauliche Umgang mit Adressen der Kunden betont. Im Internetportal des Unternehmens wird die Weitergabe von persönlichen Daten an Dritte sogar grundsätzlich ausgeschlossen. In der Realität bietet Tchibo direct GmbH in Zusammenarbeit mit der Vermarktungsfirma Arvato / AZ Direct die Adressen auf dem Adressmarkt an.

Aber was passiert mit den persönlichen Daten? Käufer der Adressen sollen umfassende Informationen über die potentiellen Kunden bekommen. Hierzu gehören neben demografischen und geografischen Angaben auch die Neigung im Versandhandel einzukaufen oder die Höhe der Kaufkraft der betroffenen Personen zu erhalten.[32]

Anhand dieses Beispiels sieht man, dass nicht nur Adressen, sondern auch umfassende persönliche Daten weitergegeben werden. Mit diesen Informationen ist es dann möglich ein umfassendes Kundenprofil zu erstellen und maßgeschneiderte Angebote dem Kunden zukommen zu lassen. Abgesehen von der Datenschutzverletzung entsteht hier ein weiteres Problem. Durch eine mögliche Zunahme dieser Geschäftspraktiken wird dem Kunden die Wahlmöglichkeit beim Produktkauf erschwert, da er oft nicht weiß, dass ihm ein solches individuelles und eingeschränktes Angebot unterbreitet wird. Wenn nur noch maßgeschneiderte Lösungen seitens der Unternehmen angeboten werden, ist es nicht mehr möglich sich frei zu informieren und zu entscheiden.

4.1.2 Kategorie Technik

Die Canon Deutschland GmbH ist der Preisträger des Big Brother Awards 2004 in der Kategorie Technik. Zum Gewinn verhalf ihr das Einbetten von Gerätekennungen in Kopiergeräte. Auf jeder Farbkopie die mit einem Canon Kopierer erstellt wird, ist eine unsichtbare Seriennummer

[32] Vgl. Freude, A. (2004), http://www.bigbrotherawards.de/2004/.com/.

des Kopierers enthalten. Seit Jahren nutzt Canon diese Technik, doch erst jetzt konnte bewiesen werden, dass diese tatsächlich existiert und angewendet wird. Ein großes Problem tritt hier zu Tage. Käufer und Kunden der Kopiergeräte erhalten keinen Hinweis auf diese implementierte Technik. Ohne technische Hilfsmittel ist es ebenfalls nicht möglich die Kennung auf den Kopien sichtbar zu machen.

Generell erscheint dieses Verfahren für eine Strafverfolgung als gerechtfertigt. So könnte beispielsweise zweifelsfrei der Copy-Shop, der gefälschte Ausweise und Banknoten herstellt, ermittelt werden. Ganz anders verhält sich aber mit Kopien, die für die Aufklärung beispielsweise von Bestechungsskandalen erstellt werden. Hier ist die Frage wer noch eine Kopie an die Presse weiterreicht, wenn ihre Anonymität nicht mehr gewährleistet ist. Denn durch die Seriennummer auf den Kopien ist eine Rückverfolgung, beispielsweise durch den Arbeitgeber, möglich. Copy-Shop Mitarbeiter bestätigen, dass dies keine Utopie ist, da in der Vergangenheit konkrete Anfragen von Ermittlungsbehörden stattfanden.[33]

Es zeigt sich inwieweit heute die Informationsfreiheit eingeschränkt werden kann. Das Beispiel von Canon ist nur ein Fall unserer Technikabhängigkeit. In zunehmendem Maße erlaubt die moderne Technik dem Nutzer der Selbigen zu beschränken. Es beginnt mit der technischen Einschränkung Banknoten auf bestimmten Geräten zu kopieren oder zu drucken und endet womöglich mit der für den Einzelnen individuellen Einschränkung Drucker, Kopierer oder Scanner in ihrer gesamten Funktion nutzen zu können.

4.1.3 Kategorie Gesundheit und Soziales

In dieser Kategorie erhält die Bundesministerin für Gesundheit und soziale Sicherung Frau Ulla Schmidt einen Big Brother Award. Grund der Auszeichnung war das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung, dass am 01.Januar 2004 in Kraft trat.
Mit diesem Gesetz wurde die versichertenbezogene Datenverarbeitung verstärkt und somit ein für den Patienten verschlechterter Datenschutz in Kauf genommen. In der Praxis wurden vor der Modernisierung des Gesetzes Abrechnungen von Krankheitskosten anonym und fallbezogen durchgeführt. Seit 2004 erhalten Krankenkassen neben den Abrechnungen für Patienten auch deren Behandlungen. Somit ist es den Krankenkassen möglich ein lückenloses Krankheitsprofil von jedem versicherten Mitglied zu erstellen.

