„CyberWars": Der unsichtbare Kampf um Informationsmacht

Johannes J. Frühbauer

I. Fiktion oder Realität?

Eine gewaltige Explosion zieht uns mitten ins Geschehen: Nachdem die Szene zunächst wie eingefroren wirkt, verwüstet in der völlig unerwarteten Dramatik der ersten Sequenzen von *Passwort: Swordfish* (USA 2001) die Druckwelle der Explosion den Straßenzug vor einem Bankgebäude. Fensterfronten bersten, Autos wirbeln durch die Luft, Passanten werden niedergestreckt oder von Feuerzungen umhüllt. Doch anders als diese konventionelle Action-Szene zunächst vermuten ließe, steht in diesem Streifen des Hollywood-Regisseurs Dominic Scena nicht die direkte, brutal-rücksichtslose Gewalt im Mittelpunkt, wenngleich sie an verschiedenen Stellen im Film durchbricht. Denn vorrangig geht es um die raffinierte Manipulation von digitalen Daten durch das flinke und offenkundig unüberbietbare Know-how des Top-Hackers Stanley Jobson: Dieser soll auf verdeckten Konten illegal angehäufte Dollar-Milliarden Regierungsgelder, die Scheinfirmen beim Drogenhandel erwirtschafteten, durch den simultanen Zugriff auf mehrere digitale Netzwerke und die geschickte Aktivierung eines Hydra-Wurms auf weltweit verteilte Privatkonten transferieren. Alles (vermeintlich oder tatsächlich) im Namen der Freiheit und Sicherheit der USA - das scheint jedenfalls der patriotisch gesinnte *bad guy* Gabriel die anderen glauben machen zu wollen.

Neben dem hier gewählten Beispiel *Passwort: Swordfish* ließen sich auch andere Produktionen aus den Traumfabriken Hollywoods anführen, die als Alpträume aus dem Cyberspace auf je ihre Weise den raffinierten und nicht selten bedrohlichen Kampf um digitale Informationen, ihre Manipulation, ihre Sabotage, ihre militär-strategische Operationalisierung, ihre geheimdienstliche Instrumentalisierung usw. thematisieren: so z.B. *Sneakers* (1991), *Hackers* (1995), *Das Netz* (1995), *Der Staatsfeind Nummer Eins* (1998), die deutsche Produktion *23 Nichts ist wie es scheint* (1998) und nicht zu vergessen den „Klassiker" *Wargames* (1982), der zwar eine besondere Zuspitzung in Zeiten des Kalten Krieges hatte, aber dennoch drastisch und auf seine Weise auf das Gefahrenpotential und die Eigendynamik der digitalen Vernetzung sowie den bedrohlichen Übergang der Virtualität in die Realität aufmerksam gemacht hat.

