Themenbereich: Infowar

Andreas Riedler und Michael Bayr

19. Juni 2001

Medientechnik und Design, FHS-Hagenberg Hauptsraße 117
A-4232 Hagenberg, Austria
Seminararbeit zu Medientheorie 6
Lehrbeauftragter: MMag. Dr. Johann Mayr

Nichts sollte so hoch geschätzt werden wie Wissen über den Gegner; nichts sollte so geheim sein wie der Erwerb dieses Wissens. [1]

[1] Sun Tzu, 4tes Jahrhundert vor Christus

Inhaltsverzeichnis

1 Kurzfassung

Ziel dieser Seminararbeit ist es zu zeigen, wie sich Information auf moderne Kriegführung auswirkt und wie es in unserer Zeit zu Kriegen in allen Bereichen der Information gekommen ist.

Hacker kämpfen gegen das Monopol von Softwarefirmen, Firmen kämpfen um den gläsernen Konsumenten, Staaten streben absolute Kontrolle und Überwachung ihrer Einwohner an. Wir befinden uns in einer Phase der Veränderungen und Weichenstellungen für unsere Zukunft.

In dieser Arbeit versuchen wir zu zeigen, wie sehr das Fernsehen und der Siegeszug des Computers die Welt der Information beeinflußt. Eine Kriegsführung ohne diese beiden Faktoren ist nicht mehr denkbar.

2 Geschichte der Informationsbeschaffung und Geheimhaltung

Sichere Nachrichtenwege sind schon seit jeher entscheidend über Erfolg und Mißerfolg eines Krieges. Je schneller ein Feind über potentielle Pläne oder Truppenbewegungen erfahren kann, desto schneller kann dieser reagieren und um so besser ist seine Position im Kampf.

Daher wird schon seit Jahrtausenden versucht, Nachrichten zu verschlüsseln und zu verstecken, damit sie nicht in falsche Hände geraten. Staaten beschäftigen dafür eigene Verschlüsselungsdienste und eigene Abteilungen mit Kryptoanalytikern. Dieser ständige Kampf zwischen Verschlüsselung und Entschlüsselung ist mit einem großen geistigen Rüstungswettlauf zu vergleichen. Der geistige Rüstungswettlauf ist auch mit einer Evolution gleichzusetzen. Ein Code wird geschaffen. Dann wird dieser eingesetzt und jetzt kommen die Kryptoanalytiker zum Zug und versuchen den Code zu dechiffrieren. Wenn nun dieser Code dechiffriert ist, stirbt er, wenn er standhält wird er weiterentwickelt. Im Prinzip findet hier auch eine natürliche Auslese statt. Die Stärken eines Codes werden immer weiter verbessert und die Schwächen werden von den Kryptoanalytikern gnadenlos ausgenutzt. Die Verschlüsselung von Daten wird immer wichtiger und heute ist geschütze Information einer der wertvollsten Güter überhaupt geworden.

> *Die Kunst der geheimen Kommunikation, auch als Kryptographie bezeichnet, wird die Schlösser und die Schlüssel des Informationszeitalters bereitstellen.* [2]

[2] Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. München. 1999. S9f.

2.1 Die Entwicklung der Geheimschriften

Geheimschriften gehen bis ins 5te Jahrhundert vor Christus zurück und fanden Aufzeichnungen Ciceros zufolge das erste Mal im Krieg zwischen Griechenland und Persien Verwendung. Ein Grieche der im Exil in Persien wohnte, warnte die Griechen vor der Aufrüstung der Perser indem er dies auf eine Holztafel ritzte und dann mit Wachs übergoß. Damit kam es zur ersten Geheimschrift (in diesem Falle wird von Steganographie gesprochen, da die Information versteckt wird) und diese Information verhalf den Griechen zu einem Sieg, da sie sonst vollkommen unerwartet angegriffen worden wären. Die Technik der Steganographie war anfänglich effizient, aber sie hatte einen entscheidenden Nachteil: Wenn eine stenganographierte Botschaft gefunden wurde, lag sie unverschlüsselt vor. Daher entstand die Notwendikeit der Kryptographie, die es ermöglicht Nachrichten zu verschlüsseln. Trotzdem verwendeten die Deutschen im zweiten Weltkrieg teilweise noch rein die Steganographie und versandten zum Beispiel kleine Punkte, mit abfotografierten Geheiminformationen, in Briefen, die sie als i-Punkte tarnten. [3]

2.2 Kryptoanalytik und Weiterentwicklung der Kryptographie

Die Entwicklung der Steganographie und der Kryptographie ging immer eng einher mit der der Kryptoanalytik. Eine der ersten Ansätze um verschlüsselte Botschaften zu dechiffrieren war die Häufigkeitsanalyse. Hier wird die Häufigkeit von einzelnen Zeichen oder Buchstaben im Text ermittelt und auf die dahinterstehenden Buchstaben geschlossen. Dieses Verfahren ent-

[3] Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. München. 1999. S18ff.

wickelte Al- Kindi, ein arabischer Kryptoanalytiker. [4]

Generell wurden die größten Fortschritte auf diesem Sektor in Arabien gemacht, denn die Europäer kämpften lange Zeit noch mit grundlegenden Problemen der Kryptographie. In Europa trieben vor allem Klöster die Entwicklung der Kryptoanalytik voran, da sie im Alten Testament nach verborgenen Botschaften suchten. [5]

Im fünfzehnten Jahrhundert erlebte die Kryptographie in Europa einen entscheidenden Schub. Das Zeitalter der Renaissance und der politischen Intrigen führte zu einem Bedarf nach geheimen Botschaften. Der fruchtbarste Boden hierfür war Italien, da es hier zig verschiedene Stadtstaaten gab, die versuchten sich gegenseitig auszuspionieren. Um die grundlegenden Probleme der einfachen Verschlüsselung zu umgehen, wurden Botschaften nun auch mit zusätzlichen unnötigen Zeichen verschlüsselt oder es wurden Zeichen für bestimmte Codeworte eingeführt[6]

Vor allem im Zuge der technologischen Entwicklungen, wird die Kryptographie und Stenographie wichtiger. So gab es Probleme mit den Telegrafisten wie die Telegrafie aufkam, da diese sich von konkurrierenden Firmen bestechen ließen und Informationen an diese weitergaben. Deswegen verwendeten betroffene Firmen dann die polyalphabetische Verschlüsselung, die sogenannte Vigenere Verschlüsselung (Buchstaben verwenden verschiedene Alphabete), die anfänglich als absolut sicher galt. [7]

Diesen Mythos zerstörte Charles Babbage, einer der faszinierendsten Fi-

[4]Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. München. 1999. S35.

[5]Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. München. 1999. S42.

[6]Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. München. 1999. S44.