[33] Vgl. Rosengart, F. (2004), http://www.bigbrotherawards.de/2004/.tec/.

Datenschutzbeauftragte warnten im September 2003 vor den Risiken der Gesetzesmodernisierung. Mit der Übermittelung von Abrechnungen der ambulanten Behandlung und versichertenbezogener Diagnosen erhalten Krankenkassen umfassende und intime Kenntnisse ihrer Mitglieder. Für das deutsche Krankenversicherungssystem bedeutet dies, dass datenschutzbedenkliche Kenntnisse von 60 Millionen Versicherten gesammelt werden können. Weiterhin wurde darauf hingewiesen, dass strenge Zweckbindungsregeln für die Daten erstellt werden müssen, ansonsten kann es für Patienten zu negativen Auswirkungen kommen. Eine Konsequenz könnte so aussehen, dass für die Krankenkassen teure Patienten nicht mehr versichert, Zahlungen verzögert oder gar mehr nicht geleistet werden.

Als ernüchternd sehen es Datenschützer auch, dass datenschutzfreundliche Technik einschließlich der Pseudonymisierung erst gar nicht berücksichtigt wurden. Somit wird der gläserne Patient ihrer Meinung nach immer wahrscheinlicher.

Ein Ausblick gibt Big Brother Awards.de für das Jahr 2005, denn mit der Einführung der elektronischen Gesundheitskarte für das Jahr 2006 bahnen sich weitere Datenschutzverletzungen an. Es ist bisher noch nicht geklärt wurden, wer auf welche Daten der Gesundheitskarte Zugriff besitzt. Dies erscheint als ein sehr schwerwiegendes Problem, da Gesundheitsdaten auf der Karte gespeichert sind.[34]

An diesem Beispiel zeigt es sich, welche Interessengruppen im Blickpunkt der Gesetzesmodernisierung standen. Wenn es die Gruppe der Versicherten gewesen wären, hätte die Bundesrepublik Deutschland heute ein System, mit dem nicht die Möglichkeit besteht würde sensible und intime Daten sammeln zu können. In welcher Weise eine Datensammlung und Datenauswertung erfolgt, kann nur spekuliert werden. Trotz des zunehmenden Kostendruck der Krankenkassen ist zu hoffen, dass eine verantwortungsvolle Behandlung von Patientendaten stattfindet. Inwieweit dies aber wirklich geschieht, wird die Zukunft zeigen.

[34] Vgl. Hülsmann, W. (2004), http://www.bigbrotherawards.de/2004/.soc/.

4.2 Datenschutzfreundliche Technologien

Da erhebliche Probleme mit Datenschutzverletzungen bestehen, könnte der Eindruck erweckt werden, dass Bürger, Unternehmen und andere Organisationen dieser Gefahr wehrlos ausgesetzt sind. Es bestehen dennoch Möglichkeiten mit Hilfe moderner Technologien, beispielsweise durch Anonymisierung und Pseudonymisierung, diesem Problem entgegenzuwirken.

4.2.1 Anonymisierung

Anonymisieren ist das Verändern personenbezogenen Daten, so das Einzelangaben die Auskünfte über sachliche und persönliche Verhältnisse beinhalten, keiner bestimmten Person mehr zugeordnet werden können oder nur mit großem Einsatz von Zeit und Kosten. Der Grad der Anonymisierung wir in den Datenschutzgesetzen des Bundes und der Länder unterschiedlich gesehen. Nach dem Bundesdatenschutzgesetz werden auch Verfahren zugelassen, die den Inhalt der oben aufgeführten Aussage wiederspiegelt.[35] Dagegen lassen die Landesdatenschutzgesetze der Länder Mecklenburg Vorpommern, Sachsen und Schleswig Holstein nur solche Verfahren als Anonymisierung zu, die keinen Rückschluss von Sachverhalten auf einzelne Personen zulassen.