Mit dem hier knapp skizzierten Filmbeispiel lassen sich außer der cineastischen Einstimmung auf die Problematik und dem exemplarischen Verweis auf ihre Inszenierung in den Narrationen von Film und Literatur (als prominentes Beispiel etwa Henning Mankell, *Die Brandmauer/ Firewall*) unter anderem folgende Aspekte verdeutlichen und vornehmlich auf die Kontexte von *InfoWar, CyberWar* oder *NetWar* übertragen: Erstens gibt es trotz des subtilen, letztlich lautlosen und oftmals unsichtbaren Agierens im Cyberspace parallel dazu brutale und schonungslose und direkte Gewaltformen die über Waffen herkömmlicher Art realisiert werden. Dies gilt auch und gerade für den Bereich des *CyberWar,* der eben nicht, wie zuweilen mit überzeugter oder naiver Zuversicht oder auch sophistischem Zynismus vermerkt wurde, reale, blutige Kriege überflüssig werden lässt und daher abzulösen vermag. Nein, vielmehr erweisen sich Konzepte des *CyberWar* als integrative Elemente in den militärischen Strategien der Kriegsführung. Kurzum: Kampf und Krieg der Gegenwart und Zukunft sind und bleiben brutal und blutig. Zweitens sollte das lautlose digitale Agieren der *Cyberwarriors* per Mausklick, mittels Tastatur und bei einer guten Tasse Kaffee (oder wie in *Passwort: Swordfish* bei einer Flasche Wein) nicht darüber hinwegtäuschen, dass dessen Wirkungen äußerst dramatisch und lebensbedrohlich sein können und sich nicht nur auf den strategischen Vorteil eines Informationsvorsprungs oder gar das elegante Umbuchen von exorbitanten Geldbeträgen beschränken. Kaltblütiges Morden in *Passwort Swordfish,* face-to-face, schockiert, reißt emotional mit, während die feinsinnigen Netzaktivitäten des Spitzenhackers übers *Interface* im Film (und vermutlich auch in der Realität) uns im Grunde genommen kalt lassen. Während die Bilder extremer Gewalt unsere sinnliche Wahrnehmung voll in Anspruch nehmen, bleiben digitale Aktionen auffallend bildlos und lassen uns unberührt. Den meisten unter uns fehlt vermutlich jegliche technische Vorstellungsgabe, was real in den virtuellen Welten vor sich geht. Und wenige vermögen die konkreten Folgen in der wirklichen Welt abschätzen. Werden sie aber sichtbar, spürbar und sogar lebensbedrohlich, dann kommt es spätestens hier zum bösen Erwachen. Daher sollte man drittens gerade vor diesem Hintergrund möglichen Verharmlosungen widerstehen: Der Einsatz von Formen virtueller Gewalt ist nicht zuletzt von seinen faktischen Folgen in der realen Welt zu sehen und zu bewerten. Die fiktionale Unterhaltungsintention des Kinos ist zu unterscheiden von den realen Dimensionen digitaler Gefahrenpotentiale der Informations- und Kommunikationstechnik (fortan ICT) in der Wirklichkeit. Nichtsdestoweniger vermag die narrative Fiktion, auf die Realität aufmerksam zu machen, ohne dass daraus jedoch gleich Hysterien oder apokalyptische Szenarien entstehen müssten.[2]

II. Den Begriffsnebel lichten: Was meinen InfoWar, CyberWar, NetWar?

Oftmals verwendete Metaphern wie „elektronisches Pearl Harbor", „Achillesferse Internet" oder „virtueller Wilder Westen" scheinen gerade solche Hysterien oder apokalyptische Vorstellungen zu bedienen. Wer die Dinge jedoch kritisch genug wahrzunehmen und einigermaßen objektiv einzuschätzen vermag, wird schnell ihre alarmistische Instrumentalisierung in hochstilisierten Bedrohungsszenarien erkennen können, die einzig und allein dazu dienen sollen, restriktive Gegenmaßnahmen zu den digitalen Gefahren als absolut notwendig, plausibel und gerechtfertigt erscheinen zu lassen.[3] Um jedoch die tatsächliche Dimension der Gefahrenpotentiale fundiert einschätzen zu können, ist es angezeigt, die häufig schlagwortartig verwendeten Bezeichnungen nach ihrem begrifflichen Gehalt zu befragen. Mit *InfoWar, CyberWar* und *NetWar* haben sich drei ICT-dimensionierte „Kriegs"-Begriffe[4] etabliert. Was bedeuten sie? Welche Merkmale enthalten sie?

1. InfoWar

In *information warfare,* oder jüngst häufiger *InfoWar,* begegnet die allgemeinste Bezeichnung, etabliert seit mehreren Jahrzehnten, verwendet für alles Mögliche. Anfang der 1970er Jahre bezeichnete *information warfare* ganz allgemein die Rolle von Medien in der Kriegsführung. Die Verwendung im Sinne der computerbasierten militärischen Strategien und Waffensysteme kam in den 1980er Jahren durch entsprechende Nutzungsanalysen von US-Militärs auf.[5] Nicht verwundern kann, dass mit Blick auf den Bedeutungsgehalt von *InfoWar* (etwa aus militärtaktischen oder geheimdienstlichen Interessen) gerne Nebelkerzen gezündet werden. Warum? Bleibt das, was mit *InfoWar* gemeint ist oder gemeint sein könnte, im Nebulösen, dann die sind mit damit einhergehenden Gefahren und die in die Wege geleiteten Gegenmaßnahmen umso schwerer auszumachen.[6] Doch trotz dieses Vernebelungspotentials steht fest: Gegenstand von *information warfare* bzw. *InfoWar* sind nach heutigem Verständnis die Informationssysteme eines Gegners: genauerhin sein Kommando-System (C3I = *Command, Control, Communication and Intelligence*); zudem der Schutz des eigenen C3I-Systems vor fremdem Einflüssen und feindlichen Manipulationen; das Wissen um