[7]Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. München. 1999. S85.

guren der Kyptographie im neunzehnten Jahrhundert als er die Vigenere Verschlüsselung durchschaute und entschlüsselte.

2.3 Die Mechanisierung der Verschlüsselung

Gegen Ende des neunzehnten Jahrhunderts schlitterte die Kryptographie in eine Krise aufgrund der Zerstörung des Vigenere Mythos und fehlender Impulse. Daher waren die Kryptographen auf der Suche nach einem neuen Verfahren, vor allem aufgrund der bahnbrechenden Erfindung des Funks welche Kryptographie unablassbar machte. Das Militär zeigte immenses Interesse am Funk, aber das Problem dieser Technologie war, das Nachrichten zwar einfach zu verschicken waren, aber genauso einfach abhörbar waren. Im ersten Weltkrieg verwendete zwar das Militär Funksprüche, doch war es eine Zeit der Rückschläge und Flops für die Kryptographie. Es gab zwar neue Chiffren, doch waren diese im wesentlichen nur Variationen und Kombinationen von Chiffren aus dem 19ten Jahrhundert und waren daher auch leicht dechiffrierbar.

Gegen Ende des Ersten Weltkriegs wurde der One-Time Pad (ein einmaliger Schlüssel) entwickelt, welcher wieder eine sichere Chiffrierung ermöglichte, da ein langes, zufälliges Codewort einmalig verwendet wird. Praktisch funktionierte dieses Verfahren aber nicht gut, da eine Vielzahl von Schlüsseln pro Tag erzeugt werden müßte und diese auch den Empfängern zugekommen lassen werden muß. Aufgrund dieser Nachteile kam dieses System nie wirklich zum Einsatz.

Der nächste Quantensprung für die Kryptographen kam mit der Entwicklung der Chiffriermaschinen. Die Entwicklung hier begann mit den Chiffrierscheiben. Die erste entwickelte der italienische Architekt Leon Alberti bereits im fünfzehnten Jahrhundert. Nach dem ersten Weltkrieg entwickelte Arthur Scherbius eine kryptographische Maschine, die im Prinzip wie die Chiffrier-

scheibe funktionierte. Diese kryptographische Maschine erlangte unter dem Namen Enigma Weltruhm. Das deutsche Militär kaufte 30.000 Enigma Maschinen und als der Krieg ausbrach, war es vollkommen klar, daß das deutsche Militär aufgrund dieser Chiffrierung einen immensen Vorteil hatte. Die Alliierten erstarrten aus Ehrfurcht vor diesem Gerät und waren anfänglich der Überzeugung das dieses Kodierung nicht zu dechiffrieren sei. Doch mit Hilfe von Spionage, Angst vor dem Krieg, der die polnischen Mathematiker zu schier unmenschlicher Arbeit trieb, und Mathematik konnte die Chiffrierung der Enigma geknackt werden. Zuerst überwanden polnische Kryptoanalytiker die Chiffrierung der einfachen Enigma, als aber die Deutschen die Enigma verbesserten, waren sie auch mit ihrem Latein am Ende. Knapp vor Ausbruch des Krieges teilten sie ihr Wissen mit den Engländern und Franzosen, die bis dahin überzeugt waren, daß der Code der Enigma nicht dechiffrierbar sei. Die Kryptoanalytiker in England, die im Bletchey Park (unter anderem Alan Turing) stationiert waren, trugen wesentlich zum Erfolg bei.

Nach dem Krieg dominierte der Computer den Kampf der Kryptologen und der Kryptoanalytiker. Die Zeit ist geprägt durch die Verwendung von Primzahlen, public und private keys und ständigen Weiterentwicklungen auf dem Sektor der Kryptographie und Steganographie. Die Entwicklung des RSA Verfahrens und von Pretty Good Privacy machte die Verschlüsselung für alle Privatpersonen zugängig. Damit ist eine neue Ära angebrochen. Problematisch ist natürlich auch der mögliche Mißbrauch dieser Verschlüsselung von kriminellen Elementen oder auch beispielsweise von Terroristen. Das wird eine der Herausforderungen der Kryptographie in der Zukunft sein: Der schwierige Spagat zwischen Schutz der Privatssphäre und Überwachungsmöglichkeit möglicher Krimineller und Terroristen [8]

[8]Singh, Simon: Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. Muñchen. 1999. S179ff.

3 Information als Waffe

Informationen und Medien sind mehr denn je auch als Waffe und Manipulationshilfen zu verstehen. Gerade in den letzten Kriegen wurde klar, daß kein Krieg gegen Public Opinion und die Presse in westlichen Ländern gewonnen werden kann. Wie konnte es aber zu solch einer Entwicklung kommen?

3.1 Wirkung des Fernsehens

Mehr als Leuten bewußt ist, hat die reportagenhafte Berichterstattung über das Leid und die exemplarischen Schicksale einzelner Menschen das Gewissen der westlichen Welt wachgerüttelt. Früher waren Menschen noch zu sehr mit eigenen Problemen und Gedanken beschäftigt um sich mit Kriegen in fernen Ländern auseinanderzusetzen oder das Leid dort zu verstehen. Aber durch solche Reportagen, Nachrichtensendungen und medienwirksame Events wie Live Aid ist das Fernsehen zu der Moralinstanz der modernen Welt geworden und hat somit, wenn man diese Idee theoretisch weiterstricken will, wahrscheinlich in ihrer Kraft und Wirksamkeit die Kirche abgelöst. [9]

Gepaart mit der Tatsache, daß Kriege eigentlich immer unklarer werden und damit auch die Grenzen zwischen Opfern, Tätern und auch klaren Rollenverteilungen fällt, befinden wir uns in einer neuen Zeit des Krieges und der Darstellung dieser in den Medien. [10]

Generell können Fernsehnachrichten und Fernsehberichterstattungen als ein einzig großer Markplatz gesehen werden. Leid und Schrecken kämpfen um Sendeplätze und Sendezeiten und nur die "stärksten" und "emotionalisierendsten" können sich durchsetzen. Nur diese haben dann auch das Potential

[9] Ignatieff, Michael: Die Zivilisierung des Krieges: Ethnische Konflikte, Menschenrechte, Medien. Rotbuch Verlag. 2000. Hamburg. S15.

