Ranja Gaafar; Stephan Kleiner; Mario Krsek; Anna Sturm

Information Warfare

1999

https://doi.org/10.25969/mediarep/1344

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Gaafar, Ranja; Kleiner, Stephan; Krsek, Mario; Sturm, Anna: Information Warfare. In: *Augen-Blick. Marburger Hefte zur Medienwissenschaft*. Heft 29: Information ist Macht. Medien und politische Strategie der USA (1999), S. 31–44. DOI: https://doi.org/10.25969/mediarep/1344.

Ranja Gaafar, Stephan Kleiner, Mario Krsek, Anna Sturm

Information Warfare.

In den letzten Jahren hat sich im gesellschaftlichen, wirtschaftlichen und militärischen Bereich ein rascher internationaler Umbruch durch die Vernetzung der Telekommunikation vollzogen. Die Gesellschaft hat sich von einer Industriegesellschaft zu einer Informationsgesellschaft entwickelt. Die unterschiedlichsten Benutzer profitieren davon. Wo vor einigen Jahren das Fax noch eine seltene und teure Einrichtung in privaten Haushalten war, kann heute jeder günstig und bequem von seinem privaten Computer aus mit dem Internet um die ganze Welt surfen und jeder überall durch sein Mobiltelefon erreichbar sein.

Bei Militäreinsätzen in Krisenregionen rechtfertigen die westlichen Mächte ihre Interventionen in ausführlichen Pressekonferenzen, bei denen mit Hilfe der neuesten militärischen Radar- und Satellitenempfänger präzise Videobilder die Glaubwürdigkeit unterstreichen und eine Notwendigkeit der militärischen Interventionen versichern sollen. Die Illusion wird aufgebaut, daß es einen Krieg geben kann ohne viel Blutvergießen, vergleichbar mit einem exakten chirurgischen Schnitt. Man erinnere sich nur an die tägliche Videovorführung während des letzten Golfkrieges im Winter 1998 oder an den Kosovokonflikt. Beispielsweise sollten die Vorher-/Nachherbilder von zerbombten Gebäuden die präzise Schlagkraft und somit die Vermeidung von Kollateralschäden der alliierten Waffensysteme veranschaulichen. Manchmal allerdings erscheint die Presse mit anderem, nicht ganz so blutfreiem Bildmaterial von Kriegsschauplätzen, was militärische Strategieentwürfe erschwert, da die Akzeptanz der Bevölkerung für eine militärische Intervention mit der steigenden Anzahl *sichtbarer* Opfer sinkt. Jedoch führt gezielt eingesetztes Propagandamaterial des „feindlichen" Landes zu einer falschen Einschätzung der Lage. Der Einsatz moderner Kommunikationstechnologie im Krieg ist inzwischen so allgemein geworden, daß ein neuer Begriff entstanden ist: *Information Warfare.*

Die damit bezeichneten Taktiken können sich aber auch gegen hochtechnologisierte Länder und deren nationale Informationsstruktur richten, von der praktisch alle gesellschaftlichen, wirtschaftlichen und sicherheitspolitischen Funktionsbereiche immer mehr abhängen. Und nicht nur die nationalen Informationsinfrastrukturen sind bei einem elektronischen Angriff gefährdet, durch die globale Vernetzung werden andere Partnerstaaten ebenfalls betroffen.

Vor der Darstellung der neuen Herausforderungen für die internationale Sicherheit sollte der Begriff *Information Warfare* geklärt werden. Im militärischen Sprachgebrauch der USA findet sich folgende offizielle Definition:

> Aktionen zur Erlangung der Informations-Oberhoheit, indem die Information des Feindes, seine informationsgestützten Prozesse, sein Informationssystem und seine Computer-Netzwerke beeinflußt und gleichzeitig die eigene Information, informationsgestützten Prozesse, Informationssysteme und Computer-Netzwerke geschützt werden.[1]

Sachlich geht es also um den „Kampf" mit und um Informationen. Man benutzt Informationen, um andere Informationssysteme zu manipulieren, zu stören oder gegebenenfalls zu zerstören. Gleichzeitig schützt man die eigene Informationsinfrastruktur vor feindlichen Angriffen. Information ist in Krisensituationen nicht mehr nur ein das militärische Vorhaben unterstützendes Mittel zum Zweck, sondern wird zunehmend ein konfliktentscheidender Machtfaktor. Ebenfalls geht es um die eigene Informationsdominanz, die beispielsweise den Vorteil schnelleren Handelns und Entscheidens mit sich bringt (sei es im militärischen oder auch wirtschaftlichen Fall). Information wird also auch als Waffe und Schutztechnologie definiert. Die Waffe und Schutztechnologie Information wird aber im Vergleich zu anderen Waffen, die meist auf die physische Zerstörung abzielen, schon lange vor einer eigentlichen Kriegshandlung eingesetzt. Die ausgeprägteste Form der *Information Warfare* bestünde darin, es gar nicht erst zu einem Einsatz „klassischer Kriegswaffen" kommen zu lassen, d.h. den Feind zu besiegen, bevor der eigentliche Kampf begonnen hat. Dadurch ergibt sich beispielsweise die Gelegenheit, einen sich anbahnenden Konflikt schon vor der Eskalation zu lösen, bzw. dem Gegner durch geschickte (Ver)Handlung (bspw. dem Gegner Informationen vorzuenthalten oder zuzuspielen) den eigenen Willen „aufzuzwingen".