Der Autor

Johannes J. Frühbauer, Studium der katholischen Theologie, Politikwissenschaft und Romanistik in Tübingen und Paris, ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Christliche Sozialethik an der Katholisch-Theologischen Fakultät der Universität Augsburg. Seine Themenschwerpunkte in Forschung und Lehre sind politische Ethik, interreligiöse Ethik, Friedensethik und Internetethik. Seine Dissertation „Gerechtigkeit denken. John Rawls' politische Philosophie aus sozialethischer Perspektive" erscheint 2005. Derzeit arbeitet er an einem Habilitationsprojekt zum Thema „Der Krieg und die Moral. Michael Walzers Beitrag zu einer internationalen Friedensethik". Für CONCILIUM schrieb er zuletzt über „Gerechtigkeitsmodelle in der gegenwärtigen Diskussion der politischen Philosophie" in Heft 2/1997. Anschrift: Universität Augsburg, Katholisch-Theologischen Fakultät, Universitätsstraße 10, D-86135 Augsburg. E-Mail: johannes.fruehbauer@kthf.uni-augsburg.de.

die ICT-Fähigkeiten des Gegners; die Weiterentwicklung der eigenen ICT-Potentiale und -Fähigkeiten und damit verbunden auch die Erhöhung der Robustheit der eigenen ICT-Systeme, was ein Erkennen der eigenen Verletzbarkeit und Fehlerpotentiale umfasst.[7] Zusammengefasst bedeutet *InfoWar* die Nutzung offensiver Maßnahmen gegen die ICT-Systeme des Gegners. Das Maßnahmenspektrum reicht hier vom direkten Einsatz gerichteter Energiewaffen zur zerstörerischen Erzeugung elektromagnetischer Impulse, über Computersabotage durch fehlerhafte Software und Viren bis hin zur Manipulation an Hard- und Software in allen Phasen der Produktion, des Vertriebs und des Einsatzes.[8]

2. CyberWar

Ausgehend vom Begriff des *information warfare* bzw. *InfoWar* hat sich in jüngerer Zeit die Bezeichnung *CyberWar* (und eher seltener *Cyberspace War*) entwickelt: Dieser scheint inzwischen der am häufigsten verwendete Terminus in der publizistischen und wissenschaftlichen Literatur zu sein.[9] Zuweilen scheint es, dass *Cyberwar* die Bezeichnung *InfoWar* abgelöst hat, zuweilen werden beide synonym nebeneinander verwendet. Das macht es nun umso schwieriger, ein jeweils klares begriffliches Profil zu gewinnen und die unterschiedlichen Termini aufgrund ihres semantischen Gehalts voneinander abzugrenzen. Die willkürliche und zuweilen metaphorische Verwendung für unterschiedlichste Inhalte und diffuse Vorstellungen lassen *CyberWar* als ebenso schwer fassbar erscheinen wie bereits den Terminus *InfoWar.* Noch stärker als bereits *InfoWar* und im Unterschied zu *NetWar* hat *CyberWar* eine eindeutig *militärische Dimension: CyberWar* wird gesehen als das neue Paradigma militärischer Konfrontation. In diesem basiert die Vorbereitung und Durchführung militärischer Operationen ganz wesentlich auf den Informations- und Kommunikationstechnologien und -systemen. Störung und Zerstörung informationeller Infrastruktur und Inhalte sind zentrale Elemente der Kriegsführung. Dabei gilt es, die Differenz des Wissens zu vergrößern: Angestrebt ist ein Maximum der Kenntnis über die eigene und gegnerische militärische Situation und zugleich die Minimierung der Informationsbasis des Feindes.[10] Diese *Fokussierung auf ICT-gestütztes Handlungswissen* generiert eine militärisch-operativ vorteilhafte Handlungsmacht: Denn Unwissenheit führt zunächst zur Desorientierung und daraus resultierend zur Handlungsohnmacht und Wehrlosigkeit des Gegners. Konventionelle militärische Parameter wie Truppenstärke und technische Ausrüstung haben allenfalls noch sekundäre Bedeutung. Primär wird die detaillierte Kenntnis dieser Parameter zum entscheidenden Faktor militärischen Agierens. Diese strategische ICT-Nutzung geht somit weit über ein mit computergesteuerten Waffen bevölkertes Schlachtfeld hinaus.[11]