[10] Ignatieff, Michael: Die Zivilisierung des Krieges: Ethnische Konflikte, Menschenrechte, Medien. Rotbuch Verlag. 2000. Hamburg.S27.

auf Spenden und Unterstützungen aus den Erste Welt Ländern. [11]

Wie aber alles in den Medien unterliegen auch die Verteilung von Sympathien und im Falle des Fernsehens die Verteilung von Sendezeiten Modetrends. [12]

3.2 Zapatistas

Eines der Themen, welches die Sympathie der Medien erringen konnte, ist die Widerstandsbewegung der Zapatistas in Mexiko. Teilweise haben sie es dem charismatischen Führer Subcomandate Marcos und dessen Anlehnung an Che Guevara, einem modernen Helden, zu verdanken, aber sicherlich auch der frühen Nutzung des damals noch jungen Mediums, des Internets. Schon 1993 wurde in einer Studie von zwei RAND (militärische Forschungseinrichtung in Kalifornien) Analysten festgestellt, daß die pro zapatistische Bewegung im Netz wohl beispiellos sei und ein sehr gutes Beispiel für Netwar wäre. [13]

Die Präsenz dieser Bewegung kann leicht bei einer Suche in Altavista (http://www.altavista.com) mit dem Suchbegriff "Zapatista" erkannt werden, bei welcher es 42868 Ergebnisse gab, wobei beispielsweise zu den Suchbegriffen "Hutu" und "Tutsi" jeweils nur um die 20000 Ergebnisse gefunden wurden, obwohl die Kämpfe zwischen Hutu und Tutsi wohl zu den blutigsten überhaupt in diesem Jahrhundert zählen. Drastisch ausgedrückt gibt eine Story über die sinnlose und unvorstellbare Gewalt in Ruanda nicht sehr viel her, wobei aber eine Story über den romantischen und idealistischen Kampf der Zapatista gegen ein ungerechtes Regime (aus ihrer Sicht) sehr wohl, zynisch gesagt, alt und jung begeistert.

[11] Ignatieff, Michael: Die Zivilisierung des Krieges: Ethnische Konflikte, Menschenrechte, Medien. Rotbuch Verlag. 2000. Hamburg. S37.

[12] Ignatieff, Michael: Die Zivilisierung des Krieges: Ethnische Konflikte, Menschenrechte, Medien. Rotbuch Verlag. Hamburg. 2000. S33.

[13] `http://www.eco.utexas.edu/faculty/Cleaver/zapsincyber.html`, 2. Mai 2001

3.3 Der virtuelle Krieg

Das Parade-Beispiel für die Darstellung von Krieg im Fernsehen ist wohl der Golfkrieg. Durch die Bilder aus dem Golfkrieg, vor allem aufgrund der Darstellung dieses Krieges als perfekter, sauberer Krieg, wurde unser Bild des Krieges nachhaltig verändert. Der Krieg erscheint virtuell, schon lange nicht mehr real. Mit präzisen Schlägen werden die Gegner angegriffen und eigentlich erscheint es, als ob kein Gegner der westlichen Militärtechnologie gewachsen ist. Dieser unerschütterliche Glauben der Menschen an die Technologie erschwert trotzdem das Leben des Militärs, da Wähler keine Toten sehen wollen, sondern nur ihre schönen rationierten Fernsehbilder vom einfachen virtuellen Tod, der niemandem wirklich wehtut und bei dem es eigentlich auch kein Leid gibt.

Um so schlimmer ist es bei solchen Kriegen wenn versehentlich zivile Ziele getroffen werden, wie beispielsweise Flüchtlingskonvois oder die chinesische Botschaft bei den NATO- Bombardements in Ex-Jugoslawien. Denn die Menschen erwarten sich von ihrem sauberen Krieg mit sauberen Waffen auch eine gewisse Zuverlässigkeit, sowie sie sich Zuverlässigkeit von ihren anderen technischen Geräten erwarten.

Der Krieg der westlichen Ländern verkommt immer mehr und mehr zu einem virtuellen Krieg. Wie empfindlich Menschen auf die Realität reagieren können, zeigt auch der Militäreinsatz Amerikas in Somalia. Nach der Ermordung der US-Soldaten und deren fernsehgerechte Schleifung durch Städte mußten die amerikanischen Politiker daraus die Konsequenzen ziehen und die Truppen aus Somalia abziehen[14]

[14]Ignatieff, Michael: Virtueller Krieg, Kosovo und die Folgen. Rotbuch Verlag. Hamburg. 2001. S76.

4 Informationstechnologie im Krieg

Mehr und mehr wird von sauberen Kriegen und Cyberwars gesprochen die angeblich ohne Risiko und Blutvergießen von statten gehen sollen. Wie weit sind wir aber von so einem Szenario entfernt und wie realistisch ist dieses? Momentan erscheinen die weit fortgeschrittenen Thesen eines Krieges mit Viren gegen Viren zwar noch eher unrealistisch, aber mit zunehmender Vernetzung und Abhängigkeit von Computernetzen, werden diese Szenarien immer realistischer. Mit Cyberterrorismus kann nämlich mit relativ wenig Aufwand großer Schaden angerichtet werden kann. Darüber hinaus sind die Gefahren einer Verhaftung oder einer rechtlichen Verfolgung noch relativ gering.

4.1 Schutzmaßnahmen einzelner Staaten

Wie ernst Regierungen diese Entwicklungen nehmen, sieht man anhand der Ansätze und Gesetze einzelner Staaten. Interessanterweise wird die größte Gefahr im Terrorismus gesehen, und Vorreiter in geplanten Abwehrmaßnahmen ist, wie so oft, Amerika mit einem geplanten Schutzschild gegen Cyberterrorismus.

Mußten Terroristen bisher ihre Waffen noch auf relativ gut zu überwachenden Waffenumschlagsplätzen kaufen, können jetzt terroristische Attacken einfach von einem Laptop ausgehen. Die Gefahren werden hier vor allem im zivilen Bereich gesehen, der nur ungenügend oder kaum auf solche Attacken vorbereitet ist und wo immenser wirtschaftlicher und menschlicher Schaden angerichtet werden kann. So sind als potentielle Ziele beispielsweise Zugzentralsysteme, Kraftwerke und Verkehrsleitsysteme zu sehen.

4.1.1 USA

Um solche Attacken und Anschläge zu verhindern plant US Verteidigungsminister Donald Rumsfeld einen gigantischen Schutzschild gegen Cyber-Attacken

sowohl für staatliche und private Netzwerke. Kostenpunkt solch eines Schutzschildes wären 30 Millarden Dollar. [15]

Die Taktik die mit diesem Schutzschild verfolgt werden soll, ist die der absoluten Abschreckung, ähnlich dem NMD Schild (National Missile Defense Schild). Wie so oft bei politischen Entscheidungen stehen hierbei aber auch wirtschaftliche Interessen im Hintergrund, denn mit diesem Schutzschild, soll der Welt die Kompetenz amerikanischer High-Tech Unternehmen gezeigt werden und so soll dieses Schutzschild auch der amerikanischen Wirtschaft einen Schub geben.

