John Arquilla/David Ronfeldt
Der Cyberkrieg kommt!*

"Wissen muß zu Können werden."
Carl von Clausewitz, Vom Kriege

Neue Formen des militärischen Konflikts

Nehmen wir einmal an, ein Krieg würde so aussehen: Zahlenmäßig kleine, leichtbewaffnete, hochmobile Streitkräfte besiegen massive, schwerbewaffnete, eingegrabene feindliche Truppen und zwingen sie zur Kapitulation, wobei auf beiden Seiten kaum menschliche Verluste zu beklagen sind. Den mobilen Truppen gelingt dies, weil sie gut vorbereitet sind, Raum für Manöver schaffen, ihre geballte Feuerkraft rasch und unerwartet einsetzen und über überlegene Kommando-, Kontroll- und Informationssysteme verfügen. Letztere sind dezentralisiert, um taktische Initiativen zu ermöglichen, und verschaffen den zentralen Befehlshabern dennoch auf beispiellose Weise Geheiminformationen und "Gesamtübersicht" für strategische Zwecke.

Kriegsführung hängt nicht mehr in erster Linie davon ab, wer auf dem Schlachtfeld das meiste Kapital, den meisten Einsatz und die meiste Technologie aufbietet, sondern davon, wer die besten Informationen über das Schlachtfeld hat. Die Sieger erkennt man daran, wie sie diese Informationen handhaben — nicht nur in der banalen Frage, wie man den Feind aufspürt, während man selbst im Verborgenen bleibt, sondern auch in Doktrin und Organisation. Das Ganze gleicht einer Schachpartie, bei der man selbst das ganze Brett, der Gegner jedoch nur seine eigenen Figuren sieht; in so einem Fall kann man sogar dann gewinnen, wenn der Gegner zusätzliche Schwerfiguren verwenden darf.

Es mag so aussehen, als ob wir aus dem US-Sieg über den Irak im Golfkrieg extrapolierten, doch greifen wir für unsere Vorstellungen eher das Beispiel der Mongolen aus dem 13. Jahrhundert auf. Deren "Horden" waren ihren Gegnern fast immer zahlenmäßig unterlegen, konnten aber dennoch das größte Kontinentalreich, das es je gab, erobern und über hundert Jahre halten. Der Schlüssel zum Erfolg der Mongolen lag darin, daß sie die absolut besten Informationen über das jeweilige Schlachtfeld hatten. Sie schlugen zu, wann und wo sie es für richtig hielten, und ihre "Blitzkuriere" ermöglichten es den oft hunderte Meilen voneinander entfernten Feldkommandanten, täglich zu kommunizieren. Sogar der oft Tausende Meilen entfernte Große Khan wußte innerhalb weniger Tage über die neuesten Entwicklungen im Felde Bescheid.

Nach dem Wegfall der aufstachelnden Bedrohung durch die Sowjetunion werden die USA nun dem innenpolitischen Druck nachgeben und versuchen, in Zukunft mit weniger Militär auszukommen. Das Kriegsführungspotential, das wir uns vorstellen, ist zwar durch das Beispiel der Mongolen inspiriert, ergibt sich jedoch in erster Linie aus unserer Analyse der Informationsrevolution und könnte es Amerika ermöglichen, sich, seine Freunde und seine weitgesteckten Interessen unabhängig von der Größe und Stärke potentieller zukünftiger Gegner zu verteidigen.

Der Fortschritt von Technologie und Wissen

Im Laufe der Geschichte haben militärische Doktrin, Organisation und Strategie tiefgreifende Veränderungen durchgemacht, die zum Teil auf bahnbrechenden technischen Neuerungen begründet waren. Von der griechischen Phalanx über die Kombination von Kanone und

Segelschiff, die "Levée en masse" und den Blitzkrieg bis hin zum "Strategic Air Command" bietet die Geschichte zahlreiche Beispiele dafür, daß sich auf der Basis neuer Waffen-, Antriebs-, Kommunikations- und Transporttechnologien ein doktrineller, organisatorischer und strategischer Wandel vollzog, der die innovative Seite in die vorteilhafte Lage versetzte, erschöpfende Zermürbungsschlachten vermeiden und statt dessen einen "Entscheidungskrieg" führen zu können.[1]

Heute erleben wir, wie sich eine Vielzahl neuer Technologien etablieren und weitere Innovationen vor der Tür stehen. Am verlockendsten erscheinen z.B. hochexplosive nicht-atomare Sprengstoffe, präzisionsgesteuerte Munitionen, Tarnbauweisen für Flugzeuge, Panzer und Schiffe, funkelektronische Kampfsysteme (REC), neue Elektronik zur Informationsbeschaffung, Störung und Täuschung, neue Informations- und Kommunikationssysteme zur Verbesserung von Kommando-, Kontroll-, Kommunikations- und Informationsfunktionen (C3I), sowie futuristische Pläne für weltraumgestützte Waffen und zur automatisierten bzw. robotischen Kriegsführung. Zusätzlich werden VR-Systeme zu Simulations- und Trainingszwecken entwickelt. Viele dieser Neuerungen fügen sich in die gängige Vorstellung von einer militärtechnologischen Revolution (MTR) ein.[2]

Die Zukunft des Krieges — insbesondere der Fähigkeit der USA, Kriege vorauszusehen und zu führen — wird zum Teil davon abhängen, wie diese technologischen Neuerungen bewertet und benutzt werden. Doch die Technologie durchdringt den Krieg nur, beherrscht ihn aber nicht, wie Militärhistoriker häufig betonen. Worauf es ankommt, ist nicht die Technologie an sich, sondern eher, im weitesten Sinne, die Organisation derselben. Russell Weigley beschreibt die Situation wie folgt:

> … die Kriegstechnologie besteht nicht nur aus Instrumenten, die in erster Linie der Kriegsführung dienen. Die Fähigkeit einer Gesellschaft, Krieg zu führen, hängt von allen Facetten ihrer Technologie ab: von Straßen und Transportfahrzeugen, Landwirtschaft, Industrie sowie der Art und Weise, wie diese Technologie organisiert wird. Um mit Van Creveld zu sprechen: "Hinter der militärischen Hardware steht allgemeine Hardware, und hinter dieser steht die Technologie als eine bestimmte Form von Know-how, als eine Weltsicht und eine Methode der Problembewältigung."[3]

Unserer Meinung nach stellt die Informationsrevolution jenen technologischen Wandel dar, der dieser allgemeinen Anschauung entspricht. Sie wird den nächsten großen Wandel im Wesen des militärischen Konfliktes und der Kriegsführung mit sich bringen.

Auswirkungen der Informationsrevolution

Die Informationsrevolution spiegelt den Fortschritt computerisierter Informations- und Kommunikationstechnologien wider, sowie die damit verbundenen Innovationen in der Organisations- und Managementtheorie. Hinsichtlich der Art und Weise, wie Informationen gesammelt, gespeichert, verarbeitet, vermittelt und präsentiert werden und wie Organisationen auf die Nutzung des wachsenden Informationsangebots ausgelegt werden, sind umwälzende Veränderungen zu verzeichnen.[4] Information wird zur strategischen Ressource, die sich im postindustriellen Zeitalter als ebenso wertvoll und einflußreich erweisen könnte wie Kapital und Arbeitskraft im Industriezeitalter. Fortschrittliche Informations- und Kommunikationssysteme können bei richtiger Anwendung die Effizienz zahlreicher Aktivitäten steigern. Aber Effizienzsteigerung ist nicht ihre einzige oder gar beste Auswirkung. Darüber hinaus wirkt die neue Technologie auch transformierend, indem sie alte Denk- und Vorgangsweisen aufbricht, neue Handlungsmöglichkeiten eröffnet und Anregungen dafür bietet, wie sich durch geänderte Vorgangsweisen bessere Resultate erzielen lassen:

Bei den Folgen einer neuen Technologie ist es nützlich, zwischen Auswirkungen ersten Grades, d.h. auf Effizienzebene, und solchen zweiten Grades, d.h. auf der Ebene des Gesellschaftssystems, zu unterscheiden. Wie die Geschichte früherer Technologien zeigt, neigt man beim Aufkommen einer neuen Technologie dazu, sich auf die Effizienzebene zu konzentrieren und die potentiellen Auswirkungen auf das Gesellschaftssystem zu unterschätzen oder gänzlich zu übersehen. Aufgrund fortschrittlicher Vernetzungstechnologien lassen sich heute Menschen, ebenso wie Datenbanken und Prozessoren, als Ressourcen in einem Netzwerk auffassen.