Im konkreten Kriegshandeln setzt das *CyberWar*-Konzept die Vernetzung aller Akteure und Aktionsebenen mit dem Kommando- und Kontrollsystem voraus. Bernhard/Ruhmann zufolge sind zumindest zwei entscheidende militärische Vorteile zu nennen: Zum einen ermöglicht die optimale individuelle Situationskenntnis (*situational awareness*) verbunden mit dem Austausch von audiovisuellen Daten zu Position und Zustand dem einzelnen Soldaten die bestmögliche Kennt-

nis seiner Lage im Kriegsgeschehen; zum andern gewinnen die Entscheidungsträger auf der Führungsebene durch die ICT-gestützte Bündelung der Daten eine exakte Übersicht zur Gesamtlage (*top-sight*): „Die Kontrolle über alle Komponenten der eigenen Seite und die Kombination dieser Informationen mit Aufklärungsdaten ermöglicht den digitalen Feldherrenhügel."[12]

In einer systematischen Ausdifferenzierung unterscheiden Shimeall/Williams/Dunlevy drei graduell voneinander abgrenzbare Formen von *CyberWar:* Erstens lässt sich CyberWar ganz allgemein als ergänzendes Element zu konventionellen militärischen Aktionen verstehen. Vorrangiges Ziel besteht in der Informationsüberlegenheit bzw. -dominanz im Kriegskontext. Es gilt, den Kriegsnebel (*fog of war*) für den Feind zu verdichten und für die eigenen Reihen zu lichten. Zweitens kennzeichnet den begrenzten CyberWar (*limited cyber war*), dass dieser sich hinsichtlich der Aktionen und Wirkungen ausschließlich auf die informationelle Infrastruktur bezieht: Sie ist das Medium, das Ziel und schließlich auch die Waffe des Angriffs. Im Visier ist die Reduzierung der gegenerischen Effektivität, indem durch etwa eingeschleuste mangelhafte Software oder andere Sabotageakte vernetzte ICT-Aktivitäten gestört oder Datenmaterial beeinträchtigt werden. Von dieser begrenzten Form wird drittens der unbegrenzte CyberWar (*unrestricted cyberwar*) unterschieden: Dieser kennt keine Unterscheidung zwischen zivilen oder militärischen Zielen. Das führt in der Praxis zu direkt oder mittelbar verursachten realen physischen Wirkungen im Bereich der Luftverkehrskontrolle, des Notfallmanagements, der Wasserversorgung oder der Energiebereitstellung und nimmt infolgedessen im zivilen Bereich die existenzielle Bedrohung und den Verlust von Menschenleben in Kauf. Ergänzend zu diesen weit reichenden und über die Grenzen des militärischen Kriegsgeschehens hinausgehenden Störwirkungen können ökonomische und soziale Folgen tiefgreifend sein.[13] Diese Wirkungsdimensionen veranlassen Shimeall/Williams/Dunlevy schließlich zu der Forderung, den Cyberspace und seine virtuellen Welten in Verteidungsplanungen mit einzubeziehen, um die möglichen Schäden in der realen Welt so gut wie möglich zu begrenzen.

Unverkennbar begegnet im CyberWar eine komplexe Form kriegerischen Handelns: CyberWar ist ein Krieg vor dem Krieg, neben dem Krieg und im Krieg.

3. NetWar

In seiner strikten Informationsbezogenheit zielt *NetWar* auf das Wissen und Selbstbild des Konfliktgegners: Hier gilt es Einfluss zu nehmen, zu modifizieren, zu stören und zerstören. Dies geschieht nicht nur durch altehrwürdige Propagandamaßnahmen, sondern durch kommunikationstechnische Infiltration von Computernetzwerken und Datenbanken oder auch durch Unterstützung der favorisierten politischen Opposition und Befreiungsbewegungen über computerbasierte Netzwerke.[14] Mit anderen Worten: Maßnahmen ganz unterschiedlicher Art und ganz diverser Akteure gehen hier Hand in Hand. Maßnahmen, die mit Blick auf ihre Wirkweisen zudem Merkmale psychologischer Kriegsführung besitzen und doch darüber hinausgehen. Ein zentraler Konfliktgegenstand des NetWar

bildet die Frage nach Meinungsmacht. NetWar entzündet sich unter anderem an Kriegsvorbereitungen und -durchführungen, an Menschenrechtsverletzungen oder Umweltgefährdungen, wie sie etwa durch Atomtest in Kauf genommen werden. Vornehmlicher Kampfplatz des NetWar ist das Internet.