Ein weiterer Faktor ist, daß die informationstechnische Überlegenheit das Abschreckungspotential eines militärisch überlegenen Staates oder Bündnisses verstärkt.

Ebenfalls ist zur Konflikteindämmung nicht nur militärische Stärke vonnöten, auch eine schnelle Kommunikation zwischen den Instanzen oder Bündnispartnern erleichtert das gemeinsame Handeln und den Entscheidungsprozeß zur Konfliktlösung. Ist jedoch keine gleichwertige Informationsgrundlage der Bündnispartner vorhanden, kann aus der Chance eine Gefahr werden. Alle diese Vorteile sind nur mit einer Internationalen Informationsinfrastruktur nutzbar. Deswegen sind gerade hochtechnologisierte Länder in der Lage, in der Welt-

[1] § 5 der Staff Instructions des Chairman of the Joint Chiefs vom 2.2.1996, zit. nach Haeni (1997).

politik eine Vormachtstellung einzunehmen. Die zunehmende Abhängigkeit von einer globalen Informationsinfrastruktur macht diese Staaten aber auch verwundbar. In der Literatur werden die verschiedenen Einteilungen der Formen von *information warfare* vorgestellt. Martin C. Libicki unterscheidet in seinem Buch *What Is Information Warfare?*[2] folgende Erscheinungsformen:

Command-and-Control Warfare

Command-and-Control Warfare (C2W) setzt Gewalt gegen konkrete Ziele ein, jeweils mit der Absicht, den „Kopf" einer Einheit vom „Körper" zu trennen, was – um im Bild zu bleiben – durch direkte Schläge auf den Kopf sowie durch Durchtrennen des Halses erfolgen kann. Die Idee, eine Armee kopf- und damit führungslos zu machen, ist ebenso alt wie effizient. Man unterscheidet zwischen zwei Arten des „Trennens", Antihead und Antineck.

War in vergangenen Kriegen der Befehlshaber noch notwendigerweise an das Schlachtfeld gebunden, ist seine Anwesenheit durch zunehmende technische Weiterentwicklung weniger wichtig geworden. Zudem ist an die Stelle des Generals, der mit einem Feldstecher auf dem Hügel steht, die Kommandozentrale getreten, die als solche auch identifiziert werden kann und deren Zerstörung einen herben Rückschlag für ein Heer bedeuten kann. Diese Zerstörung kann nun einerseits durch direkte Anwendungen von Bomben erfolgen, eine Kommandozentrale kann aber auch durch Strahlenbeschuß, Durchtrennen von Leitungen oder mittels Computerviren betriebsunfähig gemacht werden.

Momentan spricht jedoch alles dafür, daß auf lange Sicht die Kommandozentralen zunehmend geschützt und getarnt werden bzw. die äußeren Merkmale verkleinert werden und verschwinden. Kommandozentralen können – auf Kosten der Mobilität – durch Tiefbunker geschützt und Netzwerke dezentralisiert werden. Unterirdische Aggregate kombinieren Stromversorgung und Anonymität. Selbst mit immer stärker werdenden Detektoren wird es dem Angreifer schwerfallen, immer aufs Neue den Kopf zu zerstören und er wird sich dem ebenso wichtigen Verbindungsglied zwischen Haupt und Körper zuwenden:

Die elektronischen Kommunikationsmittel wären in dieser Metapher sozusagen die Nervenstränge, welche die Signale vom Kopf zum Körper schicken. Um diese erfolgreich zu durchtrennen, ist die Kenntnis der Kommunikationswege vonnöten. Für gewöhnlich genügt es, die wichtigsten Knotenpunkte zu zerschlagen, um ein Netz lahmzulegen.

---

[2] Libicki (1995).

Wichtig in diesem Zusammenhang ist (für den Verteidiger) das Konzept der Redundanz: Je höher die Anzahl der Kanäle, durch die man eine Nachricht schickt, desto höher die Wahrscheinlichkeit, daß sie am anderen Ende ankommen wird. Andererseits wird ein Strang aus 100 toten Kabeln das eine verstekken, welches für den Informationsverkehr wichtig ist. Redundanz hat eine leichte Schwächung der Leistung des Systems insgesamt zur Folge, bei erhöhter Schutzwirkung vor feindlichen Eingriffen. Eine weitere Gegenmaßnahme besteht im Aufsplitten von Informationsübermittlungseinheiten. Generell hängt natürlich der Erfolg einer Attacke vom Entwicklungsstandard des Verteidigers ab, sowie von seinem Willen, den nötigen Aufwand zu betreiben. Ein kopfloser Körper wird die Orientierung verlieren, könnte aber auch wild und unkoordiniert handeln.