Viele Organisationen installieren heute aus Effizienzgründen elektronische Netzwerke. Angestellte, die nun erstmals E-mail und andere vernetzte Anwendungen einsetzen, können dadurch effizienter arbeiten und z.B. Transaktionen weitaus rascher durchführen. Betrachtet man nicht nur die Effizienzsteigerung, sondern auch die Veränderungen in Verhalten und Organisation, so wird deutlich, mit welchen Auswirkungen zweiten Grades zu rechnen ist. Durch die neuen Technologien werden sich andere Formen der Zeiteinteilung und des Wissens sowie andere Bekanntschaften und andere Interessen ergeben. Der volle Nutzen — und die Schwierigkeiten — all dessen werden davon abhängen, wie sehr diese Technologien die Menschen in ihrem Denken und in ihrer Zusammenarbeit beeinflussen — also in den Auswirkungen zweiten Grades.[5]

Sowohl in technologischer als auch in nicht-technologischer Hinsicht setzt die Informationsrevolution Kräfte frei, die zahlreiche Institutionen strukturell verändern werden. Die grundlegenden hierarchischen Strukturen dieser Institutionen werden nun durch die Informationsrevolution gestört und angegriffen. Macht wird diffundiert und neu verteilt, oft zum Vorteil von vermeintlich schwächeren und kleineren Akteuren. Die Informationsrevolution ist grenzüberschreitend und definiert neue Grenzen für Ämter und Zuständigkeitsbereiche. Sie erweitert den von den jeweiligen Akteuren zu berücksichtigenden räumlichen und zeitlichen Horizont und zwingt so geschlossene System ganz allgemein zu größerer Offenheit. Doch obwohl sich daraus insbesondere für große, bürokratische, in die Jahre gekommene Institutionen Schwierigkeiten ergeben, wird die institutionelle Form an sich dadurch nicht obsolet. Für die Organisation unserer Gesellschaft bleiben Institutionen jeder Art weiterhin von wesentlicher Bedeutung. Die aufgeschlossenen, lernfähigen Institutionen werden ihre Strukturen und Vorgangsweisen an das Informationszeitalter anpassen. Viele werden von den traditionellen hierarchischen Organisationsmodellen zu neuen, flexiblen, vernetzten Formen übergehen. Wer es lernt, hierarchische Prinzipien und Netzwerkprinzipien miteinander zu verknüpfen, wird erfolgreich sein.[6]

Inzwischen wird gerade durch jene Veränderungen, welche den Institutionen Probleme bereiten, wie z.B. durch den Angriff auf die hierarchische Struktur, der Aufstieg organisationsübergreifender Netzwerke begünstigt. Tatsächlich festigt die Informationsrevolution die Bedeutung von Netzwerken jeglicher Form, wie etwa von sozialen oder Kommunikationsnetzwerken. Die Form des Netzwerks unterscheidet sich beträchtlich von der Form der Institution. Während (vor allem große) Institutionen sich traditionellerweise auf Hierarchien stützen und selbständiges Handeln anstreben, bestehen organisationsübergreifende Netzwerke aus (oft kleinen) Organisationen oder Teilen von Institutionen, die sich zum Zweck gemeinsamen Handelns zusammenschließen. Die Informationsrevolution begünstigt das Wachstum solcher Netzwerke, da sie unterschiedlichen, weit verstreuten Akteuren die Zusammenarbeit über größere Entfernungen hinweg ermöglicht und ihnen als Basis für Kommunikation, gegenseitige Beratung, Koordination und Kooperation ein größeres und besseres Informationsangebot zur Verfügung stellen kann als je zuvor.[7]

All das wirkt sich direkt auf die Zukunft des Militärs sowie auf die Zukunft des militärischen Konflikts und der Kriegsführung im allgemeinen aus.

Mit Netzkrieg und Cyberkrieg müssen wir rechnen

Die These dieses Artikels lautet, daß sich aufgrund der Informationsrevolution für einzelne Gesellschaften neue Konfliktformen sowie für ihre Truppen neue Formen der Kriegsführung ergeben werden. Wir schlagen vor, zwischen "Netzkrieg" — ideelle gesellschaftliche Konflikte, die z.T. durch vernetzte Kommunikation ausgetragen werden — und "Cyberkrieg" — auf militärischer Ebene — zu unterscheiden. Diese Begriffe sind zugegebenermaßen neu, und vielleicht finden sich in Zukunft noch bessere.[8] Inzwischen mögen sie jedoch dazu dienen, eine sinnvolle Unterscheidung zu treffen und das breite Spektrum der durch die Informationsrevolution zu erwartenden Veränderungen im Wesen, im Kontext und in der Handhabung militärischer Konflikte zu durchleuchten.[9]

Während sich Netzkrieg und Cyberkrieg um Information und Kommunikation drehen, zeichnet sich dahinter ein "Wissenskrieg" ab, in dem es darum geht, wer was, wann, wo und warum weiß und wie sicher Gesellschaft bzw. Militär sich ihres Wissens über sich selbst und ihre Gegner sein können.[10]

Was ist Netzkrieg?

Unter Netzkrieg verstehen wir großangelegte informationsbezogene Konflikte zwischen Staaten oder Gesellschaften. Dabei geht es darum, das tatsächliche oder vermeintliche Wissen einer Zielbevölkerung über sich und ihre Umwelt zu stören, zu beschädigen oder zu modifizieren. Zielscheibe eines Netzkrieges könnte die öffentliche Meinung oder die Meinung der Elite sein oder beides. Dazu können staatliche diplomatische Maßnahmen ebenso gehören wie Propaganda, psychologische Kampagnen, politische und kulturelle Subversion, Täuschung oder Störung lokaler Medien, Infiltration von Computernetzwerken und Datenbanken sowie Bemühungen, über Computernetzwerke regierungsfeindliche oder oppositionelle Bewegungen zu fördern. Eine Strategie des Netzkrieges kann also darin bestehen, eine Reihe bereits bekannter, bisher jedoch unabhängig voneinander eingesetzter Maßnahmen unter einem neuen Gesichtspunkt zusammenzufassen.

Der Netzkrieg stellt mit anderen Worten eine Ergänzung im Spektrum möglicher Auseinandersetzungen dar, welches wirtschaftliche, politische, gesellschaftliche und militärische Formen des "Krieges" umfaßt. Im Gegensatz zu Wirtschaftskriegen, die die Produktion und Verteilung von Waren anvisieren, und politischen Kriegen, die sich gegen die Führungsspitze und die Institutionen einer Regierung richten, wären Netzkriege daran zu erkennen, daß sie auf Information und Kommunikation abzielen.