Geplant ist hierfür die Schaffung eines zentralen Überwachungstools, des sogenannten Fidnets, welches nach Installation bestimmter Soft und Hardware in teilnehmenden Unternehmen ständig die einzelnen Netzwerke untersucht und etwaigen Attacken entgegenwirkt. [16]

4.1.2 Österreich

Wie immer hinkt Österreich diesen Entwicklungen leicht hinterher und verkündete erst im Mai Schritte in Richtung eines Schutzschildes gegen etwaige Cyber-Attacken. Ein Pilotprojekt soll Mitte dieses Jahres gestartet werden und Ziel ist es, wie in Amerika, nicht nur offizielle Stellen, sondern auch private und wirtschaftliche Einrichtungen zu schützen. Daher strebt das Bundeskanzleramt eine Kooperation mit den Sozialpartnern und der ISPA (Internet Service Providers Austria) an. Potentielle Angriffsstellen für Cyberterrorismus und Cyberwar werden momentan in der Stromversorgung und in der Telekommunikation gesehen, mit denen potentiell ganz Österreich getroffen werden kann. [17]

[15] `http://www.spiegel.de/netzwelt/politik/0,1518,121954,00.html`, 30.04.2001

[16] `http://www.futurezone.orf.at/futurezone.orf?read=detail&id=59388`, 15.03.2001

[17] Standard. Wien. 5.Mai 2001

4.1.3 England

hnlich wie die USA, setzt auch Großbritannien Akzente in Richtung Bekämpfung von Cyberterroristen. Im Terrorismus Akt 2000 wurde festgelegt, daß Leute die sich in Computersysteme hacken und damit das Leben anderer gefährden, als Terroristen einzustufen sind, und dementsprechend auch die Gerichtsbarkeit dieser Personen zu handhaben ist. Das große Problem an diesem Terrorismus Akt 2000 ist aber die Möglichkeit der willkürlichen Entscheidungen die mit diesem Terrorismus-Akt mit einhergehen, denn nun können und werden jugendliche Hacker so behandelt wie IRA Terroristen. [18]

4.2 Cyber-Attacken einzelner Staaten

Wie wird nun aber wirklich mit den Möglichkeiten der Cyber-Attacken umgegangen? Sind diese rechtlich überhaupt möglich und wie weit gehen einzelne Staaten in diesem Bereich?

4.2.1 USA

Offiziellen Meldungen zufolge, hält sich Amerika noch von möglichen Cyber Attacken zurück, aber geplant wurden bereits solche Aktionen. Zumindestens eine geplante Aktion Amerikas wurde von offiziellen Stellen zugegeben, und zwar die Planung einer gezielten Serie von Hacker Angriffen auf strategische Ziele im Kosovo.

Hierfür arbeitete sogar das Pentagon ein Handbuch mit Richtlinien für sogenannte Cyber Attacken aus. Probleme die hierbei gesehen wurden und welche auch dazu führten, daß das US-Militär von solchen Attacken Abstand nahmen, war die schwere Einschätzbarkeit der Folgen einer Cyber Attacke. So arbeitet das Pentagon für Kriege immer Studien aus mit Zahlen

[18] `http://www.pcadvisor.co.uk/news/display_news.cfm?NewsID=844`, 20. Jänner 2001

für mögliche Tote und auch für mögliche zivile Verluste. Ein Bombenangriff mag auf den ersten Blick grausamer erscheinen, aber eine Cyber-Attacke kann viel weitreichendere Folgen haben, wenn Versorgungseinrichtungen attackiert werden oder generelle infrastrukturelle Ziele. So paradox es auch klingen mag, kann man eine Cyber-Attacke bei weitem auch nicht so gut medial umsetzen. Wenn Bomben hageln, versteht jeder die Botschaft, wenn aber nach und nach der Strom ausfällt, wird das Land zwar zermürbt, aber soetwas kann leicht in die Gegenrichtung losgehen und als Kriegsverbrechen gewertet werden. Beispielsweise wären auch Aussendung von falschen Codes von Militärfahrzeugen im Krieg oder die Fälschung eines Funkspruchs eines Militärcommanders an seine Truppen Kriegsverbrechen. [19]

4.2.2 China

Praktisch offen werden die Möglichkeiten der Cyberangriffe von China verwendet, das keinen Skrupel kennt, diese Taktiken einzusetzen und so ganze Länder oder auch Bewegungen und Religionsgemeinschaften einzuschüchtern. So verkündete China für die erste Maiwoche eine Woche der Hackerangriffe auf Amerika, welche aber in diesem Ausmaß nicht wirklich stattfand. Grund für diese Aktion war der Absturz eines chinesischen Kampffliegers nach der Kollision mit einem amerikanischen Spionageflugzeug. Diese Woche der Hackerangriffe verpuffte aber eher harmlos mit der kurzzeitigen Lahmlegung der Server für die Webpage des Weißen Hauses als Höhepunkt. China war und ist schon immer sehr fortschrittlich auf dem Bereich des Informationskrieges, schon 1985 wurde der Begriff Xinxi Zhan für den Informationskrieg geschaffen. Mittlerweile gibt es in China sogar militärische Studiengänge mit diesem Namen.

Der chinesische Ansatz des Informationskriegs ist eine Art Volkskrieg frei

[19] `http://www.washingtonpost.com/wp-dyn/articles/A35345-1999Nov7.html`, 10.November 2000

nach Mao. Während früher aber Heerscharen von Bauern in den Krieg geschickt wurden, so soll es nun ein Heer von Viren geben. Sun Tsu's Thesen werden insofern verwendet, als daß er schon früher in seinen Werken empfohlen hat indirekte Angriffe zu verwenden um einen stärkeren Feind zu überwinden. Dieser stärkere Feind ist in diesem Fall Amerika. [20]

China geht seit jeher sehr restriktiv mit Information um und so gibt es in China auch nur einen beschränkten Zugang zum Internet. Auf potentielle Gefahren reagiert China hart auf allen Fronten, wie uns das Beispiel der Falun Gong Sekte zeigt. China verbot die Bewegung unter dem Vorwand es handle sich um eine staatsgefährdende Sekte, nahm führende Köpfe der Falun Gong Bewegung fest und internierte Anhänger der Bewegung. Um dieses Maßnahmenpaket abzurunden wurden die Internet-Seiten der Falun Gong vom Netz genommen. Weiters versuchte die chinesische Regierung mit Computerattacken internationale Provider zu zwingen Falun Gong Seiten vom Netz zu nehmen und auch beispielsweise Buchläden dazu zu bringen keine Bücher mehr von dieser Bewegung zu verkaufen.

Anhand dieses Beispiels sieht man die Gefahren und die Möglichkeiten eines Cyberwars.