Intelligence-Based Warfare

Intelligence-Based Warfare (IBW) bedeutet, daß Informationen über das Kriegsgelände und seine bekämpfenden Objekte unmittelbar in militärische Operationen eingebracht werden. D.h., daß immer verläßlichere Sensoren Informationen in Echtzeit an entsprechende Waffensysteme liefern, um die Trefferquote zu erhöhen.

Man unterscheidet zwischen offensiver IBW und defensiver IBW. Im *offensiven IBW* geht der Trend dahin, daß die verarbeiteten Informationen und die Waffensysteme physisch voneinander getrennt werden. Die erfolgversprechende Zukunft liegt in der elektronischen Vernetzung der einzelnen Komponenten (Networking). Durch mehrere auf das Gelände verteilte Sensoren kann eine erfolgreiche Zerstörung der Ziele erreicht werden. Ziel der IBW ist auch, die Befehlshaber vor unangenehmen Überraschungen zu schützen, ihnen die möglichst frühzeitige Erstellung von Schlachtplänen zu ermöglichen und durch besseren Informationsfluß den Gegner zu überraschen.

Defensiver IBW beschäftigt sich mit der Störung feindlicher Sensoren und Waffensystemen. Defensiver IBW arbeitet z.B. mit dem Einsatz billiger Sensoren, die es nicht lohnt, mit teuren Raketen zu zerstören oder vor Aufklärungsflugzeugen durch Störung (eine der wichtigsten Möglichkeiten künftiger Verteidigung) bzw. „Unsichtbarmachen" zu schützen. Computergestützte Sensoren können mit spezieller Software (z.B. Hacker-Kriegsführung) außer Gefecht gesetzt werden.

Die Aussicht auf Sieg ist trotz technischer Überlegenheit nicht gewiß. Low-Tech-Kriegsführer haben noch immer die Möglichkeit, sich vor High-Tech-

Gegnern effizient zu schützen. Informationstechnologie ist bis heute eben nur eine wertvolle Unterstützung auf der Suche nach Zielen, wird aber weiterhin den Soldaten am Boden nicht ersetzen können.

Electronic Warfare

Electronic Warfare (EW) widmet sich der Bekämpfung der feindlichen Kommunikation. Sie besteht aus zwei Teilgebieten: Bei der radioelektronischen Kriegführung versucht man, die physischen Grundlagen für die Übertragung von Daten zu bekämpfen. Mittel hierzu sind der Antiradar und die Antikommunikation. Der Antiradar ist im Prinzip ein Störsender, der jedoch auch immer in Gefahr läuft, selbst zum Ziel zu werden. Digitale Radare können Ziele erkennen, bevor Störsignale vom Gegner ausgesendet werden. Die Antikommunikation beinhaltet beispielsweise einen häufigen Frequenzwechsel bei der Funkübertragung von Informationen. Auch hier findet eine zunehmende Digitalisierung und Dezentralisierung statt.

Das zweite Teilgebiet der EW ist die kryptographische Kriegführung. Diese beschäftigt sich hauptsächlich mit der Verschlüsselung der eigenen und der Entschlüsselung fremder Daten. Neue Chiffrierungstechniken in privater wie in öffentlicher Kodierung auf digitaler Ebene werden in Zukunft durch parallele Verwendung mehrerer Techniken ein fast 100%iges Maß an Sicherheit bieten können. Die neuen Codes können von keinem Computer mehr gehackt werden. Falls sie dennoch auf dem Weg dekodiert und gelesen wurden, so kann dies der Empfänger feststellen.

Hacker Warfare

Einen weiteren, an Wichtigkeit stets zunehmenden und nicht minder umstrittenen Aspekt des *Information Warfare* stellt der *Hacker Warfare* dar, wobei auch dieser Begriff ein weites Feld von Kriegshandlungen umspannt, denen gemein ist, daß sie sich auf digitalen Schauplätzen vollziehen. Hierbei ist keine physische Präsenz des Angreifers in unmittelbarer Zielnähe vonnöten, die Attacke geht gewaltlos vonstatten und obwohl im Falle eines Vorteils die attackierende Partei, was den Transfer von Ideen, Informationen – selbst Geldfluß – angeht, mitunter aus dem Vollen schöpfen kann, ist der aufzubringende finanzielle Aufwand (beim Angriff, nicht unbedingt bei der Verteidigung) vergleichsweise gering.

Gekämpft wird nicht mit teuren Sprengköpfen, geschossen wird mit Bits und Bytes, mit Viren und Würmern, also Programmen, die naturgemäß reduplizierbar und modifizierbar sind. Die Relevanz dieser kriegerischen Disziplin steht also außer Frage und gewährleistet ein Interesse an und die Auseinandersetzung mit den Facetten des HW von unterschiedlichsten Seiten. Für uns von Interesse ist in erster Linie der militärische HW, der militärische Systeme gezielt durch Hacker-Attacken infiltriert.