Wie andere in diesem Spektrum vertretene Konfliktformen wären Netzkriege großteils nichtmilitärisch, könnten jedoch Dimensionen annehmen, wo eine Überschneidung mit militärischen Konflikten möglich wäre. So kann ein Wirtschaftkrieg z.B. Handelsbeschränkungen, Schleuderexporte, Unterwanderung der Geschäftsbereiche und Märkte des Ziellandes sowie Technologiediebstahl umfassen, ohne daß in eine dieser Aktivitäten Truppen eingebunden sein müssen. Es kann aber in einem Wirtschaftskrieg auch zu bewaffneten Blockaden oder zur strategischen Bombardierung von Wirtschaftsgütern kommen, also zu einem militärischen Konflikt. Ebenso kann sich ein Netzkrieg, in dessen Verlauf die militärischen C3I-Kapazitäten des Feindes ins Visier genommen werden, zumindest teilweise in einen Cyberkrieg verwandeln.

Die Formen des Netzkrieges werden von den jeweiligen Akteuren abhängen. In gewisser Hinsicht sind die Regierungen der USA und Kubas bereits in einen Netzkrieg verwickelt. Das äußert sich auf US-Seite in den Aktivitäten von Radio & TV Marti, und auf der Seite Castros durch die Aktivitäten weltweiter pro-kubanischer Unterstützungsnetzwerke.

Andere Formen des Netzkrieges könnten sich zwischen Regierungen und nichtstaatlichen Akteuren ergeben. So können z.B. Regierungen einen Netzkrieg gegen verbotene Gruppen und Organisationen führen, die in Terrorismus, Handel mit Massenvernichtungswaffen oder Drogenschmuggel verwickelt sind. Andererseits kann der Netzkrieg von Gruppen und Bewegungen, die z.B. für Umweltschutz, Menschenrechte oder religiöse Anliegen eintreten, im Kampf gegen die Politik gewisser Regierungen eingesetzt werden. Diese nichtstaatlichen Akteure können in großen transnationalen Netzwerken und Koalitionen organisiert sein.

Eine andere Form des Netzkrieges kann zwischen rivalisierenden nichtstaatlichen Akteuren auftreten, wobei die Regierungen an Seitenfronten aufmarschieren, um eine zusätzliche Beeinträchtigung nationaler Interessen zu verhindern oder auch eine der beiden Seiten zu unterstützen. Obwohl dies die spekulativste Form des Netzkrieges darstellt, zeichnen sich besonders bei den weltweiten Interessensgruppen bereits grundlegende Elemente dafür ab. Einige Bewegungen entwickeln sich immer mehr zu grenzübergreifenden Netzwerken und Koalitionen, die sich eher mit der zivilen Gesellschaft (ja sogar einer globalen zivilen Gesellschaft) als mit Nationalstaaten identifizieren und zur Forcierung ihrer Aktivitäten fortschrittliche Informationstechnologien anwenden. All das könnte sich leicht als nächste große Front für ideologische Konflikte erweisen, wobei der Netzkrieg das Hauptcharakteristikum darstellen würde.

Die meisten Netzkriege werden wahrscheinlich gewaltfrei sein, aber es ist durchaus denkbar, daß sich aus der Kombination der jeweiligen Möglichkeiten im schlimmsten Fall sehr unangenehme Low-Intensity-Konflikte ergeben. In diesem Zusammenhang stellt Martin Van Creveld[11] besorgt fest: "Die Kriege der Zukunft werden nicht von Armeen geführt werden, sondern von Gruppen, die wir heute als Terroristen, Guerilleros, Banditen und Räuber bezeichnen, die sich jedoch selbst zweifellos offiziellere Namen geben werden." Seiner Ansicht nach werden Kriege zwischen einzelnen Staaten von der Bildfläche verschwinden und der Staat als wichtigste Form gesellschaftlicher Organisation wahrscheinlich obsolet werden. Im großen und ganzen teilen wir Van Crevelds Ansicht, glauben jedoch nicht, daß der Staat auch nur potentiell obsolet ist. Vielmehr wird er im Zuge dieser Entwicklungen eine Veränderung durchmachen.

Einige Netzkriege werden sich auch mit militärischen Fragen befassen, die eine potentielle Bedrohung der internationalen Ordnung und nationalen Sicherheit darstellen, wie etwa die Weitergabe von Atomwaffen, Drogenschmuggel und Terrorismus. Außerdem werden umfassendere gesellschaftliche Trends (z.B. die Neudefinition von Sicherheitskonzepten, die neue Rolle der Interessensgruppen, das Verwischen der traditionellen Grenzen zwischen militärischem und nicht-militärischem, öffentlichem und privatem, staatlichem und gesellschaftlichem Raum) zumindest bei Teilen des Militärs das Interesse wecken, sich aktiv mit einigen Aspekten des Netzkrieges zu befassen.

Netzkriege sind keine echten Kriege im herkömmlichen Sinn, könnten aber zu einem Instrument werden, mit dem man echte Kriege im Keim ersticken kann. In einer chaotischen Welt kann Abschreckung ebensogut eine Funktion der Cyberbereitschaft und Cyberpräsenz wie der Truppenbereitschaft und Truppenpräsenz sein.

Was ist Cyberkrieg?

Unter Cyberkrieg verstehen wir die informationsbezogene Durchführung bzw. Vorbereitung von Militäreinsätzen, d.h. die Unterbrechung oder besser Zerstörung der für das Selbstverständnis des Gegners — d.h. zur Beantwortung der Fragen, wer er ist, wo er ist, was

er wann tun kann, warum er kämpft, welchen Bedrohungen er sich zuerst stellen soll, usw. — unerläßlichen Informations- und Kommunikationssysteme, ja, im weiteren Sinne sogar seiner militärischen Kultur. Cyberkrieg impliziert das Bemühen, den Gegner völlig zu durchschauen und dabei selbst so wenig wie möglich preiszugeben, d.h. das "Wissens- und Informationsgleichgewicht" zum eigenen Vorteil zu manipulieren, vor allem wenn das Kräftegleichgewicht zugunsten des Gegners ausfällt, oder mit anderen Worten, Wissen einzusetzen, um den Aufwand an Kapital und Einsatz gering zu halten.

Bei dieser Art der Kriegsführung können verschiedenste Technologien zum Einsatz kommen, vor allem solche für C3I-Zwecke: zur Erfassung, Verarbeitung und Weiterleitung von Nachrichten, zur taktischen Kommunikation, Positionierung und Freund-Feind-Identifikation (IFF) sowie für "intelligente" Waffensysteme, um nur einige Beispiele zu nennen. Weiters besteht die Möglichkeit, die Schaltkreise der gegnerischen Information und Kommunikation elektronisch zu bluffen, stören, täuschen, überlasten oder zu unterwandern. Dennoch ist der Cyberkrieg mehr als eine Reihe technologischer Maßnahmen und sollte auch nicht mit den veralteten Konzepten der computerisierten, automatisierten, robotischen oder elektronischen Kriegsführung verwechselt werden.

Der Cyberkrieg mag für die militärische Organisation und Doktrin ein weitverzweigtes Betätigungsfeld darstellen. Wie erwähnt, findet sich in den einschlägigen Werken zum Thema Informationsrevolution die Forderung nach organisatorischen Neuerungen, etwa dergestalt, daß die einzelnen Teile einer Institution eher als zusammenhängende Netzwerke denn als separate Hierarchien funktionieren. In diesem Sinne könnte der Cyberkrieg eine institutionelle Neugestaltung des Militärs sowohl innerhalb als auch zwischen den einzelnen Teilstreitkräften erfordern. Der Übergang zu vernetzten Strukturen mag eine gewisse Dezentralisierung von Kommando und Kontrolle erfordern, was angesichts der früher vertretenen Ansicht, auf der Basis neuer Technologien wäre eine stärkere zentrale Kontrolle von Militäreinsätzen möglich, sehr wohl Widerstand hervorrufen könnte. Aber Dezentralisierung ist noch nicht alles; die neue Technologie ermöglicht auch eine bessere "Gesamtübersicht", ein zentrales Verständnis der Gesamtsituation, welches das Komplexitätsmanagement entscheidend verbessert.[12] Viele Abhandlungen zum Thema der organisatorischen Umgestaltung ergehen sich in Lobeshymnen auf die Dezentralisierung. Aber Dezentralisierung allein ist nicht der Schlüssel. Dezentralisierung führt erst in Verbindung mit "Gesamtübersicht" wirklich zum Erfolg.