Verschiedene Einflussfaktoren bestimmen die Qualität der Anonymisierungsprozedur. Maßgeblich ist hier beispielsweise der Zeitpunkt der Anonymisierung, Rücknahmefestigkeit der Anonymisierung und die Mächtigkeit der Menge und Verkettungsmöglichkeiten einzelner Transaktionen. Mit Einzelangaben innerhalb eines Datensatzes wird ebenfalls die Qualität der Anonymisierung bestimmt. Hier müssen deshalb anonymitätsgefährdende Werte innerhalb der Menge zusammengefasst werden. [36]

4.2.2 Pseudonymisierung

Eine ebenfalls interessante Verfahrensweise zum Schutz von Daten ist die Pseudonymisierung. Sie wird angewendet, wenn eine Anonymisierung nicht möglich ist. Ziel ist es hier, mittels einer Zuordnungsvorschrift personengebundene Daten so zu verändern, dass ohne die Zuordnungsvorschrift kein Rückschluss der Daten auf die natürliche Person stattfinden kann.

[35] Vgl. Ernestus, W (1999), S. 253.
[36] Vgl. Ernestus, W u.a. (1997), http://www.lfd.m-v.de/informat/dsftechn/apdsftec.pdf.

Nun werden die Identifikationsdaten mittels einer Abbildungsvorschrift in ein gewähltes Kennzeichen überführt. Jetzt ist es möglich, dass ein Personenbezug nur dann hergestellt werden kann, wenn bestimmte Rahmenbedingungen gewährleistet sind. Es besteht ebenso die Möglichkeit, dass nur die betroffene Person selber eine Reinidentifikation durchführen kann.

Mehrere Einflussfaktoren bestimmen auch hier die Qualität des Verfahrens. Sie entsprechen denen der Anonymisierung. Weiterhin ist eine Speicherung und Verkettung von Datensätze unter dem selben Pseudonym möglich. Es ist ebenfalls darauf hinzuweisen, dass die Anonymisierung unter gleichen Bedingungen eine datenschutzfreundlicherer Variante darstellt, da die Herstellung eines Personenbezugs nicht möglich ist.

Aufgrund der Verknüpfbarkeit des Pseudonyms des Inhabers kann die Herstellung des Personenbezugs auf drei Weisen geschehen. Mit selbstgenerierten Pseudonymen ist nur der Betroffene selbst in der Lage, den Personenbezug wiederherzustellen. Durch Referenz-Pseudonyme gewährleistet man eine Wiederherstellung nur mit entsprechenden Referenzlisten. Mit dieser Variante ist eine Herstellung des Personenbezug in Ausnahmefällen möglich, beispielsweise bei fehlerhaften Zahlungsvorgängen. Als letzte Variante verwendet man Einweg-Pseudonyme. Aus den personenbezogenen Daten werden mittels asymmetrischer Verschlüsselung Einweg-Pseudonyme erstellt.[37] Hier kann nun festgestellt werden, dass nicht die Referenzliste den Zusammenhang zwischen Pseudonym und Identitätsdaten bildet, sondern die Bildungsvorschrift. Eine praktische Anwendung erfährt die Pseudonymisierung bei Auskunftssystemen.[38]

4.3 Fazit

Aus diesen zwei datenschutzfreundlichen Technologien ist ersichtlich, dass Datenschutz nicht an der Nichtverfügbarkeit von Technologien scheitert, sondern am mangelnden Interesse diese einzusetzen. Eine spürbare Verbesserung im Bereich des Datenschutzes für den Einzelnen ist nur dann möglich, wenn die breite Öffentlichkeit ein Interesse entwickelt, was mit ihren persönlichen Daten passiert. Nur dann kann genügend Druck von unten geschaffen werden, der eine Verbesserung in diesem Bereich bewirkt. Es darf auch nicht vergessen werden, dass in den

[37] Vgl. Bayrische Landesbeauftragte für Datenschutz (2004), http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm#Pseudonymisierung.
[38] Vgl. Ernestus, W (1999), S. 255.

sammelungswütigen Unternehmen und Organisationen auch nur Menschen arbeiten, die dann im schlimmsten Fall ihre eigenen Datenschutzrechte verletzen.

