Georg Schöfbänker

Von PLATO zur NATO[1]

Erkenntnis, Wissen und Phantasien über den Cyber- und Informationskrieg. Auf der Suche nach neuen Bedrohungen, Zusammenhängen und Denkmustern nach dem Ende des Kalten Krieges.

Einführung

Seit dem Ende des Kalten Krieges hat die westliche Staatengemeinschaft einen "realen" klassischen Krieg mit Tausenden getöteten Kombattanten geführt, obgleich es kein Krieg zwischen Nationalstaaten war. Gemäß dem Völkerrecht handelte es sich dabei um eine "Polizeiaktion" von Mitgliedern der Vereinten Nationen unter der Führung der USA gegen Irak, der zuvor Kuwait überfallen, Verbrechen an der Zivilbevölkerung begangen und Raketen auf Israel gefeuert hatte. Der Luftkrieg begann am 17. Januar 1991 und dauerte bis zur Bodenoffensive am 24. Februar, also insgesamt etwa fünf Wochen. Die Bodenoffensive dauerte nur vier Tage, nämlich bis zum 27. Februar, als ein Waffenstillstand geschlossen wurde. Kuwait wurde von den irakischen Truppen befreit, Irak jedoch blieb politisch ungeschoren, Diktator Saddam Hussein an der Macht. Iraks Kernwaffenprogramm sowie die anderen Programme zur Herstellung von Massenvernichtungswaffen wurden nach und nach in ihrer vollen Tragweite erkannt; dabei handelte es sich um Projekte, die zuvor nicht durch "Signalaufklärung" (signals intelligence, SIGINT) wie etwa durch Satellitenaufklärung wahrgenommen wurden.

Kurz bevor dieser Text fertiggestellt wurde, führten Indien und Pakistan auf unterschiedlichen Entwicklungsstufen nahezu gleichzeitig zwölf Kernwaffentests durch, wobei im Fall von Indien ein echter Thermonuklearsprengkopf getestet wurde.

Ein nuklearer Rüstungswettlauf könnte in Südostasien stattfinden, wenn dieser nicht durch eine Entspannungspolitik und vertrauensbildende Maßnahmen abgewendet werden kann. Indien hat angekündigt, superschnelle Computerleistung zur Simulation weiterer Kernwaffentest einzusetzen, genauso wie dies die fünf etablierten und erklärten Kernwaffenmächte tun.

Der Fall des Golfkrieges wurde zum Paradigma der Einschätzung neuer Konfliktszenarien und darüber, wie Informationstechnologie (IT) hinkünftiges Schlacht-Management gestalten würde — im Original heißt es "Battle Management", aber um dem eigentlichen Wortsinn, auf den der davorstehende Jargon die Sicht verstellt, zum Durchbruch zu verhelfen, müßte es eigentlich "Management des Schlachtens" heißen. Seitdem sind insbesondere in Regierungs- und Militärkreisen der USA verschiedene Projektgruppen eingerichtet worden. Wie auch die strategischen Politikberater, die Sicherheitsberater des Präsidenten, der militärisch-industriell-strategische Komplex in Washington DC sowie nahestehende Denkfabriken setzen sie Neologismen und neue Akronyme in die Welt, etwa: Info(rmations-)Krieg(-s)(führung), Cyberkrieg(-sführung), Netzkrieg (-sführung), nachrichtendienstliche Kriegsführung (intelligence based warfare, IBW), elektronische Kriegsführung (EW), Revolution in militärischen Angelegenheiten (RMA), Revolution in strategischen Angelegenheiten (RSA), C2W (Kommando-und Kontrollkriegsführung — command and control warfare), C3I (Kommando, Kontrolle, Kommunikation und Aufklärung — command, control, communication and intelligence), C4I (Kommando, Kontrolle, Kommunikation, Computernutzung und Aufklärung — command, control, communication, computation and intelligence), C4I2 (Kommando, Kontrolle, Kommunikation, Computernutzung, Aufklärung

und Interoperabilität — command, control, communication, computation, intelligence and interoperability), HIC (Konflikte hoher Intensität — high intensity conflicts), LIC (Konflikte niedriger Intensität — low intensity conflicts), OOTW (nicht kriegsähnliche Operationen — operations other than war) und so weiter und so fort.

Allein die Tatsache, daß die Diskussion über diese Fragen die Expertenkreise des Pentagon verlassen und eine größere Öffentlichkeit in den Mainstream-Außenpolitikzeitschriften der USA erreicht hat (z. B. in Foreign Affairs), ist ein glaubwürdiger und zuverlässiger Indikator dafür, daß diese Debatte in den USA entweder bereits eine außenpolitisch-strategische Angelegenheit ist oder werden wird und daß diese Debatte nach Europa kommen wird. Es handelt sich dabei nicht nur um eine Debatte der militärischen Eliten der USA. Auch in schwedischen Verteidigungskreisen wurde eine Arbeitsgruppe über Informationskrieg eingerichtet, die RMA ist eine treibende Kraft bei der Neugestaltung der Out-of-Area-Einsätze der NATO und bei der Optimierung ihrer Feuerkraft; und die Russische Föderation ist ernsthaft besorgt darüber, daß möglicherweise zwischen einem informationskriegerischen Angriff und einer permanenten kulturellen Penetration der nationalen Identität, von Denkmustern, kultureller wie auch psychologischer Werte keine klar erkennbare Grenzlinie existiert.

Eine weitere Entwicklung ist seit Ende des Golfkrieges zu beobachten: Die Halbwertszeit außenpolitischer Theorien, von Hypothesen und Erklärungen für die in immer höherem Ausmaß und höherer Geschwindigkeit interagierende Welt nach dem Ende des Kalten Krieges, für das System der internationalen Beziehungen, für die Interaktionsmuster zwischen staatlichen, nichtstaatlichen und Nichtregierungsakteuren, für neue Wirkungsweisen und Lösungsmöglichkeiten von Konflikten, für Theorien über Vorherrschaft und Macht in der postmodernen internationalen Umgebung, für die Natur staatlichen Verhaltens im internationalen System, für die Zukunft von kriegsähnlichen Konflikten, für Ethnizität und Identität und deren Auswirkungen auf Konfliktentwicklungen, hat dramatisch abgenommen.

Seit Ende der achtziger Jahre tauchen eine Reihe von modischen Theorien auf, um die mögliche Zukunft des internationalen Systems sowie Hegemonie und Macht zu erklären: "Imperiale Überdehnung" (imperial overstretch) war der Versuch, den vermuteten Verlust an Einfluß seitens der USA auf der Weltbühne zu erklären. 1990 verkündete Präsident George Bush eine auf dem System der Vereinten Nationen, dem Völkerrecht und der fortschreitenden Demokratisierung von autoritären Regimen basierende "neue Weltordnung". Beim abschließenden diplomatischen Akt, der den Kalten Krieg in Europa offiziell beendete — der Pariser KSZE Konferenz von 19. bis 21. November 1990 — wurde die Sicherheit aller am KSZE-Prozeß beteiligten Staaten als "unteilbar" bezeichnet und hervorgehoben: "Die Sicherheit eines jeden unserer Länder ist unlösbar mit der Sicherheit aller anderen Staaten der Konferenz für Sicherheit und Zusammenarbeit in Europa verbunden."