Wenngleich somit der Meinungsbildung und Einflussnahme auf die politische Öffentlichkeit im NetWar entscheidende Bedeutung kommt und sich die „Netzkrieger" sich im Gegensatz zum militärischen Kontext des CyberWar unter anderem aus zivilgesellschaftlichen Gruppen rekrutieren und mit eher zivilen Maßnahmen operieren, bleiben sabotageähnliche und den Netzbetrieb störende Aktivitäten nicht aus. Beispiele für derartige Aktivitäten im Kontext des NetWars finden sich im Kontext der Anti-Kriegs-Proteste gegen den Irakkrieg 2003. Hier konzentrierten sich Hacker-Aktivitäten beispielsweise darauf, die Abrufbarkeit von Webseiten (*web site defacement*) oder webgestützte Dienstleistungen (*denial-of-service attacks*) zu stören oder einen Internetwurm (*Scezda worm*) zu infiltrieren. Ziele waren vor allem Internetseiten öffentlicher Behörden oder kommerzieller Unternehmen.[15] Wenngleich diese NetWar-Aktivitäten eine eher geringe Bedrohungskapazität besitzen, lässt sich nicht abschätzen, welcher Wirkungsgrad erreicht werden könnte, wenn sich die unterschiedlichen netzmilitanten Gruppen koordinieren und durch konzertierte Aktionen wirken würden. Und sollte es überdies gelingen, digitalen Zugang zu GPS-Stationen zu erlangen[16], wäre nicht nur eine neue Stufe des NetWars erreicht, sondern im Grunde genommen einen Übergang zum CyberWar markiert.

Die terminologische Ausdifferenzierung bringt zwar den Vorteil, dass sich bestimme Formen einem der Begriffe zuordnen lassen, zugleich offenbart sich jedoch auch, dass durch zahlreiche Überlappungen der Phänomene und der fließenden Übergänge durch ähnliche Aktivitäten sowie durch den Einsatz desselben Arsenals an Waffen die Konturen drei skizzierten Begriffe stark verschwimmen. Daher ist zumindest anzufragen, ob eine Subsumierung sämtlicher Erscheinungsformen unter CyberWar nicht sinnvoller wäre und dass in einer zweifelsohne erforderlichen Differenzierung jeweils zwischen Akteuren und Aktionskontexten etwa militärisch, zivilgesellschaftlich, kommerziell usw. unterschieden würden. Eine Konzentrationen auf einen zentralen Begriff würde sich auch von den Gemeinsamkeiten in den Motiven und Zielen, Aktionen und Arsenalen, die sich trotz der unterschiedlichen Profile von InfoWar, CyberWar und NetWar identifizieren lassen, nahe legen.[17] Jedenfalls scheint die Begriffsbildung zum jetzigen Zeitpunkt, bei aller Tendenz hin zu „Cyber"-Terminologien, noch nicht abgeschlossen zu sein.

III. Vom CyberWar zum CyberPeace? Eine neuartige Herausforderung nicht nur für die Friedens- und Konfliktforschung

Das bestimmende Wahrnehmungs- und Reflexionsparadigma der Friedens- und Konfliktforschung der Gegenwart ist vornehmlich das Paradigma des „neuen Krieges". Seine zentralen Merkmale sind erstens die Entstaatlichung bzw. Privatisierung kriegerischer Gewalt und damit einhergehend der viel beschworene Verlust des staatlichen Gewaltmonopols, zweitens die Asymmetrisierung kriegerischer Gewalt - insofern weder gleichartige noch gleichgewichtige Gegner aufeinandertreffen -, und drittens die Verselbständigung bzw. Autonomisierung vormals militärisch kontrollierter und eingebundener Gewaltformen.[18] Obgleich es nicht zum Horizont der Erörterungen zum „neuen Krieg" gehört, ist augenscheinlich, dass die genannten Merkmale mutatis mutandis auch auf wesentliche Charakteristika in den Erscheinungsformen des CyberWars zutreffen. Doch diese Beobachtung sei nur en passant erwähnt. Unsere Blickrichtung gilt hier der generellen Aufmerksamkeit der Friedens- und Konfliktforschung für die Problematik des CyberWars.