Die Möglichkeiten und Mittel der Aggression sind äußerst vielschichtig und reichen von kleinen Schnüffeltools, die etwa Paßwörter in Erfahrung bringen, bis zu Trojanischen Pferden, die, einmal vom gegnerischen System angenommen, dieses „von innen heraus" zu Fall bringen. Selbstverständlich haben digitale Attacken nicht immer den totalen Zusammenbruch des gehackten Systems zum Ziel, vielmehr weiß man, daß es rentabler ist, die Kuh ordentlich zu melken, bevor man sie schlachtet.

Information and intelligence collection ist die Hauptmotivation für Hacker-Aktivitäten im öffentlichen wie im privaten Sektor.

Der Schwachpunkt eines jeden überhaupt zu hackenden Computersystems liegt in seiner Vernetzung. Ein geschlossenes System muß keine Attacken von außen befürchten, aber auch zwangsläufig sehr begrenzt bleiben, was seine Operationsmöglichkeiten betrifft. Sobald eine Möglichkeit der Kommunikation mit der Außenwelt eingerichtet wird, ist das System theoretisch angreifbar.

Mit der zunehmenden globalen Vernetzung und dem erhöhten Stellenwert des Computers an sich innerhalb der letzten Jahre gewinnt auch die Kriegführung mit und um den Computer an Relevanz. Die Anzahl der (bekanntgewordenen) Hacker-Aktionen steigt stetig an, die entstandenen Schäden belaufen sich auf Milliarden von Dollar.

In diesem Zusammenhang stellt das Internet einen wunden Punkt dar, der zudem noch, omnipräsent und von Natur aus so öffentlich wie nur irgend möglich, potentiell weniger wohlmeinenden Instanzen in Ermangelung ernsthafter Sicherheitsvorkehrungen die Masse der Informationen auf dem sprichwörtlichen Silbertablett kredenzt.

Für erklärte und rentable Lieblingsziele von digitalen Eindringlingen sind die Übergriffe natürlich keine Neuigkeit mehr. Man hat das Problem erkannt, für gewöhnlich stellt man eine eigene Division von Computersicherheitsexperten zusammen. Die Kriegserklärung ist angenommen und fortan testen beide Seiten sich und ihre Fähigkeiten aneinander. Das System wird ständig erforscht – von beiden Seiten – , Schwachstellen gefunden und genutzt, von Seiten der Verteidiger wieder geschlossen, neue Schwachstellen ausfindig gemacht usw. Durch stete Attacken wurden die Systembetreiber allerdings zur Wachsamkeit

gerufen, die Defensivspezialisten werden von ihren Gegnern quasi mittrainiert, Kodierungssysteme immer ausgereifter. Die Standards steigen so auf beiden Seiten, Hacker-Attacken nehmen nicht nur an Frequenz zu, sie werden auch immer ausgefeilter.

Libicki berichtet von einem Test, der zeigte, daß ein einigermaßen befähigter Hacker ohne übertriebenen Aufwand Superuser-Status in einer „überraschend hohen Anzahl" der vom DoD benutzten Computersysteme erreichen kann[3]. Wenig überraschend für die meisten von uns, für das Department of Defense durchaus bedenklich und ein Grund mehr, die Entwicklungen nicht zu vernachlässigen.

Die Hacker-Angriffe haben auch Auswirkungen auf die Nerven des Gegners. Wie gewaltsame Terroranschläge kommen die Attacken oft unverhofft, sind schnell vorbei und können beträchtlichen Schaden hinterlassen. Zwar können, falls die Systemadministratoren nicht schlafen, Sicherheitslücken nach einer Attacke wieder geschlossen werden, dennoch ist man vor wiederholten Angriffen nie wirklich sicher. Ebenso wie ein Terroranschlag kann ein großangelegter Hack auch sehr gut als Drohmittel eingesetzt werden, entsteht doch für die Attackierten ein erheblicher finanzieller und zeitlicher Aufwand zur Schadensbekämpfung.

Argumente gegen den massiven Einsatz von Hackerarmeen sind für gewöhnlich moralischer Natur, da gerade unter Computerexperten das Hacken oft verurteilt und als verwerflich betrachtet wird. Da in Kriegszeiten jedoch derartige Vorbehalte deplaziert wirken und ein Angriff auf ein gegnerisches militärisches Computersystem sicher nicht weniger moralisch ist, als Bombenhagel auf Getreidefelder prasseln zu lassen, muß man sich nach anderen Gründen umsehen und landet bei dem Einwand, daß beispielsweise eine Nation wie die USA in den meisten Fällen weit mehr von ihren Computersystemen abhängig sein wird als ihr Gegner und somit besser nicht mit Steinwürfen auf das eigene Glashaus aufmerksam machen sollte.