Gleichfalls wurden Theorien, die das "Ende der Geschichte" verkündeten, ausgerufen, die dann 1993 von Huntington in seinem Artikel in Foreign Affairs durch das Konzept von einem "Kulturkampf" (clash of civilizations) als wahrscheinlichstes inner- und zwischenstaatliches Konfliktmuster abgelöst wurden, weshalb man wiederum der US-Führung und Hegemonie bedürfe. Dieses Konzept des Kulturkampfes von fundamentalistisch orientierten Schurkenstaaten, den meistgehaßten Feindbildern der US-Außenpolitik, paßt wiederum bestens zur Bedrohungswahrnehmung postmoderner subkonventioneller Terroristen mit Massenvernichtungswaffen. Ab Mitte der neunziger Jahre begannen die sich entwickelnden Theorien und Konzepte von Cyber- und Informationskrieg auf den Mainstream der US-Außenpolitik auszuwirken. Vom Standpunkt einer seriösen unabhängigen Analyse scheint es

nicht so bedeutend zu sein, im Detail zu untersuchen, wie Cyber- und Informationskrieg eine strategische Frage wurden; wichtiger ist zu untersuchen, ob diese nicht aus US-Perspektive zu einer selbsterfüllenden Prophezeiung werden könnten.

Die Frage ist, wie hyped man einen Hype? Wie kann man einen Schritt voraus sein, indem man die Regeln des Spiels verwendet? Der erste Hype könnte darin bestehen, die Konstruktion des Informationskrieges als den zentralen Zusammenhang und als die zentrale Sicherheitsbedrohung des 21. Jahrhunderts hochzustilisieren. Der zweite Hype könnte darin bestehen, die bereits bestehende US-Hegemonie im Mediengeschäft zur unkontrollierten Weiterverbreitung dieser Auffassung zu verwenden und damit selbsterfüllend und plausibel zu machen.

Aber Informations- und Cyberkrieg sind erst an der Schwelle, Realpolitik zu werden. Die bedeutendste politische und militärische Veränderung auf der nördlichen Halbkugel in den neunziger Jahren ist der Kollaps der bipolaren Welt des Kalten Krieges und das eXlargement der NATO in Richtung Osten. Johan Galtung hat diese als "größenwahnsinnige Realpolitik" bezeichnet. Die NATO wird sich sicherlich nach Osten erweitern, wird ihr Territorium, ihren potentiellen Raum für Interventionen, für friedenserhaltende, friedensschaffende und für Out-of-Area-Missionen vergrößern, sie wird das euroatlantische Leitmotiv des 21. Jahrhunderts sein. Nordamerika und Europa werden die wichtigsten militärischen, technologischen und ökonomischen Mächte zu Beginn des 21. Jahrhunderts sein. Das scheint sicher. Eine Folgenabschätzung der möglichen Auswirkungen von Cyber-, Informations- und Netzkrieg sollten vor diesem Hintergrund stattfinden. Die wichtigsten diesbezüglichen Fragen sind:

— Wie wird die Zukunft des internationalen Systems aussehen?

— Wie werden zukünftige Kriege aussehen? Werden es Konflikte zwischen Nationalstaaten im Sinn von Clausewitz und der "Fortsetzung von Politik mit anderen Mitteln" sein?

— Wie werden die zukünftigen Konfliktursachen aussehen? Werden es Konflikte über Ethnizität, auf der Suche nach nationaler Identität, sein? Wird es zu Konflikten entlang der Konfliktlinien von Kulturkampf zwischen der westlich-christlichen, der christlich-orthodoxen und der islamischen Welt kommen?

— Werden zukünftige gewaltförmige Konflikte hauptsächlich innerstaatlicher und regionaler Natur sein, wie jüngst in Ex-Jugoslawien, Afghanistan, Kambodscha, Ruanda und Somalia oder beim gegenwärtigen Kosovo-Problem?

— Wer wird in solchen gewaltförmigen zukünftigen Konflikten agieren? Die einzige verbliebene Supermacht, die USA, Mittelmächte oder subnationale Gruppen national-ethnischer Orientierung, Clans, Warlords, gewalttätige Banden, mit genügend leichten und mittelschweren Waffen ausgestattet, um einen Genozid wie in Bosnien oder Ruanda zu evozieren? Oder Ad-hoc-Koalitionen bereitwilliger Staaten oder die UN, die OSZE oder Militärallianzen wie die NATO?

Um es offen zu sagen: Es gibt keine leichten oder wahrscheinlichen Antworten auf diese Fragen, und wenn doch, so riskieren diese, eine recht kurzfristige theoretisch-prognostische Reichweite zu haben. Weiters muß die Frage gestellt werden, ob es sich bei den Konzepten von Cyber-, Informations- und Netzkrieg um Bottom-up- oder um Topside-down-Ansätze handelt.

Verwirrende Definitionen — Oder worum es geht

Cyber-, Informations- und Netzkrieg werden in der maßgeblichen US-Literatur als überlappende Synonyme verwendet.

Cyberkrieg

Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to "know" itself.[2]

Da die vorliegende Publikation den Artikel Der Cyberkrieg kommt! von John Arquilla und David Ronfeldt enthält (s. S. 24—56), scheint es nicht nötig, deren Definitionen hier ausführlich zu zitieren.

As an innovation in warfare, we anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century. […] In a deeper sense, cyberwar signifies a tranformation in the nature of war.[3]

Netzkrieg

Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt or damage what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. […] In other words, netwar represents a new entry on the spectrum of conflict that spans economic, political, and social, as well as military forms of "war." […]

Like other forms on this spectrum, netwars would be largely non-military, but they could have dimensions that overlap into military war. […] Other kinds of netwar may arise between governments and nonstate actors.[4]

Or to the contrary they may be waged against the policies of specific governments by advocacy groups and movements — e.g. regarding environmental, human-rights or religious issues.

Most netwars will probably be non-violent […]

Some netwars will involve military issues. Candidate issue areas include nuclear proliferation, drug smuggling and antiterrorism […][5]

Netwars are not real wars, traditionally defined. But netwar might be developed into an instrument for trying, early on, to prevent a real war from arising.[6]

Beide Autoren geben jedoch noch eine andere Definition über den Zusammenhang von Cyberkrieg und Netzkrieg: "What we term cyberwar will be an ever more important entry at the military end […] Netwar will figure increasingly at the societal end […]"[7] Kurz darauf heißt es: "The term netwar denotes an emerging mode of conflict (and crime) […] short of war, in which the protagonists use — indeed, depend on using — network forms of organization, doctrine, strategy, and communication."[8]

Und schließlich: "The netwar spectrum may increasingly include a new generation of revolutionaries and activists who espouse postindustrial, information-age ideologies that are just now taking shape. In some cases, identities and loyalities may shift from the nation-state to the transnational level of a global civil society"[9] (Hervorhebung vom Verfasser).

Des weiteren diskutieren Arquilla/Ronfeldt [10] "Netzwerk-Prinzipien" als eine Form sozialer Organisation abseits aller technischen Aspekte und kommen zu dem Schluß: "[…] netwar is not just about new technologies."