4.3 Cyberwar auf dem realen Schlachtfeld

Nicht nur im Bereich der Computertechnologie wird verbissen an Möglichkeiten für den absoluten Informationskrieg gearbeitet, sondern auch im klassischen Infantriebereich, wie auch in allen anderen Bereichen des Heeres. Ein Zukunftsszenario ist es beispielsweise im Infantriebereich, den Soldaten noch weiter aufzurüsten und praktisch zu einer selbständigen Kampfmaschine mit all den nötigen Informationen zu machen. Der Plan ist es ein Exo (Außen-) Skelett zu entwickeln, welches den Soldaten ermöglichen soll mehr Lasten zu

[20] Napack, Jonathan: Cyberthreats rising in the east. In: Wired, März 2001, S 73

tragen und dadurch auch mehr Informationsgeräte bei sich zu haben. Die Vision der militärischen Planer ist es einen Soldaten oder eine ganze Einheit in einem Kriegsgebiet absetzen zu können, die für sich kämpfen kann und alle nötigen Geräte und Info mit sich hat und jederzeit der Zentrale Bilder, Videos und andere wichtige Daten übermitteln kann. [21]

[21] `http://www.heise.de/tp/deutsch/special/info/4700/1.html`, 30 Jänner 2001

5 Der Kampf um den Menschen

Der Mensch ist im Informationszeitalter zu einer wichtigen Ressource geworden. Für das Militär ist er nicht mehr nur als Bedienungseinheit für diverse Waffeneinheiten gedacht, er ist auch selbst wieder zu einer gefährlichen Waffe geworden, ausgerüstet mit einem Computer und dem Wissen wie feindliche Information vernichtet oder zu seinen Gunsten verändert werden können. Information wird in den Auseinandersetzungen der Zukunft zu der wichtigsten Ressource werden, deren Besitz und Auswertung zu einem großem Teil über Sieg oder Niederlage entscheiden wird. Die Parteien die um diese Ressourcen kämpfen sind sowohl die klassischen Machtstrukturen der Nationalstaaten oder der ethnischen Gruppen, als auch die neuen Machtstrukturen der multinationalen Konzerne und Unternehmen, die mit den Nationalstaaten um die vorherrschende Machtstellung zu konkurrieren suchen.

Eine Tatsache, die den Kampf auf Basis von Informationen besonders für kleine, finanziell nicht gut ausgerüstete Gruppierungen, und auch Terroristen wichtig macht, ist der geringe Aufwand an Material und Menschen der notwendig ist um empfindliche Schläge gegen seinen Gegner zu bewirken. Dies macht den Krieg im Cyberspace [22] zu einem Gebiet auf dem auch von staatlicher Seite große Anstrengungen unternommen werden.

> *Verteidigungsbehörden und Sicherheitsexperten glauben, daß über 120 Nationen Techniken für einen Informationskrieg entwickeln. Diese Techniken ermöglichen es unseren Feinden, sensible Datensysteme der Verteidigungsbehörden oder öffentliche Netzwerke, die die Verteidigungsbehörden unbedingt zu Kommunikationszwecken brauchen, zu kontrollieren oder zu zerstören. Terroristen und andere Widersacher sind heute dazu in der Lage, nicht*

[22] Der Begriff Cyberspace wurde von William Gibson in seinem 1984 erschienen Cyberpunk-Science-Fiction-Roman "Neuromancer" geprägt

rückführbare Attacken von jedem beliebigen Ort weltweit zu starten. Sie könnten kritische Systeme, z.B. Waffen-, Befehls- und Kontrollsysteme, mit raffinierten Computerviren infizieren, die dazu führen, daß die Systeme nicht mehr richtig arbeiten. Ebenso könnten sie die Kommunikation zwischen unseren Streitkräften abbrechen und unsere Versorgungs- und Logistiklinien beeinträchtigen, indem sie Schlüsselsysteme der Verteidigungsbehörden angreifen.
[23]

Doch nicht nur im militärischen oder wirtschaftlichen Einsatz ist der Informationskrieg zu sehen. Durch die Natur der Information, sie nicht als materielles Gut verwahren zu können ist dies ein wichtiger Angriffspunkt für terroristische Organisationen oder Guerillakämpfer. In den weltweiten Netzen kann jeder der über genügend Wissen verfügt zu einer ernsten Bedrohung werden. Die Angst vor Crackern oder Hackern, die sich Zutritt zu Computernetzen verschaffen und so Zugang zu sensiblen Daten bekommen könnten ist weit verbreitet.

5.1 Cybercrime und Infoterroristen

Die neuen Chancen in den weltweiten Netzen weitgehend unerkannt und schwer mit nationalen Gesetzen verfolgbar zu sein, haben auch die Kriminellen sehr schnell genutzt und so eine weitere Front im Cyberspace eröffnet. Der relativ neue Aspekt sich mit Tätern auseinandersetzen zu müssen die nicht direkt erfassbar sind, oft weit von den Orten ihrer Taten entfern sind oder gar nicht ermittelbar sind, stellt die Behörden vor die neue Herrausforderung, auf internationaler Ebene miteinander zu arbeiten. Die noch stark

[23]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Testimony, 05/22/96, GAO/T-AIMD-96-92)

auf nationale Ebene beschränkte Gesetzgebung bietet hier den Tätern einen nicht zu unterschätzenden Vorteil.

> *Stephen Orfrei, Viceprasident für Electronic commerce und Neue Technologien bei MasterCard, beziffert den Anteil der der Internettransaktionen von MasterCard mit ca. 2 bis 2.5 Prozent der Gesamtzahl von Transaktionen des Unternehmens. Unter Annahme der unteren Grenze von 2 Prozent, und bei einem Gesamtverlust durch Betrug von 526 Millionen Dollar, ergibt die einen Verlust durch Internetbetrug von 10.5 Millionen Dollar. .....*
>
> *Da laut Visa die Rate von Onlinebetrug um 1 drittel höher ist als die Gesamtzahl der konventionellen Betrugsfälle, ist die Schätzung auf 20 millionen Dollar allein für Visa und MasterCard eher als das untere Limit zu sehen. ...* [24]

Mehr noch als die finanziellen Verluste wiegen aber die Gefahren, der Cyberspace-Terroristen und anderer gewalttätiger Organisationen. Das organisierte Verbrechen hat längst die Möglichkeiten, die das Internet für ihre Tätigkeiten bietet erkannt, und somit eine neue Qualität erreicht. Die Kommunikation innerhalb dieser Organisationen wurde durch die Möglichkeiten des weltweiten Datenverkehrs erheblich verbessert. Der Vorsprung, den der Untergrund durch die frühe Nutzung und die somit erworbene Erfahrung im Umgang mit den weltweiten Netzen erworben hat, stellt eine große Herausforderung an ihre Gegner dar, die erst sehr spät auf diese Möglichkeiten reagiert haben. Wodurch sie sich in einem technologischen Nachteil befinden, der durch die globalen Aktionen ihrer Gegenspieler, und ihrer eigenen nationalen Ausrichtung nur noch vergrößert wird. So entzieht sich einer der meistgesuchten Männer der USA, der Terroristenführer Omar Bin Laden seit

[24] Brunker, Mike "E-business vs. the perfect Cybercrime", 3. März 2001 MSNBC-network `http://www.msnbc.com/news/376973.asp`

mehrere Jahren dem Zugriff der amerikanischen Spezialeinheiten. Durch den Einsatz von Satellitenverbindungen und starker Kryptographie ist immer die Kontrolle über sein Netzwerk des Terrors gewährleistet. Auch die ständige Versorgung mit den nötigen Informationen ist so gesichert.