Cyberkrieg kann bedeuten, daß hinsichtlich der Beschaffenheit von Streitkräften, des Ortes und der Art ihres Einsatzes sowie der Festlegung der Ziele und Modalitäten des Angriffs auf den Feind eine neue Doktrin entwickelt werden muß. Die Frage, wie und wo welche Computer — und die dazugehörigen Sensoren, Netzwerke, Datenbanken usw. — zu positionieren sind, kann genauso wichtig werden wie das früher beim Einsatz von Bombern und den sie unterstützenden Einrichtungen der Fall war. Darüber hinaus könnte der Cyberkrieg sich auch auf eine Integration der politisch-psychologischen und der militärischen Aspekte der Kriegsführung auswirken.

Alles in allem könnte der Cyberkrieg hinsichtlich der militärischen Organisation und Doktrin sowie der Strategie, Taktik und Waffenentwicklung weitreichende Fragen aufwerfen. Er läßt sich sowohl bei Low- wie auch bei High-Intensity-Konflikten, in konventionellen wie nichtkonventionellen Situationen und in der Defensive wie in der Offensive anwenden.

Wir meinen, daß der Cyberkrieg als Innovation der Kriegsführung für das 21. Jahrhundert das sein wird, was der Blitzkrieg für das 20. Jahrhundert war. Dennoch glauben wir, daß das

Konzept derzeit zu spekulativ ist, um eine präzise Definition zuzulassen. Zumindest aber erweitert es die traditionelle Bedeutung der Informationsbeschaffung in Kriegssituationen: daß man über eine überlegene C3I verfügt und versucht, den Feind zu orten, zu durchschauen, zu überraschen und zu täuschen, bevor das ihm gelingt. Das bleibt unabhängig von der Gesamtstrategie wichtig. Insofern werden informationsbezogene Faktoren durch die neuen Technologien wichtiger als je zuvor, stellen aber keinen Bruch mit der Tradition dar. Tatsächlich besteht hier eine Ähnlichkeit zu Thomas Ronas Konzept des "Informationskriegs"[13], der "eng mit anderen militärischen Operationen verknüpft ist und diese überlagert." Unser Konzept ist aber umfassender als das von Rona, welches sich hauptsächlich mit Gegenmaßnahmen zur Schädigung feindlicher Waffensysteme bei gleichzeitigem Schutz der eigenen befaßt, denn wir halten diesen Ansatz zur Definition von Cyberkrieg letztlich für zu einschränkend.

In einem tieferen Sinne bezeichnet der Cyberkrieg eine Veränderung im Wesen des Krieges. Unserer Meinung nach wird sich diese Definition von Cyberkrieg als die bessere herausstellen. Unsere Position steht im Widerspruch zu einer Sichtweise[14], bei der die Begriffe "Hyperkrieg" und "Cyberkrieg" die Auffassung umschreiben, die wichtigste Auswirkung der MTR sei das automatisierte Schlachtfeld, künftige Kriege würden hauptsächlich von "intelligenten" Waffen, Robotern und autonomen Computern ausgetragen, der Mensch werde sich der Maschine unterordnen und Gefechte würden außergewöhnlich rasch und durch eine Vielzahl von Angriffen aus der Distanz abgewickelt werden. Diese Ansicht interpretiert die Auswirkungen der Informationsrevolution völlig falsch und entspricht in keinem Punkt unserer Meinung.

Im Cyberkrieg geht es ebensosehr um Organisation wie um Technologie. Er impliziert keine Trennung von Mensch und Maschine, sondern neue Schnittstellen zwischen Mensch und Maschine, welche die Kapazitäten des Menschen verstärken. Manchmal mögen sich Gefechte rasch und aus der Ferne abspielen, aber oft genug werden sie auch aus einem langwierigen Nahkampf bestehen. Keines der beiden Extreme wird zur Norm werden, sondern vielmehr neue Kombinationen von Fern- und Nahkampf und von raschen und langsamen Einsätzen. Das postmoderne Schlachtfeld erfährt durch die Revolution der Informationstechnolgie sowohl auf strategischer als auch auf taktischer Ebene eine grundsätzliche Veränderung. Durch die zunehmende Breite und Tiefe dieses Schlachtfelds und die immer größere Genauigkeit und Zerstörungskraft selbst konventioneller Munitionstypen wurden C3I-Fragen dermaßen wichtig, daß eine diesbezügliche Überlegenheit alleine schon ausreicht, um fähigen Praktikern kriegsentscheidende Vorteile zu verschaffen. Dennoch umfaßt das Konzept des Cyberkrieges weitaus mehr als den Angriff auf feindliche C3I-Systeme bei gleichzeitiger Verbesserung und Verteidigung der eigenen. Im Sinne von Clausewitz zeichnet sich der Cyberkrieg durch das Bestreben aus, Wissen in Kampfkraft umzumünzen.

Auch wenn moderne Technologien unabdingbar sind, um einen Cyberkrieg komplett zu planen und auszuführen, stützt sich dieser doch nicht auf die moderne Technologie allein. Die Weiterentwicklung moderner Informations- und Kommunikationstechnologie spielt für das militärische Potential der USA eine entscheidende Rolle. Aber Cyberkrieg, ob er nun von den Vereinigten Staaten oder anderen Akteuren ausgetragen wird, erfordert nicht unbedingt das Vorhandensein moderner Technologie. Die organisatorischen und psychologischen Dimensionen sind wahrscheinlich ebenso wichtig wie die technischen. Unter bestimmten Umständen läßt sich ein Cyberkrieg auch mit einfachen technischen Mitteln durchführen.

Informationsbezogene Faktoren in der Militärgeschichte

Unserem Verständnis nach stellen Netzkrieg und Cyberkrieg neue (und verwandte) Konfliktformen dar, die in Zukunft an Bedeutung gewinnen werden. Die Informationsrevolution impliziert — ja, sie führt zwangsläufig dazu —, daß es in der Natur des militärischen Konfliktes und der Kriegsführung zu tiefgreifenden Veränderungen kommt. Dennoch haben diese beiden neuen Spielarten des Konflikts viele historische Vorläufer. Auch in der Vergangenheit gab es bereits Versuche, Kriege aus einer Art Cyberperspektive zu führen. Information, Kommunikation und Kontrolle sind dem Krieger ein ständiges Anliegen. Es ist historisch ausreichend belegt, daß taktische und strategische Bemühungen, den "Nebel des Krieges" zu durchdringen und den Gegner darin einzuhüllen, immer wieder eine wichtige Rolle spielten.[15]

Im Zweiten Punischen Krieg im dritten Jahrhundert v. Chr. stationierten karthagische Truppen unter der Führung Hannibals mit Spiegeln ausgestattete Beobachter auf Hügeln, die ihren Anführer über die Truppenbewegungen der Römer auf dem laufenden hielten, ohne von diesen bemerkt zu werden. Bessere Kommunikationsmethoden waren mit ein wesentlicher Grund dafür, daß Hannibals Truppen in einer Zeitspanne von 16 Jahren zahlreiche Siege erringen konnten. Als dramatischstes Beispiel für den Einsatz überlegener Informationstechniken mag die Schlacht am Trasimener See gelten, bei der es Hannibals zahlenmäßig unterlegenen Streitkräften gelang, im wahrsten Sinne des Wortes aus dem Nebel des Krieges aufzutauchen und eine mehr als doppelt so große römische Armee aufzureiben.[16]

Ein weiteres berühmtes Beispiel aus neuerer Zeit trug sich während der Napoleonischen Kriege zu. Der Königlich Britischen Kriegsflotte, die seit der Schlacht am Nil 1798 die unumstrittene Herrschaft über das Mittelmeer hatte, gelang es, die strategische Nachrichtenverbindung von Napoleons Expeditionstruppe in Nordafrika zu unterbrechen, was für diese eine katastrophale Niederlage zur Folge hatte. Die Angreifer saßen ohne Nachschub und nach Napoleons Flucht auch ohne ihren Kommandanten in Ägypten fest, bis die Briten kamen und sie gefangennahmen.