„Information Warfare: A Two-Edged Sword" heißt denn auch der Titel einer RAND-Studie zum Thema, an deren Ende das Resümee steht: „Zusammengefaßt kann man sagen, daß die US-amerikanische Heimat (US-homeland) nicht länger ein sicherer Zufluchtsort gegen äußere Angriffe sein wird."[4]

Und: Ca. 60% der Doktoranden, die in den USA in computer science and security promovieren, sind Angehörige fremder Staaten, 2/3 davon aus islamischen Ländern oder Indien.

---

[3] Ebd., S. 59.

[4] RAND Research Review 1999.

Economic Information Warfare

Economic Information Warfare setzt sich aus zwei Teilbereichen zusammen, der Informationsblockade und dem Informationsimperialismus.

Während unsere Gesellschaft sich vom Materiellen zum Virtuellen hinbewegt, wird die Kontrolle von Informationen und ihrem Fluß umstrittener und wichtiger. „Information ist Wissen und Wissen ist Macht"[5].

Eine Nation vom Zugang zu Informationsquellen jeglicher Art abzuschneiden, wäre verheerend für deren Ökonomie; eine Nation, die in der Lage dazu wäre, das zu tun, würde eine deutliche Machtstellung einnehmen und ein unschätzbares Druckmittel zur Verfügung haben.

Informationsblockade kann physikalischer wie elektronischer Natur sein. Drähte, Kabel und Antennen können zerschnitten oder zerstört, Transmitter mit Mikrowellen bestrahlt oder gejammt werden. Schwierig ist es, Direktübertragungssatelliten im Weltall zu blockieren, wenngleich auch viele der Institutionen angreifbar sind, die geosynchrone Satelliten mit Informationen füttern.

Während nach und nach alle Nationen abhängiger vom Informationsfluß werden, bleibt abzuwarten, wie sich diese Disziplin der Kriegführung entwikkeln wird.

Von *Informationsimperialismus* spricht man u.a. in Zusammenhang mit starken Industrie- und Marktzweigen. Je stärker das bereits existierende Fundament, desto größer die Chance, den Informationsvorsprung wiederum für innovative Neuerungen und Problemlösungen nutzen zu können, was in einem erneuten Vorteil resultiert, der gegen die Konkurrenz in der nächsten Runde ausgespielt werden kann. Natürlich kann man einer Partei nur schwer verbieten, die erarbeiteten Vorzüge voll auszuschöpfen und auch bei langjährigen Marktführern eines Sektors mag man nicht zu vorschnell mit dem Imperialismusvorwurf winken. Gefährlich wird es, wenn diese Vormachtstellung durch gezielte Repressionen gegen andere Parteien forciert und diese dadurch „kleingehalten" werden.

Es wird hier bewußt der Begriff „Partei" gebraucht, da der Informationsimperialismus weniger ein nationales Problem, sondern zunehmend von Interessenverbänden und Konzerne multinational ausgeübt wird. Die Grenzen zwischen „militärisch" und „zivil" verschwimmen, Firmen verlieren an nationaler Identität, der Handel des ausklingenden Jahrtausends ist kein Wettrennen zwi-

---

[5] In der Army überall bekannter Spruch, den der stellv. Verteidigungsminister Emmett Paige jr. am 30 Juli 1996 zum ersten Mal in einer Rede am Armed Forces Staff College in Norfolk, Virginia benutzt haben soll. Veröffentlicht vom *American Forces Information Service* vol 11, No 82, und in http//www.defenselink.mil/speeches/index.html

schen Nationen, sondern zwischen global handelnden Unternehmen. Selbst in Japan und anderen asiatischen Ländern, wo noch weitgehend national operiert wird, beginnt man sich in dieselbe Richtung zu bewegen.

Cyberwarfare

Von allen Gesichtspunkten des IW entzieht sich der *Cyberwarfare* am stärksten einer deutlichen Klassifizierung.

Bislang noch hauptsächlich im Raum der Spekulationen und Fiktion angesiedelt, wird er eher gedacht, als geführt, von Science-Fiction-Autoren und Kriegsspezialisten gleichermaßen. Einmal mehr sind die theoretischen strategischen Erwägungen der realen Entwicklung auf diesem Sektor voraus. Viele der Teilaspekte des CW werden Spekulationen bleiben, sollen hier aber dennoch kurz vorgestellt werden.

Informationsterrorismus ist eine Untergruppe des *Hacker Warfare* (s.o.); der Einsatz von Hackern, nicht mit dem Ziel allerdings, ein feindliches Computersystem zu zerstören, sondern um es auszubeuten im Hinblick auf Fakten, die bestimmte Individuen angreifbar, erpressbar machen. Solche Daten liegen in medizinischen und staatlichen Datenbanken parat, sie enthalten Angaben über Gesundheitszustand, Bildungsstand, Vorstrafen, Anschaffungen u.v.m., nahezu alle Files werden in Computern eingelesen und sind auch zunehmend über Netzwerke zugänglich.