5.2 Privatsphäre im Cyberspace?

Das Internet, einst ein Ort des Zusammentreffens, und der Kommunikation, in dem die Privatsphäre des Users ein eherner Grundsatz war, ist im Zuge der Kommerzialisierung, und das Vordringen der wirtschaftlichen Interessen der Computerindustrie zu einem Ort der immer stärker werdenden Überwachung geworden.

Mit der zunehmenden Verbreitung des WorldWideWeb, das die Forderung der Wirtschaft nach einem quasi-statischem Medium, bestens erfüllt. Hier wird der Benutzer zu einem passiven Konsumenten, dem der Endruck vermittelt wird ohne Hilfe im globalen Netzerk verloren zu gehen. Doch zum seinem Glück stehen schon Repräsentanten der Wirtschaft in Form von AOL, MDSN oder anderen so genannten Protalen bereit, ihn in ihre schöne neue Welt zu führen. Vom ursprünglichen Gedanken des freien Gedankenaustausches, und der weltweiten Kommuniaktion in Foren, Mailboxes und Chatrooms ist wenig geblieben. Mit dem Siegeszug des WWW und der damit verbunden passiven Haltung des Users, der anstatt kommunikativ an der Gemeinschaft teilzuhaben, nur noch passiv den vorgefertigten Texten und Bildern ausgesetzt wird, ist es gelungen das in den Anfängen interaktive Medium Internet zu einem dem Fernsehen ähnlichen passiven Medium zu machen. Um die Interessen der Anbieter dieser Informaton immer besser zu wahren, und dem User immer spezifischer mit genau auf ihn angepasste Informationen zu versorgen, ist eine enorme Gier auf möglichst persönliche Daten des Einzelnen entstanden. Kaum eine Site dieser “Informationslieferanten”, die nicht mit “personali-

sierten Inhalten" und "Userfreundlichkeit der Seitengestaltung versucht an ein möglichst komplettes Userprofil zu gelangen.

Eine ganze Industrie der Datensammler und Userklassifizierer ist in den letzten Jahren entstanden, deren einzige Aufgabe es ist, den einzelnen Benutzer in möglichst kompletter Form, mit all seinen Vorlieben und Ansichten in einer für zahlungskräftige Interessenten zugänglich zu machen.

Auch von der Softwareindustrie wird viel von "Kundenbindung" gesprochen und versucht mit diversen Lizenzmodellen und proprietären Protokollen den User an seine Produkte zu zu binden, und zu verhindern, daß er Produkte der "Mitbewerber" verwendet. Diese Lizenzen verschaffen dem Unternehmen dabei oft starke Rechte auf die Daten seiner Kunden, und auch das Senden von Daten an das Unternehmen oder ihm nahestehenden Organisationen ohne Wissen des Users ist eine verbreitete Vorgehensweise.

6 Interaktion Staat und Industrie

> *Ich sehe in naher Zukunft eine Krise auf uns zukommen, die mich sehr beunruhigt und um die Sicherheit meines Landes bangen läßt. Als Folge des Krieges haben die Großunternehmen die Herrschaft übernommen, und eine Ära der Korruption auf höchster Ebene wird die Folge sein. Um ihre Vorherrschaft zu verlängern, werden die Reichen unseres Landes so lange die Vorurteile der Menschen schüren, bis aller Reichtum in einigen wenigen Händen konzentriert und die Republik zerstört ist. Ich verspüre in diesem Augenblick größere Besorgnis um die Sicherheit meines Landes als je zuvor, sogar mitten im Kriege. Gebe Gott, dass meine Befürchtungen sich als unbegründet herausstellen mögen.* [25]

Diese Aussage von Abraham Lincoln, zu einer Zeit getätigt, in der die Auswirkungen der Informationsgesellschaft noch in keiner Weise abzusehen war, scheint sich in letzter Zeit immer mehr zu bewahrheiten. Im Zuge der Globalisierung und der immer grösser werdenden Megakonzerne wird auch die Macht dieser Konzerne auf den Staat immer größer. So werden die Interessen der Konzerne zu Interessen des Staates und umgekehrt.

6.1 Der Staat als williger Helfer der Konzerne

In den letzten Jahren begann sich ein Gespenst, das lange Zeit durch diverse Seiten und Newsgroups über Verschwörungstheorien gespukt war, zu materialisieren. Das lange als eine Wahnvorstellung paranoider Netzjunkies abgetane weltweite Abhörsystem ECHELON stellte sich als existierende, und bei weitem leistungsfähigere Installation von Anlagen quer durch die ganze Welt heraus als zuerst angenommen.

[25] Abraham Lincoln

Nach Bekanntwerden der Existenz dieser Anlagen, forderte die Europäische Union die USA auf, ihr Einblick in die Fähigkeiten und den Zweck dieser Anlagen zu geben. Diese Ansuchen wurde zunächst von den USA mit dem Hinweis auf die nationale Sicherheit und den strikten militärischen Zweck dieser Anlage verzweigte. Als der Druck der EU und ihrer Mitgliedsstaaten auf die USA allerdings groß genug wurde, und auch die nationalen Nachrichtendienste begannen intensiv zu recherchieren wurden nach und nach Daten zu ECHELON bekannt, und auch über den Zweck und die Verwendung der Anlagen. Es stellte sich heraus dass keineswegs nur militärische Daten abgehört und analysiert wurden, sonder auch Industriespionage im großen Stil gegen alle nichtamerikanischen Firmen zu einem der Primärziele von ECHELON gehören. Somit machte sich der Staat zu einem Werkzeug seiner Wirtschaft. Dies ist nur ein Beispiel in eine langen Reihe von Fällen in dem ein Staat seine Ressourcen einsetzt um der Industrie zu helfen.

6.2 Der Einfluss der Industrie auf die Regierungen

Sind es die Regierungen dieser Welt im Regelfall doch gewohnt alle Drähte der Macht fest in Händen zu halten, stehen sie durch die zunehmende Abhängigkeit von Computersystemen und Netzwerken immer mehr unter dem Druck der Computerindustrie.