Während desselben Konflikts gelang es einige Jahre später der britischen Fregatte Lord Cochranes im Alleingang, die französischen Truppen praktisch an der gesamten spanischen und an weiten Teilen der französischen Mittelmeerküste in völlige Verwirrung zu stürzen. Die Franzosen verwendeten zur Nachrichtenübermittlung ein Signalsystem, mit dem sie ihre Truppen auf Gefahren aufmerksam machten und Küstenschiffen sichere Fahrt signalisierten. Cochrane ließ diese Signalstationen überfallen und griff dann, oft gemeinsam mit spanischen Guerrillatruppen, auf spektakuläre Weise an, während die französischen Kommunikation unterbrochen war.[17]

So könnte man Ereignis um Ereignis aus der Militärgeschichte anführen, um die Bedeutung der Faktoren Information und Kommunikation zu illustrieren. Aber dies soll nur eine kurze Abhandlung zur Einführung des Cyberkriegskonzepts sein. Deshalb wollen wir uns lieber gleich einem frühen Beispiel, einem praktischen Vorbild dieser aufstrebenden neuen Form der Kriegsführung, zuwenden.

Ein frühes Beispiel für Cyberkrieg: Die Mongolen

Im Laufe der Geschichte lassen sich überall, wenn auch in verschiedener Intensität, Versuche nachweisen, die Kommunikationssysteme des Feindes anzugreifen und die eigenen zu schützen. Dem reinen Cyberkrieg (oder eigentlich Netzkrieg) kam jedoch wohl die Kriegsführung der Mongolen, welche im 12. und 13. Jahrhundert ihren Höhepunkt erreichte, am nächsten. Eine Untersuchung der militärischen Praktiken der Mongolen sollte daher zur

Entwicklung von Grundlagen für eine ähnliche Form der Kriegsführung in der postmodernen Welt sehr aufschlußreich sein. Außerdem läßt sich anhand dieses Beispiels einmal mehr belegen, daß Cyberkrieg nicht von Spitzentechnologie, sondern eher von unserer Auffassung von Konflikt und strategischer Interaktion abhängt.

Auf militärischer Ebene bestand die Erfolgsstrategie der mongolischen Doktrin nahezu ausschließlich darin, den genauen Standort ihrer Feinde festzustellen und gleichzeitig den eigenen bis zum Angriff geheimzuhalten. So gelang es ihnen, trotz ihrer chronischen zahlenmäßigen Unterlegenheit die besten, größten Armeen des chinesischen Kaiserreiches, des Islam und des Christentums zu schlagen.

Am einfachsten läßt sich ihr Vorteil durch eine Analogie aus dem Schachspiel veranschaulichen: Ein Krieg gegen die Mongolen glich einer Partie gegen einen Gegner, der die Anordnung seiner Figuren vor unserem Blick verbergen, selbst jedoch sowohl seine als auch unsere Figuren sehen kann. Unter diesen Voraussetzungen kann man davon ausgehen, daß der Spieler, der über die Züge beider Seiten Bescheid weiß, auch mit viel weniger Figuren gewinnen wird. Darüber hinaus würde der massive Einsatz zusätzlicher Truppen durch die "halbblinde" Seite bei der "sehenden" Seite noch lange keine derartige Aufrüstung erfordern. (Insofern liegt die Ähnlichkeit weniger beim Schach, als vielmehr beim "Kriegsspiel", einem dem Schach verwandten Spiel, bei dem beide Spieler anfangs die Position des Gegners nicht kennen. In unserer Analogie kann einer der Spieler durch den normalerweise zwischen den beiden Spielbrettern aufgestellten Sichtschutz hindurchsehen.)

Genauso war es mit den Mongolen. In einem ihrer größten Feldzüge gegen das mächtige moslemische Reich von Khurasan (etwa im Gebiet des heutigen Iran, Irak und Teilen der zentralasiatischen Teilrepubliken der ehemaligen Sowjetunion), schlug eine mongolische Armee von rund 125.000 Mann einen Feind, dessen stehendes Heer fast eine halbe Million Mann und ebensoviele Reservestreitkräfte, umfaßte. Wie war das möglich? Dadurch, daß die Mongolen die lineare, nach vorne gerichtete Aufstellung der feindlichen Truppen identifizierten und diesen auswichen. Die Verteidiger wurden umgangen und die zwischen Hauptstadt und Front pendelnden Kurieren abgefangen.

Muhammad Ali Schah, der Herrscher von Khwarizm, hielt das Ausbleiben von Nachrichten von der Front für ein gutes Zeichen, bis sich eines Tages ein Kurier bis zur Hauptstadt Samarkand durchschlagen konnte, nachdem er mit knapper Not einer mongolischen Patrouille entkommen war. Muhammad erkundigte sich nach seinem Heer und erhielt die Auskunft, daß die Grenzen gesichert seien. Der Kurier fügte jedoch hinzu, daß er nur eine Tagesreise von der Hauptstadt entfernt ein riesiges mongolisches Heer beobachtet hatte. Der Schah ergriff die Flucht, und seine Hauptstadt wurde rasch eingenommen. Als diese Nachricht die an der Grenze stationierten Heere erreichte, kam es zu einer allgemeinen Kapitulation. Muhammad verbrachte den Rest seines Lebens in einem Versteck auf der Insel Abeschkum im Kaspischen Meer, wo er schließlich an einer Brustfellentzündung starb.

Der Feldzug gegen Khurasan ist typisch für die strategische Vorgangsweise der Mongolen, die den Feind zuerst blendeten, um ihn dann an zentraler Stelle zu treffen (ihn Schachmatt zu setzen). Zu Schlachten kam es nur selten, da diese zur Erreichung des Kriegszieles oft gar nicht nötig waren. Dennoch gab es Zeiten, wo sich Konfrontationen nicht vermeiden ließen. In solchen Fällen verließen sich die Mongolen hauptsächlich auf koordinierte Einsätze, mit denen sie Pläne und Kontrolle ihrer Gegner zunichtemachten. So gelang es den Mongolen etwa, in der Schlacht von Liegnitz gegen die verbündeten polnisch-preußischen Truppen eine Armee anzugreifen und zu schlagen, die gut viermal so groß war wie ihre eigene. Ihr Erfolg

rührte daher, daß sie einen klaren Überblick über die Schlachtordnung des Verteidigungsbündnisses bewahrten, während sie die Gegner über ihren eigenen Standort im unklaren ließen. So jagten Teile des westlichen Heeres hinter kleinen Abordnungen her, die nur als Lockvögel dienten, und landeten in den Fängen der mongolischen Hauptstreitmacht. Auf diese Weise wurden die Polen und Preußen sozusagen stückweise besiegt. Die Mongolen waren sich ihrer Informationen sogar dermaßen sicher, daß sie während der Schlacht abwechselnd mit den Polen und Preußen ein- und denselben Flußübergang benutzten.[18]