Im Gegensatz zu den weiter oben unter *Hacker Warfare* genannten syntaktischen Vorgehensweisen wird bei *semantischen Attacken* das System weder ausgebeutet noch zum Absturz gebracht, vielmehr wird es so modifiziert, daß es – natürlich unbemerkt vom Betreiber – mit falschen Informationen arbeitet und aufgrund dessen solche wieder generiert. Die Funktionsfähigkeit des Systems wird daher nicht beeinträchtigt – es funktioniert so „gut" wie vorher, nur unter anderen – falschen – Voraussetzungen. Die Implikationen liegen auf der Hand; ein solches System würde beispielsweise im Konfliktfall modifizierte – also falsche – Signale von bspw. zielsuchenden Sensoren bekommen, diese veränderten Parameter richtig verarbeiten und so die falsche Entscheidung treffen.

Im Gegensatz zu den realen militärischen Kriegsschauplätzen mit deren Schrecken und Verlusten ist man mit *Simula Warfare* in der Lage, ganze Kriege mit Hilfe immer überzeugenderer Simulationen durchzuspielen. Es ist auch möglich, Waffen und Sensoren in echter Umgebung mit falscher Munition zu testen.

Die Idee, daß echte Schlachten nach und nach durch Simulation ersetzt werden können, ist eine sympathische, aber wenig wahrscheinliche. Viele Aspekte einer Auseinandersetzung lassen sich schwer simulieren, selbst wenn beide Seiten alle Informationen über Strategien, Heermasse etc. zur Verfügung stellen würden. Leider sieht es danach aus, als würde *Simula Warfare* den echten Krieg nicht allzu bald ablösen.

Der *Gibson Warfare* ist benannt nach William Gibson, Science-Fiction-Autor und Erfinder des Matrix/Cyberspace, vorgestellt in seiner *Neuromancer*-Reihe. Der Cyberspace ist hier eine virtuelle Welt, in der sich die Figuren, ihre Körper, über Neuro-Interfaces eingestöpselt in Computerterminals, die Realität zurücklassend, via Simulacrum frei bewegen können. Solche Konstrukte, man kann sie auch Agenten nennen, beinhalten Eigenschaften und Persönlichkeitsmerkmale des Users und repräsentieren seine Person in der virtuellen Welt.

In der Realität werden bereits Agenten entwickelt, die, auf Software-Basis und mit den Vorlieben eines Benutzers ausgestattet, etwa für ihn im Internet Reisen buchen oder Bücher kaufen könnten, während dieser seine Zeit besser nutzen kann.

Was die Anwendung solcher virtuellen Agenten und überhaupt der künstlichen Intelligenz (KI) in kriegerischen Handlungen angeht, so ist auch hier vermutlich die Imagination der Realität voraus, allerdings sollen schon Bomber mit ähnlichen, quasi-intelligenten Programmen bestückt worden sein, welche die Steuerung und Attacken voll übernehmen.

Psychological Warfare

Psychological Warfare umfaßt den Gebrauch von Informationen „against the human mind“[6]. Es gibt fünf Kategorien des *Psychological Warfare*:

- Operationen gegen nationale Interessen,
- Operationen gegen das nationale Bestreben
- Operationen gegen gegnerische Befehlshaber/ Führer
- Operationen gegen Truppen
- Operationen innerhalb kultureller Konflikte

Es gibt also während des Krieges den sogenannten „counter will“ einer Nation, der einen psychologischen Krieg über die Bildübertragung führt. Denn es ist letztendlich das Ziel jedes militärischen Eingreifens, den Willen und die Ausdauer des Gegner zu brechen.

---

[6] Libicki (1995), S. 35.

Bei einem Einsatz in Somalia zum Beispiel starben neunzehn „US Rangers" und CNN zeigte damals, wie Somalier die toten Körper der Amerikaner über die Straßen schleiften. Wohl ähnlich wie während des Vietnam-Krieges spielte auch hier der Einfluß auf das Publikum in Amerika eine große Rolle. Denn das Ergebnis dieser Bildübertragung war, daß die US-Einheiten sich aus dem Land zurückzogen und der somalische „clan leader" Mohammed Aidid als Sieger in einem nicht von ihm geführten Information War hervorging. Der Druck der Bevölkerung auf die Regierung schien das bewirkt zu haben, denn die Fernsehbilder nahmen den Zuschauern den Glauben, für eine gute Sache zu kämpfen. Vor allem standen diese Bilder in totalem Widerspruch zu den offiziellen Beteuerungen der Politiker und des Militär.

Über einen *Direct Broadcast Satellite* (DBS) fällt – wie Libicki erläutert – die Zensur weg und dieser ist jedem zugänglich. In Nordamerika existiert DBS schon seit 1994. Es bietet sich für jede Völkergruppe, jede Nation die Möglichkeit, vierundzwanzig Stunden am Tag Nachrichten an die Zuschauer zu richten.