Informationskrieg

Arquilla/Ronfeldt weigern sich, den Begriff "Informationskrieg" zu definieren[11], da er zu breit und zu schmal sei, um angemessen sein zu können. Im Gegensatz zu dieser Position verwenden hochrangige US-Militärbehörden eine andere Sprache zur Beschreibung des Konzepts von Informationskrieg. Die nicht klassifizierten Doktrinen der Vereinigten Generalstabschefs (1996), die Joint Vision 2010, wie auch die Joint Doctrine for Command and Control Warfare, definieren Informationskrieg explizit und implizit. Die Joint Vision 2010 definiert Informationskrieg nicht explizit und verweist vorwiegend auf die militärischen Auswirkungen des Informationszeitalters:

> We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.
>
> Information superiority will require both offensive and defensive information warfare (IW). Offensive information warfare will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy an adversary's command and control capability, as well as nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers.
>
> There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead. Traditional defensive IW operations include physical security measures and encryption. Nontraditional actions will range from antivirus protection to innovative methods of secure data transmission. In addition, increased strategic level programs will be required in this critical area.[12]

Hingegen gibt die Joint Doctrine for Command and Control Warfare eine explizite Definition von Informationskrieg:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.[13]

In Joint Pub 3-13.1 werden Aspekte des Informationskrieges in einem breiteren Sinn gefaßt, sie enthalten ebenso psychologische Kriegsführung (PsyOp) sowie den Gebrauch der globalen Informationsinfrastruktur (GII). In diesem Dokument wird der Informationskrieg umfassender definiert und auch die Anwendung nicht-technischer und nicht-militärischer Mittel einbezogen. Die folgenden Tabellen mögen als semantische Raster zur Diskussion der US-Konzepte dienen:

Arquilla/Ronfeldt	Cyberkrieg	Netzkrieg	Informationskrieg
Konflikt-Niveau	hoch	mittel – hoch	—
Konflikt-Ursachen	nichtdefiniert	nichtdefiniert	—
Akteure	Nationalstaat	Nationalstaat militärisch Schurkenstaaten militärisch, paramilitärisch, „terroristisch"; NGOs „globale Zivilgesellschaft"	— Gesellschaft
Bedrohungs-wahrnehmung	alarmistisch	alarmistisch	—
Sub-Konzepte	Schlachtfeld gesteigerte Tödlichkeit Revolution in militärischen Angelegenheiten	Propaganda psychologische Kriegführung Medienkontrolle, „reflexive Kontrolle"	—
weitreichende Auswirkungen	Transformation der Natur des Krieges	„Kulturkampf" Transformation in der Anwendung von Propaganda und psychologischer Kriegführung	
Kanäle/Mittel	militärische und zivile Kommando- und Kontrollsysteme	Computer-Netzwerke Internet alle Medienkanäle	

Joint Pub 3-13[14] Joint Vision 2010	Informationskrieg. Kaum eine Unterscheidung zu nichtmilitärischen Anwendungen
Konflikt-Niveau	hoch; heiße und kalte Kriege
Konflikt-Ursachen	nichtdefiniert
Akteure	Nationalstaaten; Militär
außenpolitischer Design	„Power projection, enabled by overseas presence, will likely remain the fundamental strategic concept of our future force" (Joint Vision 2010, 4)
Bedrohungs-wahrnehmung	alarmistisch
Sub-Konzepte	„dominant battlespace awareness"; increased capability to kill; RMA; directed energy weapons (lasers); C2 warfare: „C2W is an application of IW in military operations and is a subset of IW." (Joint Vision 2010, I-4)
weitreichende Auswirkungen	Vollständige Transformation der Durchführung konventioneller militärischer Operationen
Kanäle/Mittel	Revolution in militärischen Angelegenheiten

Libicki erstellte in What is Information Warfare?[15] einen sehr umfassenden Definitionsraum, der die technisch-militärischen Aspekte des Schlachtfeldes genauso umfaßt wie kulturelle Aspekte. Wir zitieren diese Definitionen hier vollständig, um die Tragweite der Auswirkungen diskutieren zu können.

Form	Subtype	Is It New?	Effectiveness
C2W	Antihead	Command systems, rather than commanders, are the target.	New technologies of dispersion and replication suggest that tomorrow's command centers can be protected.
	Antineck	Hard wired communication links matter.	New techniques (e.g., redundancy, efficient error encoding) permit operations under reduced bitflows.
IEW		The cheaper the more can be thrown into a system that looks for targets.	The United States will build the first system of sensing systems, but stealth aside, pays too little attention to hiding.
EW	Antiradar	Around since WW II.	Dispersed generators and collectors will survive attack better than monolithic systems.
	Anticomms	Around since WW II.	Spread spectrum, frequency hopping and directional antennas all suggest communications will get through.
	Cryptography	Digital code making is now easy.	New code making technologies (DES, PKE) favor code makers over code breakers.
Psychological Warfare	Antiwill	No.	Propaganda must adapt first to CNN than to Ma-TV.
	Antitroop	No. DBS and Ma-TV.	Propaganda techniques must adapt to.
	Anti commander	No.	The basic calculus of deception will still be difficult.
	Kulturkampf	Old history.	Clash of civilisations?
Hacker Warfare	Yes.		All societies are becoming potentially more vulnerable but good home keeping can secure systems.
Economic Information Warfare	Economic	Yes.	Very few countries are yet that dependent on high bandwidth information flows.
	Techno-Imperialism	Since the 1970s.	Trade and war involve competition, but trade is not war.
Cyber-Warfare	Info-Terrorism	Dirty linen is dirty linen whether paper or computer files.	The threat may be a good reason for tough privacy laws.
	Semantic	Yes.	Too soon to tell.
	Simula-warfare	Approaching virtual reality.	If both sides are civilised enough to simulate warfare, why would they fight at all?
	Gibson-warfare	Yes.	The stuff of science fiction.

Von Software zu Soft Power — Oder auf der Suche nach neuen Bedrohungen?

"I'm running out of demons. I'm down to Kim Il Sung and Castro."

Der Vorsitzende der Vereinigten Generalstabschefs, Collin Powell, 1991 (nach dem Golfkrieg), vor dem US-Kongress.[16]

Es ist jedoch noch nicht klar, was die Henne und was das Ei war. Führte der Wegfall realer Bedrohungen am Ende des Kalten Krieges zu dieser Form von Cyber- und Informationskriegs-Enthusiasmus, dessen wir jetzt als treibende Kraft in Pentagon-Kreisen gewahr werden? Oder lief es eher anders herum, wie Friedrich Kittler[17] meint, und erweist sich womöglich die Computerindustrie als "empirische wie kriegerische Bande globaler Konzerne", die ihr letztes und möglicherweise (un-?)friendly Take-over — nämlich jenes des Pentagon selbst — vorbereitet? Verglichen mit den Erlösen aus militärischer Hardware (1 Flugzeugträger 100 Milliarden US$, 1 Jagd-U-Boot 10 Milliarden US$, 1 B2 strategischer Tarnkappenbomber 1 Milliarde US$) sind Software, Kommunikationsmittel und Infrastruktur relativ billig. Aber die rapide und aggressive Digitalisierung der Streitkräfte der USA und die Vorbereitung auf alle wahrscheinlichen und unwahrscheinlichen Cyber- und

Informationskriegszenarios verleihen der gesamten Kommunikations- und Computerbranche einen gewaltigen Auftrieb. Nicht zu vergessen, die strategischen Computer-Initiativen des US-Energieministeriums mit der Absicht, bis 2004 die schnellsten Supercomputer mit einer Rechenleistung von 30—100 Teraflops zu bauen.[18]

The transformation of U.S. military forces goes well beyond gaining information superiority and developing new technologies. Through a wide variety of analyses, wargames, studies, experiments, and exercises, the Department is systematically and aggressively investigating new operational concepts, doctrines, and organizational approaches that will enable U.S. forces to maintain full spectrum dominance of the battlespace well into the 21st century. [19]

Theorien über Rüstungswettläufe unterscheiden zwischen zwei grundsätzlichen Erklärungen oder einer Kombination von beiden. Vereinfachend gesagt, geht die eine Theorie von Aktions-Reaktionsmustern der potentiellen Gegner aus. Diesem Außenleitungstheorem ist als Vorbedingung, als Erklärungswert (Explanandum) und auch als Rechtfertigung eine systemimmanente wechselseitige Bedrohungswahrnehmung zu eigen. Die theoretische Antwort im Kalten Krieg war die "gesicherte wechselseitige Vernichtung" (mutually assured destruction, MAD) durch Kernwaffen. In einer streng wissenschaftstheoretischen Auslegung des Theorems "Staaten rüsten, weil andere Staaten genauso rüsten und deshalb eine Gefahr für die nationale Sicherheit darstellen können" — dies ist der (neo-)realistische Ansatz — kann dieses Theorem gar nicht falsifiziert werden, es ist tautologisch.