Und welche Vorteile hatten die Mongolen bezüglich Mobilität und Feuerkraft? Bestimmt waren sie anderen Heeren schon dadurch überlegen, daß ihre Divisionen rund 80 Meilen pro Tag zurücklegen konnten und daß ihre Hornbögen eine durchschnittlich 50 bis 100 Meter größere Reichweite hatten als jene ihrer Feinde. Aber keiner dieser Faktoren konnte die Vorteile aufwiegen, über die ihre Feinde aufgrund ihrer Befestigungstechnik verfügten, und auch die Rüstungen westlicher Streitkräfte waren im Nahkampf gegen die Mongolen deutlich von Vorteil. So gerieten die taktischen Operationen der Mongolen durch gut verteidigte Städte oft ziemlich ins Stocken,[19] und Nahkampfgefechte bereiteten ihnen größte Schwierigkeiten und forderten zahlreiche Opfer. Tatsächlich hat die Verbissenheit und Effektivität der preußisch-polnischen Streitkräfte bei Liegnitz, insbesondere ihrer Kavallerie, die Mongolen wahrscheinlich davon abgehalten, weiter nach Europa vorzudringen.[20] In der Schlacht von Hims bewiesen dann die Mamelucken, daß auch die Streitkräfte des Islam in der Lage waren, die Mongolen taktisch zu besiegen. Weder dem Islam noch dem Christentum gelang es jedoch, die Mongolen strategisch zu überlisten.

Offensichtlich lag der Schlüssel zum Erfolg der Mongolen in deren überlegenen Kommando-, Kontroll-, Kommunikations- und Informationsmethoden. Ihre Späher und Kuriere führten immer drei oder vier Ersatzpferde mit sich, so daß sie auch weiterreiten konnten, wenn ein Tier müde wurde. Auf diese Weise konnten die mongolischen Reiter, relativ gesehen, so etwas wie einen Geheimdienst auf die Beine stellen, der fast wie über Satelliten Informationen über die Schlachtordnung und Absichten des Feindes quasi in Echtzeit weitergeben konnte. Gleichzeitig ermöglichte es diese Steppenversion des "Pony Express" (der Khan nannte sie "Blitzkuriere") den Feldgenerälen, das Hauptkommando, das oft tausende Meilen vom Kriegsschauplatz entfernt war, innerhalb von vier bis fünf Tagen über das Kriegsgeschehen in Kenntnis zu setzen. Zur Nachrichtenübermittlung zwischen den im Feld stationierten Truppen verwendeten die Mongolen auch ein ausgefeiltes Signalsystem, das rasche taktische Winkelzüge erlaubte, wann immer diese notwendig waren. Organisatorisch legten die Mongolen das Hauptgewicht auf ein dezentrales Kommando im Felde, wohingegen ihre Feinde im allgemeinen dazu angehalten waren, Befehle aus der jeweiligen Hauptstadt abzuwarten. Durch die Entwicklung eines Kommunikationssystems, mit dem sie ihre Oberbefehlshaber ständig über den neuesten Stand der Dinge in Kenntnis setzen konnten, erlangten die Mongolen zugleich Gesamtübersicht und Dezentralisierung. Der Khan "ließ seine Truppen auf breiter Front vorrücken und steuerte sie über ein hochentwickeltes Kommunikationssystem"; das war das Geheimnis seines Erfolges.[21]

In strategischer Hinsicht zielten die Mongolen zuerst darauf ab, die Kommunikation des Feindes zu stören, um ihn dann an seiner empfindlichsten Stelle zu treffen. Anders als Clausewitz legten sie kaum Wert auf die Vernichtung feindlicher Streitkräfte, bevor sie weiter vorrückten. Auch waren die Feldzüge der Mongolen keineswegs "linear". Sie griffen an, wo sie wollten, wann immer die Umstände günstig erschienen.

Es ist eine große Schande für ihre christlichen und moslemischen Feinde, daß sie die Organisations- und Kommunikationstechniken der Mongolen nicht öfter nachzuahmen

versuchten. Daß die Mamelucken schließlich den Vorstoß der Mongolen nach Ägypten verhinderten, lag daran, daß sie die mongolischen Truppenbewegungen beobachteten und daß Kilawan, der König, der sie in die Schlacht führte, seine Truppen im Kampfgetümmel auf effiziente, kurzentschlosse Weise befehligte. Außerdem konnten die Mamelucken durch den Einsatz von Brieftauben die strategische Kommunikation noch rascher bewältigen als die Blitzkuriere der Mongolen und so rechtzeitig Truppen für eine effiziente Verteidigung zusammenziehen.[22]

Die Mongolen stellen aber nicht nur ein Beispiel für den Cyberkrieg dar — sie waren auch Meister des Netzkrieges. In ihren frühen Feldzügen verwendeten sie Terrortaktiken, um jeglichen Widerstand zu schwächen. Vor jeder Invasion ließen sie die Nachricht verbreiten, daß sie jede Stadt, die ihnen Widerstand leisten würde, schleifen und ihre Bewohner niedermetzeln würden. Sollte sich eine Stadt andererseits freiwillig ergeben, so hieße das einfach, daß sie ab dann unter mongolischer Oberhoheit stünde; das würde zwar anfangs einige Fälle von Vergewaltigung und Plünderung nach sich ziehen, danach jedoch in eine etwas zerstreute Form der Besatzung übergehen. So kam es, daß sich zahlreiche Städte freiwillig ergaben. In späteren Feldzügen — als die Mongolen erfuhren, daß sowohl Christen als auch Moslems sie für die dunklen Mächte von Gog und Magog hielten, welche den "Weltuntergang" verkündeten — taten sie das ihre, um dieses Bild aufrechtzuerhalten. Sie nannten sich fortan Tartaren, als wären sie Diener des "Tartarus", der klassischen Unterwelt. Später, als klar war, daß die Welt nicht untergehen würde, nahmen die Mongolen bereitwillig einmal das Christentum, ein andermal den Islam an, je nachdem, welche der beiden Religionen einem bestimmten Volk das Joch der Gefangenschaft erleichterte. Dieser utilitaristische Zugang zur Religion erschwerte die Bildung gegnerischer Bündnisse.

Einige Experten behaupten, die Mongolen wären ein Beispiel für frühe Experimente mit der Strategie des Blitzkriegs.[23] Unserer Meinung nach bestehen aber zwischen Cyberkrieg und Blitzkrieg wesentliche Unterschiede, und die Mongolen lassen sich eher ersterem als letzerem zurechnen.

Blitzkrieg, Volkskrieg und darüber hinaus

Die relative Bedeutung des gegen Kommando, Kontrolle und Kommunikation des Feindes gerichteten Krieges ist mit dem Aufkommen der mechanisierten Kriegsführung gewachsen. Im Zweiten Weltkrieg erhob die deutsche Blitzkriegsdoktrin — in gewisser Weise ein Vorläufer des Cyberkrieges — ausdrücklich die Störung feindlicher Kommunikation und Kontrolle zu einem sowohl taktischen als auch strategischen Ziel. Dadurch, daß alle deutschen Panzer mit Funk ausgestattet waren, konnte etwa Deutschland seine taktischen Kräfte in dem langen Krieg gegen die Sowjetunion, deren Panzer zwar zahlreicher und besser gebaut, jedoch nur für Kommandanten mit Funkgeräten ausgestattet waren, vervielfachen.[24]

Auf strategischer Ebene stellte die Zerstörung der Hauptzentrale der sowjetischen Kommunikation und Kontrolle durch die Eroberung Moskaus ein Schlüsselelement in der Planung der Operation Barbarossa dar. Als sich jedoch während des Feldzuges die Möglichkeit ergab, in der Ukraine große materielle Gewinne zu erzielen, ließ Hitler General Guderians Panzer von ihrem Vormarsch auf Moskau abschwenken, und Moskau wurde nie eingenommen. Diesmal sollte es für die Deutschen keinen "Blitzsieg" geben, denn sie fanden sich bald auf der schwächeren Seite eines massiven Zermürbungskampfes, der in eine vernichtende Niederlage münden sollte.[25]

Nach dem Zweiten Weltkrieg wurden Informations- und Kommunikationstechnologien in den großen Industriestaaten wesentlich verbessert. Wichtige und für den Cyberkrieg interessante Kriege fanden zwischen diesen Staaten und den unterentwickelten Ländern der Dritten Welt statt. Ein Vergleich von zwei Schlüsselkonflikten unterstreicht die wachsende Bedeutung und gesteigerte Anwendbarkeit der Prinzipien des Cyberkrieges: auf der einen Seite der in den sechziger und siebziger Jahren von Nordvietnam und dem Vietcong ausgetragene Volkskrieg, und auf der anderen Seite ein konventionellerer Konflikt aus jüngerer Zeit, zwischen einer von Amerika angeführten Koaliton und dem Irak.