> *Alle nicht-staatlichen Organisationen, die das dreihundertjährige Gewaltmonopol der Nationalstaaten unter heutigen Computerbedingungen Schritt um Schritt zersetzen würden, nennen die nationalstaatlich finanzierten Strategen des Informationskrieges immer nur umweltverseuchte Ökologen, friedensverseuchte Linke und islamverseuchte Terrorbanden. Was sie unterschlugen, ist die Computerbranche selber - nicht als mythische Letzte Grenze freier Hacker, sondern als ebenso empirische wie kriegerische Bande*

globaler Konzerne. Diese Bande hat es immerhin schon geschafft, die Staatsmonopole für Post, Funk und Telekommunikation aufzurollen. [26]

Die Macht, die Unternehmen wie Mircosoft[27] auf die Wirtschaft und die Regierungen haben ruft regelmäßig die Datenschützer und nationalen Nachrichtendienste[28] auf den Plan. Um zu überprüfen ob man sich damit nicht der heimlichen Kontrolle von diesen Firmen und den Geheimdiensten der Heimat dieser Firmen ausliefert. [29] Die aggressive Politik dieser Firmen, sich mit allen möglichen Mitteln Marktanteile zu erobern und in sensible Bereiche vorzudringen, gleicht einer Infiltration mit feindlichen Agenten.

6.3 Der Aufstand der Hacker

Entgegen den immer strikter werdenden Einschränkungen, die uns die Softwareindustrie auferlegt, gibt es auch einen immer stärker werdenden Gegentrend. Ausgelöst von einigen Hackern, die sich nicht mit der Veränderung der Softwareszene abfinden wollten, und sich nicht in die Korsettes strenger Softwarelizenzen und Non-Disclosure-Agreements(NDA's) zwängen lassen wollten. Sie begannen im Gegensatz zu den kommerziellen Softwareschmieden die frei Verfuegbarkeit von Software und die Möglichkeit, diese zu verändern und zu benutzen zur Tugend zu erheben. Vom ursprünglichen Geist des Internets, Community und Interaktivität inspiriert begann die Free Software Foundation [30] rund um Richard M. Stallman mit der Entwicklung eines

[26] Kittler, Friedrich. In: Stocker, Gerfried; Schöpf, Christine. Information.Macht.Krieg, Springer Verlag. Wien. 1998. S306f

[27] `http:www.microsoft.com`

[28] `http://www.heise.de/tp/deutsch/special/info/6933/1.html`

[29] es wurde in Microsoft Windows und in einem Emailprogramm von Lotus ein als NSA-Key berühmtgewordener versteckter Zugang zum System entdeckt. `http://www.kutz.de/pcsicherheit/windows2.htm`

[30] `http://www.fsf.org`

freien Betriebssystemes, dem GNU (Gnu is Not Unix) Operating System[31], das 1994 mit dem bereits fertiggestelltem Linux - Kernels des Finnen Linus Torvalds [32] zu einem funktionstüchtigem Betriebssystem mit allen notwendigen Tools vereint wurde. Ein Jahr früher, 1993 wurde die erste Version von FreeBSD [33]veröffentlicht, die an der Berkely Universität entstanden war, und unter einer ähnlichen Lizenz [34] stand, die allerdings nicht so restriktiv im Bezug auf die weiterverwenung des Codes war wie die GPL.

Duch die Gnu General Public Licence[35], die von Richard M. Stallman für die Sicherstellung der Freiheit des Codes und des Users entwickelt wurde, wurden viele Entwickler ermutigt ihren eigenen Code zu dem Projekt beizutragen, und eigene Projekte unter GPL zu stellen. Das GNU - Projekt, das hohen Wert auf seinen philosophischen Background legt[36] hatte seine Ziel, ein freies Betriebssystem zu schaffen zwar erreicht, doch wurde es von vielen Entwicklern gerade wegen seines Philosphischen Ansatzes abgelehnt. Resultierend daraus entstand die, mehr dem Unternehmertum zugetane OpenSource Bewegung, die zwar auch das offenlegen des Sourcecodes an sich fordert, aber gleichzeitig die Freiheiten gegenüber dem Benutzer auf dem das Free Software - Prinzip aufbaut nicht sicherstellen. [37]

[31] `http://www.gnu.org`

[32] `http://www.kernel.org`

[33] `www.freebsd.org`

[34] Dies ist die originale BSD-Lizenz, heute steht FreeBSD unter GPL `http://www.xfree86.org/3.3.6/COPYRIGHT2.html`

[35] `http://www.gnu.org/copyleft/gpl.html`

[36] `http://www.gnu.org/philosophy/`

[37] `www.gnu.org/philosopy/free-software-for-freedom.html`

7 Auswirkung auf das Individuum

Es sollte jedem, der das Internet nutzt, klar sein, daß der Infowar nicht etwa eine abstrakte Vorstellung über eine künftig mögliche Art der Kriegsführung ist, sondern daß dieser Krieg bereits tobt. Und zwar nicht etwa in den entfernten Ecken der Militärgeheimdienste, oder zwischen chinesischen Crackern, die den Klassenfeind USA schaden wollen. Der wirkliche Infowar findet direkt an unseren Einwahlknoten oder auf unseren Festplatten statt.

Jeder einzelne User ist im Visier der Datenspione und Infosammler. Jeder, der Zugang zu Informationen hat, die für eine andere Gruppe von Nutzen sein kann, ist ein potenzielles Ziel. Die Überwachung nicht verschlüsselter elektronischer Post, ist seit der Enttarnung von ECHELON traurige Gewissheit. Das auch im privaten Bereich die Interressen von diversen Gruppierungen zu Angriffen führt zeigt das folgende Beispiel:

> *Gegen Ende des Jahres 1994 begannen Postings von alt.religion.-scientology zu verschwinden, manchmal mit der Erklärung, daß das Posting wegen Copyright-Verletzungen gelöscht werden mußte. Bis heute ist es nicht klar, wer hinter der Ausführung dieser Cancelbots - so werden die Löschautomaten genannt - steckt. Die Church of Scientology wies jegliche Verantwortung von sich. Die Anti-Scientologen begannen, den anonymen Teilnehmer als Cancelbunny zu bezeichnen, ein ironischer Bezug sowohl zu dem hüpfenden Hasen aus der bekannten Batterien-Werbung als auch zu dem bekannten Netzbewohner Cancelmoose, der (das?, die?) es zu seiner Aufgabe gemacht hat, einen cancelbot-Prozeß aufzubauen, der bei anderen Spam- Aktionen im Internet zum Einsatz kommen soll. Aber wer oder was auch immer der Cancelbunny sein mag, seine Bemühungen wurden schnell pariert durch die Entwicklung einer anderen Software-Waffe mit dem treffenden*

Namen Lazarus. Lazarus stellt gelöschte Nachrichten wieder her, oder, genauer gesagt, macht den Original-Absender und alle Teilnehmer einer Newsgroup darauf aufmerksam, daß eine bestimmte Nachricht gelöscht wurde. Es bleibt dem Absender belassen, die Nachricht wiederherzustellen, wenn der Löschbefehl nicht von ihm oder ihr ausgegangen war. [38]

Diese anfänglich noch harmlosen ersten Geplänkel, änderten schnell ihre Qualität, als der Interne Geheimdienst der Scientologen begann, die "feindlichen" User zu überwachen und auszuspionieren. Der sekteninterne Geheimdienst der Scientologen führt inzwischen penibel Buch über alle, die es wagten, sich in Foren oder WWW-Sites gegen die Sekte zu stellen.