Nicht das Militär hat diesen pathologischen Zirkelschluß wechselseitiger Fehlwahrnehmungen durchbrochen, sondern die Politik mit ihren vertrauensbildenden Maßnahmen.

Der andere Ansatz versucht Rüstung durch eine innengeleitete Theorie zu erklären, durch Lobby-Interessen, durch die Trägheit von Bürokratien und die Eigendynamik des wissenschaftlich-industriell-militärischen Komplexes, eine Gefahr für einen demokratisch verfaßten Staat, vor der der frühere US-Präsident Eisenhower in seiner Abschlußrede anläßlich seines Ausscheidens aus dem Amt 1961 gewarnt hat.

Wie auch immer, ein dritter Definitionsraum scheint mir erforderlich, um das möglicherweise gerade beginnende Informationskrieg-Wettrüsten erklären zu können, und dieser hat zu Clausewitz zurückzukehren.

In der Fachwelt der Theorien internationaler Beziehungen und auch in jener der Friedensforschung herrscht größtenteils Übereinstimmung über die These, wonach demokratisch verfaßte Staaten höchstwahrscheinlich untereinander weder um Territorium noch um Ressourcen oder andere Werte blutige Kriege führen (werden). Diese Resultate werden auch von "Cyber-Theoretikern", z. B. von Alvin und Heidi Toffler, geteilt, die meinen:

The world, thus, is entering into a global order — or disorder, as the case may be — that is post-Westphalian, and post-Clausewitzian. It is something new. In a dialectical sense, it bears some resemblance to the pre-Westphalian order of diverse kinds of polities, but it involves a much higher order of complexity among actors, and, above all, it changes at hyper-speed.[20]

Drei Annahmen verleihen der These Plausibilität, daß Demokratien westlichen Zuschnitts untereinander keine Kriege führen:

Sie sind fähig, ihre Konflikte mit nichtmilitärischen Mitteln zu lösen.

Die Globalisierung führt zu einer irreversibel dichten wechselseitigen Abhängigkeit, die jeden "realen" militärischen Konflikt von vornherein ausschließt.

Die "dritte Welle" oder die "dritte industrielle Revolution", in der wir uns gerade befinden, führt zu einer Transformation des industriell geprägten Nationalstaates in eine globale Informationsgesellschaft, wo zunehmend mehr Güter und Dienstleistungen innerhalb dieser globalen Informationsinfrastruktur gehandelt und verkauft werden. (Obwohl neue Technologien als primäre Antriebskräfte dieses Wandels angesehen werden, so gibt es doch alternative Interpretationen dieses Transformationsprozesses, etwa jene in der von Schumpeter stehenden Tradition der Ökonomie, bei der Technologie, Institutionen, Kultur, Werte und Wahrnehmungen in einem wesentlich komplexeren und unvorhersehbareren Interaktionsgeflecht stehen.)

Deshalb wird Clausewitz vielleicht zu uns zurückkehren, nicht durch die Vordertüre des Industriezeitalters, sondern auch durch die Hintertüre des Informationskriegszeitalters, und das auch bei Demokratien westlicher Verfaßtheit, nämlich dann, wenn der Informationskrieg als die "Fortsetzung von Politik mit anderen Mitteln" begriffen wird.

Sieht man sich die oben dargestellten semantischen Raster an, so sind psychologische Kriegsführung, Kulturkampf, Techno-Imperialismus und Informations-Terrorismus die wahrscheinlichsten Kandidaten für den unblutigen Schlachtplatz des Informationskriegs,[21] oder eines — wie die Russen es nennen — "informationsbasierenden psychologischen Kampfes" oder eines "Volksinformationskriegs", wie die Chinesen meinen.

Joseph Nye und William Owen haben 1996 aus US-Perspektive eine derartige Annäherung in ihrem Artikel "Americas Information Edge" in Foreign Affairs, dem "Zeitgeist-Zentralorgan" der US-Außenpolitik, unternommen, wobei sie Herrschaft über Information nicht nur als militärischen Aktivposten, sondern auch als geopolitisches Instrument begreifen:

> Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerfull than any other. […] The information edge is equally important as force multiplier of American diplomacy, including "soft power" — the attraction of American democracy and free markets,[22]

während gleichzeitig "soft power" definiert wird als

> the ability to achieve desired outcomes in international affairs through attraction rather than coercion. It works by convincing others to follow, or getting them to agree to, norms and institutions that produce the desired behavior.[23]

Nachdem die "Vorzüge" der US-amerikanischen Populärkultur[24] und die weltweite Informations- und Medienhegemonie hervorgehoben wurden, schlußfolgern Nye/Owen:

> In truth, the 21st century, not the twenthies, will turn out to be the period of America's greatest preeminence. Information is the new coin of the international realm, and the United States is better positioned than any other country to multiply the potency of its hard and soft power resources through information.[25]

Diese Auffassung wird weitgehend geteilt. Die Tofflers sprechen von "Medien-Haubitzen" der USA (Hollywood, CNN), die niemand anderem zur Verfügung stünden.[26] Panarin[27], ein Mitglied der Russischen Akademie der Wissenschaften und regierungsnaher Experte für Informationskrieg, sieht den Beginn eines Info-Krieg-Konzeptes als Mittel der US-Außenpolitik in der Ära der "Hollywood-Präsidentschaft" Ronald Reagans und des SDI-Projekts angesiedelt. Er identifiziert vier verschieden Komponenten im Bereich der

Wahrnehmung nationaler Sicherheit und nationaler Interessen der USA: Diplomatie, Ökonomie, Militär und Information.

Was jedoch zunächst vornehm und nobel in diplomatischer Sprache formuliert wurde ("Information Superiority", "Soft Power") kommt seit zwei Jahren grob und brutal in den maßgeblichen militärischen und politischen Doktrin- Dokumenten daher,[28] wenn es um die Struktur, Gestalt und Aufgabe der Streitkräfte der USA im 21. Jahrhundert geht: Der absolute Wille zur politischen und militärischen Weltvorherrschaft, Hegemonie, Dominanz und Beherrschung (z. B. eröffnet sich die Metapher "Full Spectrum Dominance" zweifach: als die vollständige Beherrschung und Oberhoheit über das elektromagnetische Spektrum für Aufklärung, Überwachung, Blendung, Störung und Abhörung, aber ebenso für "Machtprojektion" im "nationalen Interesse") durch (nicht nur, aber auch zunehmend wichtig) cyberkriegartige Maßnahmen, sicherlich in defensiver, aber auch in offensiver Art und Weise. Nur um ein paar Beispiele entlang und neben der "Cyber-Debatte" zu geben:

— Die alle vier Jahre stattfindende Neubewertung des Verteidigungskonzeptes (Quadrennial Defense Review, QDR) aus dem Mai 1997 für den US Kongreß[29] (QDR 1997) beharrt — genauso wie die Joint Vision 2010-Doktrin — nach wie vor auf der Notwendigkeit, gleichzeitig zwei große konventionelle Kriege führen und gewinnen zu können, z. B. auf Kriegsschauplätzen am Persischen Golf und in Asien.

— Die QDR definiert den Anspruch, weiterhin zwölf Flugzeugträger-Kampfgruppen weltweit einsatzbereit zu halten, während die angesehene Publikation des Internationalen Instituts für Strategische Studien in London (IISS), die Military Balance 1997/98[30] gerade einen (nicht einsatzbereiten) russischen, zwei französische, drei britische und einen indischen Flugzeugträger im gesamten Rest der Welt zu vermelden vermag.