Jeder dieser beiden Kriege stellt einen Wendepunkt dar. Im Falle Vietnams hat der Feind vielleicht die Cyberprinzipien effizienter eingesetzt als die Vereinigten Staaten, und zwar nicht nur auf militärischem Gebiet, sondern auch dort, wo der Cyberkrieg in die politischen und sozialen Dimensionen des Konfliktes vordringt. Im Falle des Krieges gegen den Irak haben die USA die Prinzipien des Cyberkrieges — natürlich hat man sie damals noch nicht als solche bezeichnet — auf überlegene Weise gegen einen Feind angewendet, dessen Organisation, Doktrin, Strategie und Taktik aus einer anderen Ära stammten.

Im Vietnamkrieg schienen die Vereinigten Staaten durch alle Kommando- und Kontrollinstanzen hindurch im Vorteil — von der Erstellung quantitativer Indikatoren über Computermodelle und Datenbanken zur Analyse des Kriegsverlaufes von Washington aus bis zu Feldfunkgeräten für die prompte Anforderung von Luftangriffen, Verstärkung und Rettungseinsätzen. Aber im Banne der Computerisierung und der quantitativen Techniken übersahen die Analytiker die flexibleren, subtileren Aspekte dieses Krieges, in denen der Feind Gewinne verbuchen konnte. Die hervorragenden Kommunikationssysteme der USA ermutigten zu unangemessener Einmischung von oben in Gefechte und Feldzüge, die man am besten am Kriegsschauplatz selbst geplant und ausgetragen hätte.

Während die US-Truppen über bessere taktische Kommunikation verfügten, blieb die strategische Kommunikation der Guerilla davon zum Großteil unberührt. In der Zwischenzeit operierten die Nordvietnamesen und der Vietcong auf der Basis der Doktrin von Mao Zedong: "Das Kommando gehört für strategische Zwecke zentralisiert und für taktische Zwecke dezentralisiert"[26] — eine klassische Kombination von Gesamtübersicht und Dezentralisierung. Die Vereinigten Staaten ließen es andererseits scheinbar zu, daß ihre Befehlshaber durch die rechtzeitige Verfügbarkeit großer Mengen an Information auf hoher Ebene dazu verleitet wurden, die zentrale taktische und strategische Kontrolle beizubehalten, im Glauben, die Gesamtübersicht zu haben, selbst wenn dies gar nicht der Fall war.

Das Beispiel Vietnam verdeutlicht unseren Standpunkt, daß gute Kommunikation alleine für einen Cyberkrieg zu wenig ist, auch wenn sie die notwendigen Rahmenbedingungen schafft. Für ein solches Unternehmen ist es unerläßlich, die Aufrechterhaltung der eigenen Kommunikation bei gleichzeitiger Ausschaltung der gegnerischen als überaus wertvolle und gewichtige Punkte in der eigenen Doktrin zu verankern. Dies zieht die Entwicklung von Taktiken und operationellen Strategien nach sich, welche die fundamentalen theoretischen Lehrsätze der starren Plan- als auch der traditionellen Manöverkriegsführung über Bord werfen. Eine aufreibende Zermürbungstaktik wie die von Grant oder abruptes Vorstoßen wie bei Guderian werden nicht mehr ausreichen. Statt dessen wird man völlig andere Modelle in Betracht ziehen müssen, die auf die systematische Verwirrung des Feindes abzielen.

In gewissem Maße lassen die neuesten Erfahrungen der USA aus dem Golfkrieg darauf schließen, daß sich eine gesteigerte Sensibilität für Cyberprinzipien breitmacht. Präsident Bush gab von Beginn an deutlich zu verstehen, daß er nicht beabsichtigte, taktische oder gar

einsatzstrategische Aktionen auf Mikroebene zu leiten. Das steht an sich schon in krassem Gegensatz zum klassischen Bild von Präsident Johnson, der, über Landkarten von Nordvietnam gebeugt, jedes einzelne Ziel für die "Operation Rollender Donner" selbst aussucht.

Bei den Militäroperationen im Golfkrieg kamen bedeutende Cyberelemente ins Spiel, die oft als "Kräftemultiplikatoren" dienten.[27] Der gleich zu Kriegsbeginn geführte Schlag gegen die Kontrolltürme der irakischen Luftverteidigung mit Apache-Helikoptern ist hier nur ein, wenn auch ein sehr wichtiges Beispiel. Zusätzlich wußte das alliierte Bündnis über die irakische Truppenaufstellung bestens Bescheid, während der Irak quasi zum Blindkampf gezwungen war. Ein weiteres Beispiel dafür, wie Informationsbeherrschung als Kräftemultiplikator eingesetzt werden kann, ist die Tatsache, daß eine relativ kleine mobile Marineeinheit (weniger als 20.000 Mann) in der Lage war, sich von der Festlandfront abzusetzen und knapp 125.000 irakische Verteidiger festzunageln.

Im Golfkrieg wurde auch ein deutlicher Versuch unternommen, die Prinzipien des Netzkrieges anzuwenden. Die Schaffung eines internationalen Konsens gegen die irakische Aggression, unterstützt durch ein Großaufgebot an mechanisierten Streitkräfte, sollte Saddam Hussein zum Rückzug zu bewegen. Sein unnachgiebiges Verhalten läßt darauf schließen, daß seine Kriegsvorstellung aus einer früheren Generation stammte.

Institutionen kontra Netzwerke — eine mögliche Auswirkung

Das Militär im herkömmlichen Sinne ist eine Institution, die bewaffnete Truppen ins Feld schickt. Institutionen sind normalerweise hierarchisch organisiert, und Militärinstitutionen sind besonders stark von Hierarchien abhängig.

Im Zuge der Informationsrevolution werden jedoch Hierarchien aufgelöst und neue Richtlinien zur Organisation von Institutionen und deren Abteilungen erstellt. Darüber hinaus begünstigt die Informationsrevolution das Netzwerk als Organisationsform. Auf diese Punkte sind wir bereits im ersten Abschnitt dieses Beitrags eingegangen.

Der zweite Abschnitt wird nun anhand eines kurzen geschichtlichen Überblicks diese Erkenntnisse vertiefen. Die Mongolen, ein klassisches Beispiel einer historischen Streitmacht, deren Kriegsführung an den Prinzipien des Cyberkrieges orientiert war, waren nicht als Hierarchie, sondern eher als Netzwerk organisiert. Auch in jüngerer Vergangenheit konnte eine relativ unbedeutende Militärmacht — die kombinierten Streitkräfte von Nordvietnam und Vietcong — eine moderne Großmacht dadurch besiegen, daß sie in vielerlei Hinsicht eher als Netzwerk und nicht als Institution agierten und zu ihrer politischen Unterstützung sogar im Ausland Netzwerke aufbauten. Bei den von den Mongolen bzw. Vietnamesen bezwungenen Gegnern handelte es sich jeweils um große Institutionen, deren Militärstreitkräfte darauf ausgelegt waren, plangemäße Zermürbungskriege zu führen.