[38]The First Internet War; The State of Nature and the First Internet War: Scientology, its Critics, Anarchy, and Law in Cyberspace. David G. Post, Reason magazine. April 1996. (1996 David G. Post. Permission granted to redistribute freely, in whole or in part, with this notice attached.)

8 Ausblick in die Zukunft

> *Wenn die autoritäre Technologie einmal mit Hilfe neuer Formen der Massenkontrolle, ihrem Füllhorn an Beruhigungsmitteln und Aphrotisiaka, Ihre Macht konsolidiert, kann die Demokratie dann in irgendeiner Form überleben?* [39]

Ist die Demokratie als Staatsform überholt?

In Anbetracht der immer weiter fortschreitenden Aufhebung der Privatsphäre und dem immer stärker werdenden Einfluss der Unternehmen auf Staat und Privatperson, ist dies eine Frage die sich füher oder später stellen wird. Obwohl sicher keiner der Machtkomplexe offen einen Sturz der Demokratie anstrebt, findet doch langsam und unaufhaltsam ein Wandel des Demokratieverständnisses statt. Mit Hilfe der Medien, wird eine immer stärkere Akzeptanz von totaler berwachung des Menschen zu seinem eigenen Wohle, etabliert. Dies führt zu einer immer stärkeren Verstrickung von Staat und Unternehmen, die im Endeffekt den Staat zum Spielball wirtschaftlicher Interessen macht.

Es besteht die Gefahr, daß die Entwicklung in die Richtung einer Zukunftswelt geht, wie sie der Autor Neil Stephenson in seinem Roman Snow Crash [40]beschreibt. In dieser Welt haben Unternehmen und das organisierte Verbrechen die Kontrolle über das Leben der Menschen. Die traditionellen Staatsformen sind aufgelöst und an deren Stelle treten stadtstaatlich geführte "Franchise" Unternehmen, die den Menschen neben Arbeit auch Wohnraum und ihre eigenen Gesetze vorgeben. Der soziale Status und die Lebensqualität werden hier noch viel extremer davon bestimmt wo man lebt und arbeitet. Totale Überwachung ist zu einer akzeptierten Tatsache geworden. In

[39]Mumford, Lewis. In: Druckey, Thimothy: Diabolische Unsichtbarkeit. Springer. Wien, 1998

[40]Stephenson, Neal: Snow Crash. Bantam Doubleday Dell Pub. 2000

dieser Welt ist der Zugang zur Information und die Information zu einem entscheidenden Machtfakor geworden.

In dieser reglementierten Welt erscheint die virtuelle Welt als letzte Zufluchtsstätte, in der die Menschen das sein können, was sie wollen und in der sie nach ihren eigenen Regeln leben können. Diese Freiheit ist aber auch nur eine vordergründige, da jeder hier auch gewissen Regeln folgen muß, und die einzigen wahren Freien sind in dieser Welt die Hacker, die eigentlich zu einem großen Teil auch die Erbauer dieses Systems waren und sich dadurch Freiheiten erschaffen haben die normalen Benutzern nicht zugnglich sind. Das ist in einer gewissen Weise paradox, denn die Sündenböcke der Stadtstaaten und deren Rechtfertigung für bestimmte Sicherheitsmaßnahmen, sind in diesem Roman eigentlich die Leute, die für aller Freiheit kämpfen.

So ist es eigentlich zu überlegen, wer nun die wirklich Bösen in dieser Welt der neuen Bedrohungen sind und wer eigentlich von den Entwicklungen momentan profitiert. Denn im Endeffekt lässt sich alles auf die Gier nach Macht und Geld reduzieren..

Literatur

Bücher

[1] Ignatieff, Michael: Die Zivilisierung des Krieges: Ethnische Konflikte, Menschenrechte, Medien. Rotbuch Verlag. Hamburg. 2000.

[2] Ignatieff, Michael: Virtueller Krieg, Kosovo und die Folgen. Rotbuch Verlag. Hamburg. 2001.

[3] Singh, Simon: Geheime Botschaften: Die Kunst der Verschlsselung von der Antike bis in die Zeiten des Internet. Carl Hanser Verlag. Muñchen. 1999.

[4] Tzu, Sun: Art of War. Westview Press. 1994.

[5] Stephenson, Neal: Snow Crash. Bantam Doubleday Dell Pub. 2000.

[6] Stocker, Gerfried; Schöpf Christine: Information.Macht.Krieg Springer Verlag. 1998

Online

[7] `http://www.abcnews.go.com/sections/world/DailyNews/hamas010308.html`, 15.Mrz 2001

[8] `http://www.eco.utexas.edu/faculty/Cleaver/zapsincyber.html`, 2. Mai 2001

[9] `http://www.futurezone.orf.at/futurezone.orf?read=detail&id=59388`,15. Mrz 2001

[10] `http://www.futurezone.orf.at/futurezone.orf?read=detail&id=7333`,15. Mrz 2001

[11] http://www.futurezone.orf.at/futurezone.orf?read=detail&id=59950,15. Mrz 2001

[12] http://www.futurezone.orf.at/futurezone.orf?read=detail&id=59988,15. Mrz 2001

[13] http://www.futurezone.orf.at/futurezone.orf?read=detail&id=22604,30. Mrz 2001

[14] http://www.heise.de/tp/deutsch/special/info/4700/1.html, 30 Jnner 2001

[15] http://www.pcadvisor.co.uk/news/display_news.cfm?NewsID=844, 20. Jnner 2001

[16] http://www.spiegel.de/netzwelt/politik/0,1518,121954,00.html, 30. April 2001

[17] http://www.washingtonpost.com/wp-dyn/articles/A35345-1999Nov7.html, 10.November 2000

[18] http://www.gnu.org 26. Ferbuar 2001

[19] http://www.gnu.org/philosophy, 15. März 2001

[20] http://www.gnu.org/philosophy/free_software-for-freedom.html, 15. März 2001

[21] http://www.freebsd.org, 7. Mai 2001

[22] http://www.kernel.org, 7. Mai 2001

Zeitschriften

[23] Napack, Jonathan: Cyberthreats rising in the east. In: Wired, Mrz 2001, S 73

Zeitungen

[24] Standard. Wien. 5.Mai 2001