Während des Golfkrieges machten US-Soldaten von psychologischen Methoden Gebrauch um den Willen des irakischen Volkes zu schwächen.

> Im Golfkrieg haben die Koalitionsstreitkräfte viele Iraker davon überzeugt, daß sie länger leben würden, wenn sie ihre verwundbaren Fahrzeuge verlassen. Diese Überzeugungsarbeit wurde unterstützt durch Waffen, die eben solche Fahrzeuge während der Kämpfe zerstörten. [7]

Man kann also mit Einschüchterungsversuchen und dem geschickten Ausnutzen der Todesangst des Gegners einen Krieg bestimmen. Der offene „Psychological War" würde dann eintreten, wenn die Drohungen oder Provokationen über Fernseh-/Computerbilder den einzelnen militärischen Truppen des Gegners zugänglich werden würden: „Was würde passieren, wenn man den Fahrern mitteilen könnte, daß sie geortet worden sind und gleich zum Ziel eines tödlichen Angriffs werden, wenn sie nicht selbst das Fahrzeug unbrauchbar machen?"[8]

Weiterhin ist es notwendig, so viele Informationen wie möglich über die Soldaten zu sammeln. Diese Datenbeschaffung ist in Industrienationen durch computergespeicherte persönliche Angaben einfacher als z.B. in unterentwikkelten Ländern.

Die Operationen gegen die militärische Führung sind dann erfolgreich, wenn der Feind mit falschen strategischen Informationen getäuscht wird.

---

[7] Ebd., S. 39.

[8] Ebd., S. 40.

Libicki spricht außerdem den sogenannten „Kulturkampf" an, wobei er hier auf Samuel Huntingtons *The Clash of Civilization*[9] anspielt. Hierbei geht es in erster Linie um den westlichen Einfluß – zumeist der USA – auf andere Gesellschaften. So beklagen die Franzosen und Kanadier den „US cultural export"[10]. Und es ist nicht nur der Export von Produkten, sondern auch der ideologische: „Aber die Politik der USA ist es, die politische Kultur der USA (z.B. Mehrheitsregierung, Minderheitenrechte) zu exportieren und in Übersee einzuführen; wenn man von den Handelsregeln absieht, schweigt die Politik strenggenommen ausnahmslos über andere kulturelle Einflüsse."[11]

Ein Krieg kann also ganz entscheidend über Medien und den kalkulierten öffentlichen Auftritt der Verantwortlichen bestimmt werden. Es ist heute im Zeitalter von Information Warfare nicht mehr möglich, die Greuel des Krieges offen darzulegen. Die Medienmacher sind gezwungen, sich den rigorosen Zensuren des Angreifers und des Gegners zu beugen und bereits ausgewähltes Material zu präsentieren.

Gary Shepard berichtete für ABC live aus dem El-Rashid Hotel in Bagdad, als die ersten amerikanischen Bomben fielen, und er kommentierte dieses „Ereignis": „Es ist das größte Feuerwerk, das ich je sah. Das ist wie Silvester, es ist phantastisch."[12]

Neue Herausforderungen für die Sicherheitspolitik

Um den Gefahren entgegenzuwirken, welche die Abhängigkeit von der Technologie mit sich bringt, muß sich die Sicherheitspolitik der neuen Herausforderungen klar werden:

Am gefährlichsten erscheinen die Möglichkeiten der Daten- und Nachrichtenmanipulation, sei es in verdeckter oder öffentlicher Form. Gezielte Falschinformation oder Meinungsäußerung können nach Belieben gestreut oder verhindert werden. Für kleinere Staaten ist es wesentlich günstiger und effektiver, in ihr elektronisches Netz zu investieren, als ihr Militärpotential aufzubauen. Ein weiteres Problem ist, daß der Angreifer kaum auszumachen ist, sogar der Angriff selbst oftmals erst spät entdeckt oder als solcher erkannt wird. 1996, in einer Testreihe von Angriffen auf die Rechner des US-Verteidigungsministeri-

---

[9] Huntington (1996).

[10] Libicki (1995), S. 46.

[11] Ebd., S. 47.

[12] Schöner neuer Krieg. In: *Spiegel Special* Nr. 1/1995, S. 91.

ums durch die Defense Information Agency wurden nur vier Prozent der Angriffe als solche erkannt.

Es werden neue Akteure (z.B. nicht-staatliche Organisationen, Wirtschaftsimperien) auftreten, die Staaten herausfordern können. Unkonventionelle Kriegführung wird in diesem Zusammenhang die Regel sein. Kleine nicht-staatliche Organisationen (z.B. Terrorgruppen) können ihre Interessen in kürzester Zeit über eine große räumliche Distanz international zur Geltung bringen.