Gegenüber einem ins Zentrum gerückten Stellenwert des religiös-kulturellen Konfliktfaktors hat die Aufmerksamkeit der Friedens- und Konfliktforschung für die reale Herausforderung des CyberWars derzeit noch stiefmütterlichen Charakter. So werden beispielsweise die Friedensgutachten der zurückliegenden Jahre als kollektive Stimme der deutschen Institute zur Friedens- und Konfliktforschung inhaltlich dominiert von den Entwicklungen (wohlgemerkt ohne Einbeziehung der ICT-Dimension!) in den steten Konfliktregionen Naher und Mittlerer Osten sowie von der Frage, wie dem internationalen Terrorismus nach dem 9. 11. 2001 wirksam zu begegnen ist.[19]

Nur am Rande sei vermerkt, dass auch die wissenschaftliche Aufmerksamkeit der Informationsethik, Cyberethik oder Internetethik zur Problematik des CyberWars auffallend zurückhaltend ist. Im Zentrum der Darstellungen finden sich entweder theoretisch akzentuierte und nicht selten philosophisch angehauchte Grundlagenfragen, eine für das Internet adaptierte Fortschreibung medienethischer Fragestellungen oder die Problematisierung praktischer Herausforderungen, wie sie unter vielem anderem im digital divide oder in Fragen des Kinder- und Jugendschutzes stehen.[20]

Mit Blick auf konventionelle Konflikte und Kriege ist es zur plausiblen Selbstverständlichkeit geworden, neben den Analysen der Konfliktursachen und Strategien der Konfliktbearbeitungen auch stets die Reflexion auf die Perspektive des Friedens mit einzubeziehen: Welche Gelingensbedingungen für eine friedliche und zivile Konfliktbearbeitung sind erforderlich? Wie lässt sich Frieden gewinnen und stabilisieren? Doch hat diese enge Verbindung zwischen Krieg und Frieden auch Geltung in den Welten des Cyberspace? Will und kann die Rede vom *CyberPeace* mehr sein als bloße Rhetorik? Ein kurzer Blick auf die Debatte zum

CyberPeace erschließt uns zunächst folgende zentralen Erkenntnisse: Erstens existiert Einsicht in die Notwendigkeit, auch den Cyberspace, das *Web*, das Internet oder wie immer wir diese virtuellen Räume der Digitalisierung bezeichnen, in friedenspolitische, -ethische und -pädagogische Konzeptionen einzubeziehen. Dass diese Einsicht jedoch nicht von allen Seiten geteilt wird, dürfte kaum verwundern. Denn unübersehbar gibt es handfeste Interessen, an den Möglichkeiten des CyberWars, aber auch an der Aufrechterhaltung seiner Schreckensdimension, mit der restriktive Maßnahmen im Namen von Sicherheit und Freiheit gerechtfertigt werden können, festzuhalten. Zweitens gibt es offenkundig „Definitionsprobleme", die eine Abgrenzung der militärischen zur zivilen Nutzung des ICT derzeit als schwierig erscheinen lassen. Drittens ist die Verlagerung der Debatte über den CyberWar auf den Sektor des Cybercrime höchst umstritten. Während die eine Seite unterstreicht, dass mit internationalen Cybercrime-Abkommen und dem daraus kodifizierbaren Strafrecht den Aktivitäten deutlich besser beizukommen sei, als mit Instrumenten hoch angesiedelter Sicherheitspolitik, verweisen Kritiker dieser Verschiebung der Diskussion darauf, dass durch die Umsetzung der geplanten Vorschriften mit Einschnitten in den generell erwünschten freien Informationsfluss, bei Bürgerrechten und beim Schutz der Privatssphäre zu rechnen sei und überdies problematischerweise gerade staatliche Akteure von den geplanten Abkommen ausgenommen würden. Viertens erweist es sich augenscheinlich als äußerst schwierig, klassische Rüstungskontrollmethoden auf den Kontext von ICT und die Herausforderung des CyberWar zu übertragen.[21]