— Die USA sind der einzige Staat der Welt, der nach wie vor ca. 150 Kernwaffen — frei fallende Bomben des Typs B-61 — außerhalb seines Territoriums auf dem Boden von sieben europäischen NATO-Staaten disloziert hat, nämlich in Belgien, Deutschland, Griechenland, Großbritannien, Italien, den Niederlanden und der Türkei. Diese sollen von US- und NATO-Streitkräften zum Einsatz gebracht werden. Die NATO-Staaten einschließlich der USA verurteilten kürzlich die indischen und pakistanischen Kernwaffentests, aber insistierten zuletzt Mitte Juni 1998 darauf, "that NATO's nuclear forces […] continue to play a unique andessential role in alliance strategy."[31]

— Das US-Kernwaffenarsenal befindet sich gerade in der Phase einer millionenschweren Funktionsverbesserung, mit der es möglich sein wird, blitzschnell — und weltweit — verschiedenste Eventualfälle ins Visier zu nehmen. Zwei Tage, nachdem von den Vereinigten Generalstabschefs ihre Joint Doctrine for Command and Control Warfare (C2W)[32] veröffentlicht wurde, wurde auch das Dokument Doctrine for Joint Theater Nuclear Operations[33] in Kraft gesetzt, nämlich am 9. Februar 1996. Danach, im Dezember 1997, erließ Präsident Clinton eine hochgradig klassifizierte präsidentielle Direktive (Presidential Decision Directive, PDD-60) mit neuen Leitlinien für die nukleare Zielplanung. Hintergrundinformationen basierend auf dieser Direktive sowie die Analyse der nichtklassifizierten Doktrin Joint-Pub 3-12.1 zeichnen ein dramatisch neues und einzigartiges Bild der zukünftigen nuklearen Zielplanung der USA. Als der einzige Staat der Welt, der jemals zwei Arten von Massenvernichtungswaffen im Krieg eingesetzt hat (Kernwaffen und chemische Waffen)[34], führen die USA einen neuen Typ von Kernwaffe, eine neue erd-und bunkerpenetrierende Waffe im Subkilotonnen-Bereich ein, die gegen Schurkenstaaten und am Schlachtfeld verwendet werden soll.

Im Detail handelt es sich um folgende Zielsetzungen: "kriegsförmige Erwiderung" (belligerent response, nukleare Vergeltungsmaßnahmen gegen Nichtkernwaffenstaaten, die Massenvernichtungswaffen einsetzen), "Kampfstoffabwehr" (agent defeat, die thermische Vernichtung chemischer und biologischer Substanzen am Boden und in der Luft), die Zerstörung von Einrichtungen und Operationszentren "nichtstaatlicher Akteure", und nicht zuletzt handelt es sich um nukleare Präventivschläge gegen waffenfähige nukleare, chemische und biologische Einrichtungen und Kommando- und Kontrollzentren. Diese Konzepte gehen weit über das hinaus, was im Kalten Krieg als Abschreckung bezeichnet wurde und was dafür auserkoren war, um eine als überlegen wahrgenommene konventionelle Kräftekonstellation in einer Blockkonfrontation oder am Schlachtfeld abzuwehren. Unter dem Titel "Erwünschte Resultate des Einsatzes von Kernwaffen" werden folgende Zielsetzungen hervorgehoben:[35]

— Decisively change the perception of enemy leaders about their ability to win.

— Demonstrate to enemy leaders that, should the conflict continue or escalate, the certain loss outweighs the potential gain.

— Promptly resolve the conflict on terms favorable to the United States and our allies.

— Preclude the enemy from achieving its objectives.

— Ensure the success of the effort by US and/or multinational forces.

Die Erfindung neuer militärischer und nicht-militärischer Bedrohungen

Eine militärische Bedrohung des US-amerikanischen Territoriums ist nicht in Sicht. Strategische ICBM-Kapazitäten (interkontinentale ballistische Raketen), die das US-Territorium bedrohen könnten, besitzen nur die Russische Föderation, China, Frankreich und Großbritannien. Möglicherweise wird Indien mit einer solchen Kapazität hervortreten, die "Schurkenstaaten" — Irak, Iran, Libyen, Nord-Korea, Syrien und wer noch immer zu diesem Club stoßen mag — sind weit, weit entfernt davon.

Folgt man jedoch der QDR von 1997, so stellen sich "new threats and dangers — harder to define and more difficult to track" dar. Diese Bedrohungen erstrecken sich vom Einsatz von Massenvernichtungswaffen durch Terroristen, ein Szenario das von Hollywood in den vergangenen Jahren massiv propagandistisch ausgeschlachtet wurde,[36] über psychologische Kriegsführung und Info-Terrorismus (der jüngste "James Bond"-Film), bis hin zu cyber-terroristischen Attacken auf die nationale Informationsinfrastruktur der USA; lediglich der letzte Hollywood-Hype (der Film Deep Impact), der einen Zusammenstoß der Erde mit einem Asteroiden etwa gegen 2010 thematisiert, findet sich noch nicht in der QDR.

Man kann davon ausgehen, daß Derartiges bald implementiert werden wird, da es das meistgeliebte Steckenpferd von Edward Teller darstellte, Kernwaffen in erdnahen Orbits zu stationieren, nachdem das ursprüngliche SDI-Projekt nicht von der Stelle kam. Anders das Nachfolgeprojekt: "The National Missile Defense (NMD) remains a high priority. The Administration and Congress have agreed to keep this program on an accelerated research and development path aimed at creating the option to make a decision on deployment possible as early as fiscal year 2000, if the threat warrants." (QDR 1997). Die überzeugendste Kombination für Pentagon-Planungen wäre sicherlich ein Angriff von Kommunisten aus dem Weltraum. Wenn der erste Hollywood-Film darüber herauskommt, können Sie mit Sicherheit davon ausgehen, daß das Pentagon dazu eine Projektgruppe eingerichtet hat. (Die NASA hatte

tatsächlich bereits eine Projektgruppe zur Asteroidenbeobachtung und Erdbedrohung eingerichtet, bevor der Film Deep Impact herauskam.)

Spaß beiseite: Die QDR wird die USA mit einem Verteidigungsbudget, das nur um 23 Prozent unter dem langjährigen Durchschnitt des Kalten Krieges zwischen 1976 und 1990 liegt,[37] ins 21. Jahrhundert führen. Nach jüngsten offiziellen NATO-Angaben über das erklärte gesamte US- und NATO-Budget (in gegenwärtigen Preisen und Wechselkursen) ergeben sich folgende Größen, gerundet in Milliarden US$):[38]

1975	1980	1985	1990	1993	1994	1995	1996	1997
88	138	258	306	298	288	278	271	273

Damit ist das erklärte gesamte Verteidigungsbudget der USA 1997 um 15 Milliarden US$ höher als 1985 und nur um 33 Milliarden niedriger als 1990, als der Kalte Krieg offiziell beendet war.