5. Gesamtfazit

Mit dieser Arbeit wollte ich zeigen welche Möglichkeiten es gibt, die Errungenschaften moderner Technologien in verschieden Bereichen des heutigen Lebens einzusetzen. Im Rahmen des militärischen Sektors zeigt sich besonders gut, mit welchen Aufklärungs- und Waffensystemen heutige und zukünftige Kriege geführt werden können. Daneben ist hervorzuheben, dass sich aufgrund der hohen Anschaffungs- und Wartungskosten, technologisch hochwertige Waffensysteme nicht alle Staaten leisten können. Die Vereinigten Staaten von Amerika unternehmen immense Anstrengungen, um ihre Technologieüberlegenheit gegenüber dem Rest der Welt zu erhalten. Hier stellt sich dem interessierten Leser die Frage, ob die letzte verbliebene Weltmacht in der Zukunft ihre Probleme eher mit politischen oder militärischen Mitteln lösen wird. Es besteht die Möglichkeit, dass die Hemmschwelle für einen Waffengang aufgrund keiner ebenbürtiger Gegner sinken kann. Hier ist zu hoffen, dass sich die USA ihrer Verantwortung in der Welt wieder bewusst wird und verantwortungsvoll mit ihrem militärischen Potential umgeht.

Aber auch im Abschnitt der Spionage wurde aufgezeigt, mit welchen Absichten heutzutage staatliche und nicht staatliche Spionage betrieben wird. War zu Zeiten des Kalten Krieges der Gegner noch im anderen ideologischen Lager zu finden, verschieben sich heute Spionagetätigkeiten auf befreundete und verbündete Nationen. Anders ist es auch nicht zu erklären, dass in vielen Staaten Wirtschaftsspionage einen bedeutenden Stellenwert inne hat. Hier muss wieder die USA genannt werden, die mit all ihren zur Verfügung stehenden Technologien neben der zu akzeptierenden Terrorismus- und Kriminalitätsbekämpfung, ihre Mittel auch bewusst für Wirtschaftspionage einsetzen.

Im Bereich des Datenschutzes schließt sich der Kreis. Denn man sieht, dass mit der fortschreitenden technologischen Entwicklung, personengebundene Daten leichter gesammelt und interessengeleitet gegen den Besitzer eingesetzt werden kann. Ebenfalls ist eine starke Verbindung zwischen den drei Bereichen zu erkennen. Mit Satteliten und Abhörstationen am Boden können militärische Gegner überwacht werden. Ebenso einfach ist es mit genau diesen Anlagen, die eigene Bevölkerung oder Bürger andere Nationen zu überwachen und auszuspionieren.

Inwieweit aus dem technologischen Wettrüsten, egal ob ziviler oder militärischer Natur ein Sieger hervorgehen wird oder überhaupt kann, bleibt abzuwarten.

Für die Bevölkerung sämtlicher Nationen wäre es von Vorteil, wenn verantwortungsvoll handelnde Regierungen moderne Technologien wirkungsvoll zu friedlichen Zwecken einsetzen würden. Ein Erfolg ist aber nur dann möglich, wenn die Vereinigten Staaten von Amerika vom gewohnten alleinigen Handel absehen und weltweite Konflikte wieder im Rahmen der Völkergemeinschaft gelöst werden.

Literaturverzeichnis

Becker, K. u.a. (2003):

Echelon, http://www.bpb.de/publikationen/U3P11A,0,0,5_4_Echelon.html#art0, 18.12.2004.

Bendrath, R. (2001):

Informationskriegsabteilungen der US-Streitkräfte, http://www.fogis.de/fogis-ap3.PDF, 18.12.2004.

Bendrath, R. (2001):

Krieger in den Datennetzen**,** http://www.heise.de/tp/r4/artikel/7/7892/1.html**,** 18.12.2004.

Bocklet, W. (2004):

Infanterist der Zukunft, http://www.soldat-und-technik.de/08-2004/idz.pdf, 18.12.2004.

Ernestus, W u.a. (1997):

Datenschutzfreundliche Technologien, http://www.lfd.m-v.de/informat/dsftechn/apdsftec.pdf, 18.12.2004.

Ernestus, W u.a. (1997):

Datenschutzfreundliche Technologien, http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm#Pseudonymisierung, 18.12.2004.

Ernestus, W (1999):

Datenschutzfreundliche Technologien, in: Fox, D. (Hrsg.), Datenschutz und Datensicherheit, Wiesbaden 1999.

Freude, A. (2004):

Kategorie Wirtschaft & Verbraucherschutz, http://www.bigbrotherawards.de/2004/.com/, 18.12.2004.

Hutter, R. (2002):

"Cyber-Terror": Risiken im Informationszeitalter, **http://www.bpb.de/publikationen/NVN0CA,2,0,CyberTerror:_Risiken_im_Informationszeitalter.html**, 18.12.2004.