Welche konkreten Perspektiven zur Realisierung von CyberPeace lassen sich aus heutiger Sicht benennen? Ein erster Schritt ist in einschlägigen Deklarationen oder Memoranden zu sehen, die an die friedliche Nutzung des Cyberspace appellieren und Impulse für ein entsprechendes friedensorientiertes Bewusstsein und auch für Friedensprozesse geben.[22] Ein weiterer friedensförderlicher Schritt besteht darin, den Import übersteigerter amerikanischer Bedrohungsszenarien nach Europa zu vermeiden, um Plädoyers für den CyberWar und dessen Konzeptionalisierungen den Boden zu entziehen. Drittens wird als ein ganz zentraler Schritt gesehen, wenn es gelänge, den Schutz kritischer nationaler Infrastrukturen (Wasser- und Energieversorgung) im völkerrechtlichem Rahmen zu normieren und von CyberWar-Aktivitäten auszunehmen. Viertens ist es folglich für einen CyberPeace zuträglich, wenn sich Cracks und Hacker dazu verpflichten, gerade die kritischen Infrastrukturen aus ihren Aktivitäten auszunehmen.[23]

Halten wir abschließend fest: Den vielschichtigen Realitäten und Gefahrenpotentialen des CyberWar die Forderung nach einem CyberPeace entgegenzustellen erscheint notwendig und berechtigt, selbst wenn hier ein David einem Goliath begegnet. Um eine realistische Perspektive zu haben, um wirksam werden zu können, bedarf es fraglos der gemeinsamen Anstrengungen der Beteiligten und Betroffenen. Die Herausforderung zu einem CyberPeace gilt es auf mindestens vier Ebenen in den Blick, ja in Angriff zu nehmen: ethisch, politisch, rechtlich und technisch. *Ethisch* durch die Auseinandersetzung mit den Aspekten von Freiheit,

Privatheit, Sicherheit, Macht und Menschenrechte, aber auch durch die Frage nach dem Wahrheitsgehalt von Information und ihrer Manipulation; Schutz und Sicherheit des Individuums wie auch gesellschaftlich-ziviler Einrichtungen (Stichwort: Schutz „kritischer Infrastrukturen"[24]) stehen hier im Vordergrund. *Politisch* insofern die aus der ethischen Reflexion gewonnen normativen Einsichten und die aus dem zivilgesellschaftlichem Diskurs hervorgehenden Positionen in konkretes Handeln umzusetzen sind, möglichst mit international erarbeiteten und abgestimmten Agenden. *Rechtlich* insofern die als notwendig erkannten Maßnahmen konkrete einklagbare und sanktionsfähige Rechtsgestalt annehmen. *Informations- und kommunikationstechnisch* gilt es über das Know-how jene Maßnahmen durchzuführen, die sich auf den rein technischen Bereich beziehen (etwa alles rund um Sicherheit).

Die reale Welt wird mit den Wirklichkeiten des CyberWar leben müssen. Die Forderung nach einem CyberPeace jedoch schafft allerdings ein sensibles und kritisches Bewusstsein für die Problematik des CyberWar, und mehr noch: Über internationale Verständigungs- und Verpflichtungsprozesse könnte es gelingen, die Spielräume für Strategien und Aktionen des CyberWar weitmöglichst zu begrenzen. Ultimatives Ziel der Entwicklung im ICT-Bereich darf nicht die Militarisierung, sondern kann nur die Zivilisierung der Informationsgesellschaft sein.[25]

[1] Gleich zu Beginn sei darauf hingewiesen, dass gedruckte Publikationen zur Thematik rund um Cyberwars alles andere als Legion sind. Eine Vielzahl an Informationen und fundierten Beiträgen zur Thematik findet sich jedoch gewissermaßen naturgemäß in den Netzwelten des Cyberspace; dies erklärt, warum im Folgenden etliche Referenzen zur Frage des CyberWar auf Fundorte im World Wide Web und eher selten auf physisch greifbare Publikationen verweisen. Unter diesen „Raritäten" geben beispielsweise einen Überblick zur Problematik und zu den „kriegerischen" Aktivitäten im Kontext der Informations- und Kommunikationstechnik (ICT): Jean Guisnel, *CyberWars. Espionage on the Internet,* Cambridge/Mass. 1999; Winn Schwartau, *Cybershock. Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption,* New York 2000.