Auch mangelt es an Transparenz darüber, welcher Anteil dieser deklarierten Ausgaben direkt oder indirekt für Cyber — und Informationskriegsprojekte aufgewendet wird, wenn man etwa die in der "Visions 2010"-Kampagne für gemeinsame Echtzeitkriegsführung in globalem Ausmaß anfallenden Kosten, jene für die weltraumbasierenden Projekte für Kommando- und Kontrollkriegsführung (C2W, für Satelliten-Überwachung und -Aufklärung), die für die weltraum- und bodengestützten Projekte für die schlachtfeldbezogene, taktische und strategische Abwehr ballistischer Raketen oder jene für die Initiativen für die RMA in Rechnung stellt.[39] Darüber hinaus sind die strategischen Computer-Initiativen für computerbasierende Simulationen von Kernwaffentests[40] gemäß dem "Stewardship Stockpile Program" nicht im Budget des US-Verteidigungsministeriums, sondern in jenem des Energieministeriums angeführt. Genauso wenig sind die 26,7 Milliarden US$ für das Finanzjahr 1997 für geheimdienstliche Aktivitäten einschließlich CIA, NSA oder anderer Dienste im offiziellen Verteidigungshaushalt enthalten.[41]

Als die "realen Bedrohungen" gegen Ende des Kalten Krieges mehr und mehr zu verblassen begannen, tauchten austauschbare Module für militärische Bedrohungen und Legitimationszusammenhänge auf. "The agnosticism of the uncertainty hawks extends not only to the specifics of discrete future events […] but also to the general character and magnitude of possible threats."[42] Die USA taumeln im Zwielicht von Ungewißheit und Unsicherheit, und dieses vorherrschende Mantra begann zeitgleich, sich auch innerhalb der NATO-Bürokratie auszubreiten und zu wuchern. Die Antworten darauf sind nicht präventiver Natur (z. B. in Form von Technologiekontroll-Export-Regimen oder präventiver Diplomatie), sondern sind Gegenmaßnahmen gegen die Proliferation von nuklearen und anderen Massenvernichtungswaffen und gegen Angriffe außerhalb des eigenen Territoriums, aber innerhalb des nationalen Interesses. Es zeigt sich daran, daß das "nationale Interesse" der USA nun global definiert wird und nicht nur die "alten Ölquellen im persischen Golf" einschließt, sondern möglicherweise auch bald die "neuen Ölquellen" im Festlandsockel des Kaspischen Meeres umfassen wird (eine der heißesten Regionen der Welt, zwischen der Russischen Föderation, Kasachstan, Aserbaidschan, Iran und Turkmenistan, Handlungsort des Kulturkampfes zwischen der Russischen Föderation, den USA und der islamischen Welt). Letztendlich erscheint es nicht überraschend, daß die wichtigsten, direktesten und klarsten Antworten für geoökonomische und geopolitische Herausforderungen für die Außenpolitik der USA auf technologisch-technokratischen Antworten beruhen.

Um die Joint Vision 2010 umzusetzen, mit der politisch die Absicht verbunden wird — "to respond to the full spectrum of crises that threaten US interests"[43] — wurde nach intensiver Nachdenkarbeit des Pentagons ein neues Akronym-Monster kreiert und kürzlich (April 1998) von Verteidigungsminister William S. Cohen bestätigt. Nicht Cyberkrieg, nicht Informationskrieg, nicht Kommando- und Kontrollkrieg (C2W), nicht C3I, auch nicht C4I, nein. C4ISR ist der letzte Standard der Diskussion und der diesbezüglichen Forderungen des Pentagons: "Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance", was man vielleicht am besten mit "Kommando, Kontrolle, Kommunikation, Computer, nachrichtendienstliche Aufklärung, technische Überwachung und technische Aufklärung" übersetzen kann. Das Pentagon hat dabei kürzlich die "most important C4ISR architecture initiative", nämlich die "Joint Technical Architecture"[44] in die Welt gesetzt, die das nachrichtentechnische Rückgrat für die "Revolution in militärischen Angelegenheiten" zur Verfügung stellen soll. Die sechs bedeutsamsten Komponenten bei dieser sich abzeichnenden C4ISR-Architektur für das Jahr 2010 und darüber hinaus sind:

— A robust multisensor information grid providing dominant awareness of the battlespace to U. S. commanders and forces.

— Advanced battle-management capabilities that allow employment of globally deployed forces faster and more flexibly than those of potential adversaries.

— A sensor-to-shooter grid to enable dynamic targeting and cuing of precision-guided weapons, cooperative engagement, integrated air defense, and rapid battle damage assessment and re-strike.

— An information operations capability able to penetrate, manipulate, or deny an adversary’s battlespace awareness or unimpeded use of his own forces.

— A joint communications grid with adequate capacity, resilience, and network management capabilities to support the above capabilities as well as the range of communications requirements among commanders and forces.

— An information defense system to protect globally distributed communications and processing networks from interference or exploitation by an adversary.[45]

Cyber- und Informationskriege: Hype oder Realität?

Einige Fragen sind hier aufgeworfen worden, etwa zum Verhältnis zwischen dem Außenpolitikdesign der USA und dem Antrieb, der hinter den Cyber- und Informationskriegskonzepten steht. Handelt es sich dabei um ein "Grand Design" oder schlicht und einfach um das Ergebnis erratischer Entscheidungen verschiedener Bürokratien und der gegenwärtigen Regierung? Es scheint viel weniger als eine Verschwörung zu sein, aber auch viel mehr als nur ein neuer Trend im militärischen Alltag.

Definiert man Informationskrieg als irgend etwas zwischen Klatsch, C-irgendwas-Kriegsführung und der Anwendung von Supercomputern, so gibt es nicht viel Neues unter der Sonne, abgesehen von den hochentwickelten Informationskanälen und Informationsverarbeitungskapazitäten.

Wenn es sich bei Informations- und Cyberkriegsführung darum handelt, vor oder unmittelbar während der Kampfhandlungen Einfluß auf den Geist, das Bewußtsein und die Wahrnehmung feindlicher Eliten auszuüben, auf ihren Realitätssinn und ihr Selbstverständnis, so ist dieses Konzept so alt wie die Aphorismen von Sunzi über die "Kunst des Krieges", die gegenwärtig in US-Werken eine intensive Rezeption erfahren, also etwa zweitausend Jahre. Im 20.

Jahrhundert wurde dieser Ansatz "psychologische Kriegsführung" oder "reflexive Kontrolle" genannt.

Dreht sich die Debatte jedoch um das reale Schlachtfeld, um alle Subtypen von Cyberkriegsführung im Spektrum zwischen C2W und C4ISR und um die Revolution in militärischen Angelegenheiten, so geht es vor allem um gesteigerte Letalität und Tötungsfähigkeit über große Distanzen und in Echtzeit. Es handelt sich um eine Machtprojektion ohne physische Präsenz. Im eindringlichsten philosophischen Wortsinn werden hiermit politische und militärische Macht und die Fähigkeit zu töten "virtuell". Die Absichten dazu und die Realisierung dessen sind bei den USA am weitesten gediehen. Und dahinter steht eine politische Vorstellung.

Die Auswirkungen von Cyber- und Netzkrieg abzuschätzen — im Sinne eines Hackens globaler oder nationaler Informationsinfrastrukturen (gleichgültig, ob es sich dabei um zivile oder militärische handelt) durch Individuen, Nichtregierungsorganisationen oder Staaten mit tatsächlich lebensgefährlichen Folgen — ist nicht eben einfach. Möglicherweise handelt es sich bei dieser intendiert alarmistischen Interpretation um eine Propagandalüge außerordentlicher Größenordnung, weshalb eine Unterscheidung zwischen Tatsachen und Fiktion dringend nötig wäre. Die realen bewaffneten Konflikte in der realen Welt der neunziger Jahre wurden mit leichten und mittelschweren Feuerwaffen (teilweise natürlich auch mit schweren Waffen) und mit Landminen ausgetragen, und sie töteten etwa zwei Millionen Menschen, meist unschuldige Zivilisten.