Politische und geographische Grenzen sowie nationale Souveränität verlieren an Bedeutung für die Kriegführung. Es gibt kein Staatsterritorium mehr, das sich im Falle eines gewaltsamen Konfliktes mit militärischen Mitteln verteidigen könnte.

Vormals klare Abgrenzungen zwischen verschiedenen Konfliktformen verwischen zusehends: Konflikte finden ohne formale Kriegserklärung statt, staatlich gelenkte/unterstützte Aktionen (auch Terrorakte) lassen sich oftmals kaum von nicht-staatlichen unterscheiden; so ist auch militärisches nicht immer von kriminellem Handeln abzugrenzen, Bürgerkriege bekommen den Charakter zwischenstaatlicher Konflikte und umgekehrt, offene Aggression vermischt sich mit verdeckter Repression. Das zukünftige Konflikt- und Kriegsbild wird weitgehend unklar und die Übergänge zwischen verschiedenen Formen der Auseinandersetzung („Blauhelmeinsätze"/Kampfeinsätze) werden fließend sein.

Zivile Entwicklungen werden zunehmend militärisch genutzt (spin-in, Kommerzialisierung, breite Verfügbarkeit, Kostengesichtspunkte). Dies trägt zur Vermischung der Konfliktformen bei. Auch läßt die verstärkte Kommerzialisierung militärischer Systeme vermuten, daß viele Länder und Akteure dazu in der Lage sein werden, diese technologischen Entwicklungen militärisch nutzbar zu machen. Technologietransfer wird nicht zu vermeiden sein. Zu bedenken ist, daß sich insbesondere Länder, die traditionell nicht dazu in der Lage sind, erstklassige Streitkräfte aufzustellen, von Investitionen in Informationstechnologien einen disproportionalen Effekt versprechen können.

Im Rahmen aller Konflikte – sieht man von dem „großen Krieg" ab – wird auf Seiten des Westens eine nur geringe Kollateralschadensakzeptanz anzunehmen sein. Dieses Element politischer Kultur wird durch Fernsehbilder aus dem Konfliktgebiet noch verstärkt („CNN-Effekt"). Mit der Zunahme von Verlusten beim Gegner, insbesondere unter der Zivilbevölkerung, wird im Falle begrenzter Konflikte die innenpolitische Akzeptanz und Unterstützung für den Militäreinsatz sinken. Konfliktlösung, auch durch militärische Intervention, wird abhängig vom Informationseinfluß auf die Bevölkerung. Denn

nur solche Opfer beeinflussen die öffentliche Meinung im o.a. Sinn, die auch, möglichst in der Form bewegter Bilder, sichtbar in Erscheinung treten. Deshalb ist es seit dem Golfkrieg ein wichtiges Element des *Information Warfare*, die Berichterstattung durch Bildjournalisten und Fernsehkamerateams – auch der eigenen Seite – gezielt zu kontrollieren.

Gerade die USA setzen wie kaum ein anderes Land auf die Nutzung von Informationstechnologien. Dies trifft auch und gerade auf den militärischen Bereich zu. Die USA können die eigene Sicherheit nur gewährleisten, wenn sie, wie oben erwähnt, die Technologieforschung weiter fördert. Deshalb investieren sie wie kein anderes Land in ihren Verteidigungshaushalt, mit einem deutlichen Schwerpunkt auf der Anschaffung von elektronischen Ausrüstungen.

Es wäre eine Illusion, anzunehmen, daß Kriege sich demnächst unblutig auf dem Bildschirm eines Computers entscheiden werden. Letztendlich wird es in Krisengebieten und -zeiten immer zu einer Entscheidung am Boden kommen müssen. Joseph S. Nye jr. und William A. Owen nehmen diesbezüglich kein Blatt vor den Mund: Die ganze Medien- und Kommunikationstechnologie diene letztlich dem Ziel „tödliche Gewalt mit größerer Geschwindigkeit, Reichweite und Präzision einzusetzen".[13] So auch im Kosovokonflikt, in dem die UCK nach einiger Zeit soweit von den Westmächten ausgerüstet war, um den Serben einen Kampf am Boden aufzwingen zu können. Eine Woche später kam ein Friedensangebot von Milosevic.

Benutzte Literatur

Haeni, Reto E.: Information Warfare – an Introduction. Washington 1997.

Huntington, Samuel: The Clash of Civilization. New York 1996; dt. erschienen: Der Kampf der Kulturen: die Neugestaltung der Weltpolitik im 21. Jahrhundert. München 1996.

Libicki, Martin C.: What is Information Warfare? US Government Printing Office 1995.

Nye, Joseph S. jr. und Owen, William A. America's Information Edge. In: *Foreign Affairs*, März/April 1996

RAND Research Review 1999.

Schöner neuer Krieg. In: *Spiegel Special* Nr. 1/1995.

The Information Edge. In: *Foreign Affairs*, März/April 1996.

http//www.defenselink.mil/speeches/index.html

[13] Nye/Owen 1996, S. 23.