Hülsmann, W. (2004):

Kategorie Gesundheit & Soziales, **http://www.bigbrotherawards.de/2004/.soc/**, 18.12.2004.

Krieger, W. (2003):

Geheimdienste in der Weltgeschichte, München 2003.

Lange, S. (2003):

In der Königsklasse unbemannter Flugzeuge, http://www.swp-berlin.org/common/get_document.php?id=865, 18.12.2004.

Lorenz, H. D. (2002):

Kommando Strategische Aufklärung in Dienst gestellt, http://www.sipotec.net/IAP_Aktuell/S_02_09.html, 18.12.2004.

Lux, C./Peske T. (2002):

Competitive Intelligence und Wirtschaftsspionage, Wiesbaden 2002.

Palm, G./Rötzer, F. (2002):

Enduring War- eine Einführung, in: Rötzer, F. (Hrsg.), Medien Terror Krieg, Hannover 2002.

Raven, K.:

Echelon - Das globale Abhörnetzwerk, http://kai.iks-jena.de/miniwahr/echelon1.html, 18.12.2004.

Rosengart, F. (2004):

Kategorie Technik, http://www.bigbrotherawards.de/2004/.tec/, 18.12.2004.

Schuldt F. (2003):

Jäger und Sammler,
http://www.streitkraeftebasis.de/C1256C290043532F/vwContentFrame/5EB0F4856E3BA144C1256EA000252BCB, 18.12.2004.

Weckbach-Mara, F. (2003):

Bundeswehrsoldaten in Kabul werden besser geschützt,
http://www.wams.de/data/2003/06/22/122831.html?prx=1, 18.12.2004.

o.V. (2004):

Internet-Strukturdaten, http://www.forschungsgruppe.de/Ergebnisse/Internet-Strukturdaten/web_III_04.pdf, 18.12.2004.

o.V. (2004):

Elektronische Kriegsführung,
http://de.wikipedia.org/wiki/Elektronische_Kriegsf%C3%Bchrung, 18.12.2004.

o.V.:

Schule für Strategische Aufklärung,
http://www.streitkraeftebasis.de/C1256C290043532F/vwContentFrame/FD293B60E634E7CEC1256EA000375924, 18.12.2004.

o.V. (2003):

Elektronische Kampfführung,
http://www.bwb.org/C1256DF2004FF94C/Docname/ORGANISATION_WTD81_AUFGABEN_ELOKA_ELOKA.HTM, 18.12.2004.

o.V. (2004):

Elektronische Kampfführung,
http://de.wikipedia.org/wiki/Elektronische_Kampff%C3%BChrung, 18.12.2004.

o.V. (2002):

Kommando Strategische Aufklärung,

http://www.bundeswehr.de/forces/streitkraeftebasis/030110_strat_aufkl.php,

18.12.2004.

o.V. (2001):

Transportpanzer 1, EloKa, HUMMEL,

http://www.sipotec.net/Neu_Ausr/Waffensysteme/hummel_beschr.html, 18.12.2004.

o.V. (2001):

Transportpanzer 1, A1, FUCHS, EloKa, Fernmeldeaufklärung,

http://www.sipotec.net/Neu_Ausr/Waffensysteme/fuchsfmaufkl_beschr.html,

18.12.2004.

o.V. (2003):

SAR-Lupe, http://www.ohb-system.de/dt/pdf/sar-lupe-broschure.pdf, 18.12.2004.

o.V. (2004):

Spionage, http://de.wikipedia.org/wiki/Spionage, 18.12.2004.

o.V. (2004):

Vorsicht! Wirtschaftsspione,

http://www.n24.de/wirtschaft/wirtschaftspolitik/index.php/a20041013143457316 86.

18.12.2004.

o.V.:

Wirtschaftsspionage heute, http://www.kdm-portal.com/sp_heute.html, 18.12.2004

o.V. (2004):

Volkszählungsurteil, http://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil,

18.12.2004.

o.V. (2003):

Neufassung des Bundesdatenschutzgesetzes vom 14. Januar 2003, http://www.datenschutz-portal.de/Dokumente/Neufassung%20des%20Bundesdatenschutzgesetzes.doc. 18.12.2004.

o.V. (2004):

Willkommen zu den deutschen BigBrotherAwards, **http://www.bigbrotherawards.de/**, 18.12.2004.