Das "The Day After"-Szenario der DARPA (Defense Advanced Research Projects Agency der USA), das als Übung für eine Bedrohungssituation im Jahr 2000 inszeniert wurde, von dem Anderson und Hearn[46] berichten, geht davon aus, daß Hacker-Angriffe auf das Finanzsystem, auf die Elektrizitäts- und Ölversorgung, auf den Flugverkehr und das Eisenbahnsystem sowie auf Fernsehanstalten in drei Weltregionen — den USA, Europa und dem Persischen Golf — gleichzeitig stattfinden und dort schwere Unfälle mit Menschenopfern und hohem materiellem Schaden zu beklagen sind. Gleichzeitig jedoch gibt dieses Planspiel keinerlei plausible Begründung dafür, auf welchem technischen Weg oder mitttels welcher Maßnahmen die Angriffe auf die Netzwerke durchgeführt werden, es ist nur von einer "niedrigen Eintrittsschwelle" die Rede.

Es sind im wesentlichen vier Argumente, die dagegen sprechen, daß ein Netzkrieg lebensbedrohende Gefahren größeren Stils nach sich ziehen könnte:

— Groß angelegte Angriffe, wie sie im "The Day After"-Szenario beschrieben werden, können nicht von Individuen, auch nicht von gut organisierten Nichtregierungsorganisationen oder subnationalen Gruppen durchgeführt werden.

— Sollten solche Szenarien tatsächlich Wirklichkeit werden, so höchstwahrscheinlich in der Morgendämmerung eines großen Krieges, wobei die politischen Spannungen und die politischen Akteure bekannt wären.

— Jeder, der Informationssysteme in einem derartigen Stil angreift, hinterläßt eine elektronische Spur, durch die er identifiziert werden kann.

— Sicherungsmaßnahmen für weit verzweigte Kommunikationssysteme sind sowohl auf der Ebene der physischen Signalträger wie auch auf der Ebene der Software leichter durchzuführen als die Verteidigung geschlossener Systeme. Offene Systeme, basierend auf

universellen Protokollen, etwa auf TCP/IP und dessen Derivaten, wie sie im Internet, in Intranets und im "Extranet" Anwendung finden, sind auf verschiedenste Weise redundant. (Selbst die NATO erwägt gegenwärtig, "verborgene" Web-Seiten mit klassifizierten Informationen für die Mitglieder des Programms "Partnerschaft für den Frieden" einzurichten. Ein erfolgreiches Hacken dieser Web-Seiten würde keinen größeren "Schaden" anrichten, als klassifizierte Informationen offenzulegen.)

Um zu einem Schluß zu kommen: Meiner Einschätzung nach stellen Massenvernichtungswaffen wie Giftgas, biologische oder radiologische Waffen oder primitive Kernwaffen in den Händen von Terroristen[47] eine weit größere Sicherheitsbedrohung dar, als das Hacken von nationalen oder globalen Informationsinfrastrukturen. Es gibt in der Tat einige wenige und sehr spekulative Szenarien, die alle um die Kernwaffen der USA und der Russischen Föderation kreisen, denn die könnten tatsächlich ein Desaster auslösen:

> It is important to recognize that soon both sides (US and Russia) will have the ability to use holograms and other IT manifestations that will offer the opportunity to completely fool one another both on the battlefield and through the airwaves […] A hacker simulating an incoming ICBM nuclear attack on the radar screens of the military of either Russia or the United States is but one manifestation of this threat.[48]

Das Hacken der Abschußcodes von strategischen Kernwaffen, das eine Paralyse der jeweiligen US-amerikanischen oder russischen Fähigkeit, einen Gegenschlag auszulösen, hervorrufen könnte, der Versuch, positive Kontrolle über die jeweils anderen Kernwaffenarsenale zu erlangen, der Versuch, elektronische Kontrolle über die jeweilig anderen Frühwarnsatelliten zu erlangen, und schließlich, das Szenario, auf einen "realen" oder "wahrgenommenen" Hacker-Angriff auf das eigene Kommando- und Kontrollsystem der strategischen Kernwaffen unmittelbar mit einem nuklearen Gegenschlag zu reagieren — all diese Szenarien sind Teil dieser hyper-alarmistischen Betrachtungsweise.

Es kann hier keine seriöse Antwort darauf gegeben werden, ob solche Szenarien tatsächlich eine ernsthafte Gefahr für die Menschheit darstellen. Es ist aus der nicht-klassifizierten Literatur nur sehr wenig über die tatsächliche technische Verfaßtheit der nuklearen Kommando- und Kontrollketten der USA und der Russischen Föderation bekannt. Die Gefahr liegt mehr in der Natur der Kernwaffen selbst.

Ich möchte meine abschließende Betrachtung im Licht von Platos Höhlen-Gleichnisses zu Ende führen. Es sollte illustrieren, daß Erkenntnis und Wissen immer ein "Schatten" der Realität sind. In diesem Sinn war Plato ein früher Konstruktivist, der eine Unterscheidung zwischen einer "realen" und einer "konstruierten Realität" hinterfragte und als partiell oder vollständig ununterscheidbar bezeichnete. Psychologische und soziologische Theorien im 20. Jahrhundert gehen so weit, die "Konstruktion sozialer Realität" vollständig auf eine Funktion der Wahrnehmung zurückzuführen.

Plato in der modernen Sprachumgebung der Cyber-Debatte anzuwenden, bedeutet, jene Grenzlinie zwischen Hype, propagandistischer Instrumentalisierung und Ausschlachtung der Cyberkriegs-Debatte einerseits und der Realität andererseits zu finden.

Günther Anders, ein österreichischer Philosoph, hat bereits 1960 die prinzipielle Verwundbarkeit von großtechnischen Systemen und Netzwerken und alle damit verbundenen Folgeprobleme vorhergesehen, als er seine Gleichung "Apparat = Welt" formulierte:[49] "Die katastrophische Gefährlichkeit einer solchen Universalmaschine liegt auf der Hand. Würde nämlich — was bei der Degradierung aller Apparate zu Apparatteilen der Fall wäre — die

totale Interdependenz zwischen allen ihren Teilen Wirklichkeit werden, dann würde jedes Versagen eines Teiles automatisch den ganzen Apparat in Mitleidenschaft ziehen, also still legen."[50]

Dem gibt es fast nichts hinzuzufügen, außer meiner Einschätzung, daß wesentlich mehr empirische Forschung nötig wäre, um die Interaktion zwischen dem Militär und den Neuen Informationstechnologien zu verstehen. Mindestens genauso wichtig wäre die Etablierung eines Frühwarnsystems und von "Wachhunden", um so früh wie möglich einen beginnenden Rüstungswettlauf auf dem Sektor der Informationskriegsführung erkennen zu können.

Fußnoten:

[1] Van Creveld, Martin: Command in War. Harvard Press, Cambridge/Mass. 1985, 264, zitiert nach Arquilla, John; Ronfeldt, David: "Cyberwar is Coming!". In: Arquilla, John; Ronfeldt, David (Hg.): Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica 1997, 58, Fußnote 11, formulierte es folgendermaßen: "From Plato to NATO, the history of command in war consists essentially of an endless quest for certainty …" S. auch Seite 24—56 im vorliegenden Band.