[2] Vgl. hierzu: Thomas Hausmanninger, *Amerikanische Apokalypsen. Theologisch-ethische Überlegungen zu katastrophischen Narrationen in den USA,* in: Franz Sedlmeier/ders. (Hg.), Inquire Pacem. Beiträge zu einer Theologie des Friedens, Augsburg 2004, 317-347 (Lit. !).

[3] Vgl. Jean Guisnel, *CyberWars. Espionage on the Internet,* aaO., 47ff et passim.

[4] Ich umgehe hier eine ausführliche komparativ orientierte Analyse des „klassischen" Verständnisses von Krieg und des sich entwickelten Bedeutungsgehaltes von „Krieg" in *InfoWar, CyberWar* und *NetWar;* nichtsdestoweniger bin ich mir der (an dieser Stelle nicht zu realisierenden) Notwendigkeit einer solchen begrifflichen Ermittlung und Profilierung sowie der daraus resultierenden Abgrenzung bewusst.

[5] Ute Bernhardt/Ingo Ruhmann, *Krieg und Frieden im Internet,* 1998, in: www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=6271 (Zugriff: 30.11.2004); siehe dort auch die weiteren Verweise auf einschlägige Quellen.

[6] Vgl. ebd.

[7] Vgl. ebd.

[8] Vgl. ebd. Hier finden sich auch Angaben zu weiteren konkreten technischen Maßnahmen im InfoWar.

[9] Auch die Titelformulierung dieses Themenheftes spiegelt diese bevorzugte sprachliche Fokussierung auf die „Cyber"-Bezeichnung wider.

[10] Vgl. Ute Bernhardt/Ingo Ruhmann, *Krieg und Frieden im Internet*, aaO.

[11] Vgl. ebd.

[12] Ebd.

[13] Vgl. Timothy Shimeall/Phil Williams/Casey Dunlevy, *Countering Cyber War*, in: NATO Review, Winter 2001/2002, in: www.cert.org/archive/pdf/counter_cyberwar.pdf (Zugriff 16. 12. 2004).

[14] Vgl. Ute Bernhardt/Ingo Ruhmann, *Krieg und Frieden im Internet*, aaO.

[15] Vgl. Joab Jackson, *All Quiet on the Cyber-War Front*, in: www.washingtontechnology.com/news/1_1/daily_news/20474-1.html.

[16] Vgl. ebd.

[17] Vgl. hierzu die hilfreiche systematische Zusammenstellung und Ordnung der Phänomene bei Thomas Hausmanninger, *Amerikanische Apokalypsen*, aaO., 335f.

[18] Vgl. Herfried Münkler, *Die neuen Kriege*, Reinbek 2002, 10f.

[19] Siehe hierzu etwa die *Friedensgutachten 2001, 2002, 2003* und *2004*, hg. von Christoph Weller/ Bruno Schoch/Corinna Hausdewell/Reinhard Mutz u.a., Münster.

[20] Vgl. Thomas Hausmanninger/Rafael Capurro (Hg.), *Netzethik. Grundlegungsfragen der Internetethik*, München 2002; vgl. Thomas Hausmanninger (Hg.), *Handeln im Netz. Bereichsethiken und Jugendschutz im Internet*, München 2003; vgl. Rupert M. Scheule/Rafael Capurro/Thomas Hausmanninger (Hg.), *Vernetzt gespalten. Der Digital Divide in ethischer Perspektive*, München 2004.

[21] Vgl. Stefan Krempl, *Im Trippelschritt zum Cyberpeace*, in: www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=3616 (Zugriff: 18. 12. 2004); vgl. auch die Infopeace-Erklärung des Chaos Computer Club unter: http://ccc.de/CRD/CRD990107.html (Zugriff 18. 12. 2004).

[22] Vgl. Stefan Krempl, *Im Trippelschritt zum Cyberpeace*, aaO.

[23] Vgl. ebd.

[24] Weiterführende Informationen hierzu siehe: www.bsi.bund.de/fachthem.kritis/links.htm (Zugriff 30. 11. 2004).

[25] Vgl. Ute Bernhardt/Ingo Ruhmann, *Krieg und Frieden im Internet*, aaO.