[2] Arquilla/Ronfeldt: Cyberwar is coming!, 30

[3] Ibid., 31

[4] Ibid., 28

[5] Ibid., 29

[6] Ibid., 30

[7] Arquilla, John; Ronfeldt, David: "The Advent of Netwar". In: Arquilla, John; Ronfeldt, David (Hg.); RAND: In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica 1997, 275

[8] Ibid., 277

[9] Ibid., 278

[10] Ibid., 285

[11] Ibid., 279

[12] Joint Vision 2010. 16

[13] Joint Pub 3-13.1, GL-8

[14] George J. Stein unterscheidet in seinem Beitrag InfoWar: Worte zählen im vorliegenden Band zwei Subkonzepte: "(a) andere Anwendungsformen von InfoWar im Rahmen militärischer Operationen und (b) Anwendungsformen von InfoWar auch im Rahmen nichtmilitärischer Operationen geben kann. Genauso findet C2W "in allen Bereichen militärischer Operationen und in allen Konfliktsituationen" Anwendung. Es ist somit nicht mehr nur darauf beschränkt, auf dem Schlachtfeld den Befehlsfluß des feindlichen Kommandos zu unterbrechen. Die Joint Doctrine for Command and Control Warfare ist insgesamt wahrscheinlich die geeignetste Ausgangsbasis, um die Evolution des InfoWar zu verfolgen." (siehe S. 59—60)

[15] Dieses Dokument ist im Web zitiert unter: http://www.ndu.edu/ndu/inss/actpubs/act003/a003ch10.html>

[16] Zitiert nach: Conetta, Carl; Knight, Charles: "Inventing Threats". In: Bulletin of the Atomic Scientists, March/April 1998, 32

[17] Vgl. Kittler, Friedrich: "Zur Theoriegeschichte von Information Warfare" im vorliegenden Band, S. 301—307

[18] Im Februar 1998 erhielt IBM vom amerikanischen Energieministerium (DoE) einen Vertrag in der Größenordnung von 500 Millionen US$, um die weltschnellsten Supercomputer im Rahmen des "Stockpile Stewardship Program" für Kernwaffentestsimulationen zu bauen. Die Rechenleistung soll zwischen 2001 und 2004 zwischen 30 und 100 Teraflops erreichen.

[19] William S. Cohen im April 1998 in einem Report des US-Verteidigungsministeriums an den US-Kongreß, Kapitel 15. Cohen, William S.: Annual Report to the President and the Congress. U.S. Department of Defense, April 1998. Zitiert nach: http://www.fas.org/man/docs/adr 99/index.html

[20] Toffler, Alvin; Toffler, Heidi: "The New Intangibles". In: In Athena's Camp. xx

[21] Was sich jedoch in weiterer Folge durchaus als "blutig" erweisen könnte.

[22] Nye, Joseph; Owen, William: "America's Information Edge". In: Foreign Affairs. March/April 1996, 20

[23] Ibid., 21. Es sei am Rande erwähnt: Russische Theoretiker nannten den Versuch, das Verhalten eines Gegenübers gegen seinen Willen zu beeinflussen, in der Tradition Iwan Pawlows "reflexive Kontrolle".

[24] Was man auf die fürchterliche "dreifache-M-Verblödung" — McDonalds, Michael Jackson und Madonna — auf den Punkt bringen könnte.

[25] Nye/Owen: ibid., 35

[26] Toffler/Toffler: ibid., xvi

[27] Vgl. Igor Nikolaewitsch Panarin: InfoWar und Autorität. Siehe S. 105—110 im vorliegenden Band

[28] Namentlich: Joint Pub 3-13.1, die Quadrennial Defense Review von 1997, die Joint Vision 2010 und der aus dem April 1998 stammende Report of the DoD to Congress.

[29] Zitiert nach: http://www.fas.org/man/docs/qdr/index.html

[30] IISS, International Institute for Strategic Studies: The Military Balance 1997/98. London 1998

[31] NATO Press Communiqué M-DPC/NPG-1 (98),72, 11 June 1998

[32] Joint Pub 3-13.1

[33] Joint Pub 3-13.1

[34] Der Einsatz der Kernwaffen gegen Hiroshima und Nagasaki sind weithin bekannt.

[35] Joint Pub 3-12.1, I-2

[36] Gen. Eugene Habiger, der Oberbefehlshaber der nuklear-strategischen Streitkräfte der USA besuchte Ende Mai 1998 die Kernwaffenstandorte der Russischen Föderation, um mehr über die Kernwaffen der anderen großen Nuklearmacht zu erfahren: "I want to put to bed this concern that there are loose nukes in Russia," sagte Habiger in einem Interview mit The Associated Press. bevor er in die USA zurückflog. "My observations are that the Russians are indeed very serious about security." (Associated Press, 7 June 1998)

[37] Conetta/Knight: ibid., 32

[38] NATO Press Communique M-DPC-2(97)147, 2nd Dec. 1997

[39] Folgende Ausgaben sind nur ausgewählte Bereiche der DARPA (Defense Advanced Research Projects Agency) für das Finanzjahr 1998, in Millionen US$. Quelle: http://www.arpa.mil/ documents/98_budget.html

Title - FY 1996 - -FY 1997 - - FY 1998 - -FY 1999
Defense research sciences - - - - - - - - - 76.459 - - - 90.701 - - - 76.009 - - - 80.936
Next generation internet - - - - - - - - - - -0.000 - - - - 0.000 - - - 40.000 - - - 40.000
Computing sys; comm technology - - 361.528 - - -314.969 - - 341.752 - - -371.471
Tactical technology - - - - - - - - - - - - 120.440 - - -121.520 - - 155.329 - - - 177.995
Integrated command; control tech - - - - 44.395 - - - 59.672 - - - 37.000 - - - - 40.000
Advanced electronics technologies - - - 389.610 - - 360.288 - - 277.044 - - - 282.668
Command, cont'l; communications sys - 0.000 - - -102.996 - - 163.800 - - - 172.600
Sensor; guidance technology - - - - - - - - 0.000 - - - 108.360 - - 166.855 - - - 200.582
Agency total - - - - - - - - - - - - - - - - -2.269.202 - - 2.140.436 - 2.204.403 - 2.271.934

[40] Einen Überblick darüber gibt: Explosive Alliances. Nuclear Weapons Simulation Research at American Universities. Zusammengestellt vom Natural Resources Defence Council. Quelle: http://www.nrdc.org/nrdcpro/expl/eainx.html

[41] Laut CIA ist diese Budget 1997 leicht — um 0,2% gegenüber dem Finanzjahr 1996 — gewachsen. Es war erst das zweite Mal seit 1945, daß diese gut versteckten Ausgaben veröffentlicht wurden. Neue Zürcher Zeitung, 25. März 1998, 4

[42] Conetta/Knight, ibid., 34

[43] Cohen, William S. (1998): Annual Report to the President and the Congress. U.S. Department of Defense, April 1998. Zitiert nach: http://www.fas.org/man/docs/adr_99/index.html

[44] Cohen, ibid., Kapitel 8

[45] Cohen, ibid., Kapitel 13

[46] Anderson, Robert H.; Hearn, Anthony C., National Defense Research Institute, RAND: "An Exploration of Cyberspace Security R&D Investment Strategies for DARPA". In: Arquilla, John; Ronfeldt, David (Hg.): In Athena's Camp. Preparing for Conflict in the Information Age. Santa Monica 1997, 1—19

[47] Mir scheint, daß insbesondere bei Szenarien wie dem Diebstahl von Kernwaffen durch Terroristen oder subnationale Gruppen die alarmistische Position stark übertrieben ist.

[48] Thomas, Timothy L.: "Information Technology: US/Russian Perspectives and Potential for Military Political Cooperation". In: Cross, Sharyl; Zevelev, Igor; Kremenyuk,Victor; Gevorgian, Vagan (Hg.): Global Security Beyond the Millennium: American and Russian Perspectives, MacMillan Press (forthcoming), 69—89

[49] Anders, Günther: Die Antiquiertheit des Menschen. 2. Band, 4. unveränderte Auflage, C.H. Beck, München 1986, 111

[50] Anders, Günther, ibid., 114