An diesem Punkt lassen sich noch weitere, von aktuellen Ereignissen abgeleitete Beobachtungen anführen. Die meisten Gegner der Vereinigten Staaten und ihrer Verbündeten in Low-Intensity-Konflikten — internationale Terroristen, Guerillaaufstände, Drogenkartelle, ethnische Splittergruppen sowie Rassen- und Stammesunruhen —, sind als Netzwerke organisiert (wenn auch auf Führungsebene oft relativ hierarchisch). Vielleicht bereitet es militärischen (und polizeilichen) Institutionen auch deshalb Schwierigkeiten, in Low-Intensity-Konflikte einzugreifen, weil derartige Konflikte eben nicht dazu gedacht sind, von Institutionen bekämpft zu werden.

Daraus lernen wir folgendes: Netzwerke können Institutionen besiegen und sind selbst wahrscheinlich nur durch Netzwerke zu bekämpfen. Wer die Form des Netzwerks beherrscht, dem gehört die Zukunft.

Fragen für die Zukunft

Die Auswirkungen einer revolutionären Technologie sind anfangs oft nicht absehbar. So war es beim Panzer, beim Maschinengewehr und beim Telefon. 1870 waren z. B. die Franzosen mit ihrem neuentwickelten Schnellfeuermaschinengewehr den Preußen in punkto Feuerkraft potentiell weit überlegen. Leider glich diese frühe Version des Maschinengewehrs eher einem Feldgeschütz als einem Gewehr und wurde hinter der Front, bei der Artillerie, eingesetzt. So hatte die Waffe, die eine Generation später den Ersten Weltkrieg dominieren sollte, kaum Auswirkungen auf den französisch-preußischen Konflikt. Die Menschen neigen dazu, neue Technologien in etablierte Handlungsweisen zu integrieren; von einer neuen Technologie wird erwartet, daß sie sich innerhalb der bisher gültigen Effizienz- und Effektivitätsnormen bewährt.

Es kann einige Zeit dauern, bis man erkennt, daß durch die Integration neuer Technologie in alte Handlungsweisen oft neue Ineffizienzen entstehen, auch wenn einige Aktivitäten tatsächlich effizienter werden. Und noch länger kann es dauern, bis man erkennt, daß die jeweilige Tätigkeit selbst — in operationeller wie organisatorischer Hinsicht — restrukturiert, vielleicht sogar transformiert werden müßte, um das Potential der neuen Technologie voll auszuschöpfen.[28] Dieses Muster zeichnet sich bei den ersten Einsätzen von Telefon und Elektromotor ab und wiederholt sich bei Computeranwendungen in der Geschäftswelt.

Warum sollte das beim Cyberkrieg anderes sein? Neue informationstechnologische Anwendungen sind dabei, die Geschäftswelt in operationeller und organisatorischer Hinsicht zu verändern. In der Welt der Regierungen wird die Revolution der Informationstechnologie größtenteils nur langsam und zögernd umgesetzt. Erwartungsgemäß sollte die Welt des Militärs zum Teil aufgrund der stärkeren Abhängigkeit von hierarchischen Strukturen hinter diesen Entwicklungen zurückbleiben. Teile des US-Militärs zeigen jedoch bereits sehr großes Interesse an der Umsetzung der Informationsrevolution, wobei ein kontinuierliches, aber oft auch stockendes Wechselspiel von operationellen und organisatorischen Neuerungen zu erwarten ist.

Gesteigertes Bewußtsein für die Informationsrevolution

In einigen Kreisen des US-Militärs verbreitet sich die Erkenntnis, daß die Informationsrevolution das Wesen der Krieges verändern könnte und die MTR eine Zeit der Neubewertung und des Experimentierens einleitet, vergleichbar mit den zwanziger und dreißiger Jahren, die Deutschlands bahnbrechende Blitzkriegsdoktrin hervorbrachten. Man fragt sich, wie die neuen Technologien auf innovative Weise anzuwenden sind. So wird argumentiert, daß es den Streitkräften durch die MTR immer leichter möglich würde, sich aus dem unmittelbaren Kampfgeschehen herauszuhalten und feindliche Ziele mit Hochpräzisionswaffen zu zerstören, die aus großer Entfernung, ja, sogar aus dem Weltraum, abgefeuert würden. Anderen Argumentationen zufolge könnten durch die Informationsrevolution Konflikte und Kriege immer öfter im Low-Intensity-Bereich angesiedelt sein, woraus sich erst recht neue Formen des Nahkampfes ergeben würden. Militäranalytiker und -strategen haben offensichtlich gerade erst begonnen, die relevanten Fragen zu erkennen und einen entsprechenden Umdenkprozeß einzuleiten.

Das Militär bleibt — wie weite Teile der Geschäftswelt — in einer Phase, wo Teile neuer Technologien installiert werden, um die Effizienz spezifischer Operationen zu steigern. Sicher können essentielle Cyberkriegstechniken auch dazu dienen, unabhängig von der Gesamtstrategie die Kosteneffizienz vieler Militäroperationen zu verbessern (auch wenn man keinen Cyberkrieg im Schilde führt). So können etwa verbesserte Methoden der Überwachung und Informationsbeschaffung, mit denen sich der bestmögliche Zeitpunkt für Überraschungsaktionen ermitteln läßt (was in gewisser Weise auch Zweck des neuen Joint Targeting Network JTN ist), auch einer herkömmlichen Zermürbungskriegsstrategie dienlich sein. Ebenso können neue Methoden, die Mitglieder einer Einheit in Echtzeit über Standort und Vorgehen ihrer Kameraden zu informieren, wie ein kürzlich durchgeführtes Experiment mit intervehikularen Informationssystemen (IVIS) gezeigt hat, die Konzentration der Truppe als Einheit sowie die Beibehaltung dieser Konzentration während des gesamten Einsatzes erleichtern. Die Liste der neuen Techniken, die wir hier aufzählen könnten, ist lang und wird ständig erweitert.

Wir schlagen eine methodische Untersuchung der Frage vor, welche spezifisch neuen technischen Möglichkeiten die Informationsrevolution unabhängig von der jeweiligen Doktrin und Strategie für die Kriegsführung bieten kann, sowie eine Analyse der aufgrund dieser neuen Möglichkeiten zu erwartenden Formen operationeller und organisatorischer Innovationen. Wir wissen zwar, daß das nicht dasselbe ist, wie den Sprung nach vorne zu wagen und vorzuschlagen, daß der Cyberkrieg diese Fragen großteils beantwortet, aber dieser Artikel braucht ja nicht so methodisch zu sein. Es soll auf spekulative und suggestive Weise darauf aufmerksam machen, daß das Thema Cyberkrieg weitere Diskussionen und Forschungen verdient.

Anzeichen und Aspekte des Cyberkrieges

Bezüglich der Informations- und Kommunikationsdimension des Krieges sowie der Rolle des "Wissens" in Konfliktszenarien müssen neue theoretische Grundlagen geschaffen werden. Der Cyberkrieg besteht nicht nur aus einer Reihe neuer Operationstechniken. Vielmehr entwickelt er sich unserer Ansicht nach zu einer neuen Form der Kriegsführung, die eine neue Herangehensweise an Pläne und Strategien sowie neue Formen der Doktrin und der Organisation erfordert.

Wie könnte ein Cyberkrieg aussehen? Gibt es verschiedene Arten davon? Was wären die unverkennbaren Attribute einer Cyberkriegsdoktrin? Welche Stellung nimmt der Cyberkrieg in der Geschichte der Kriegsführung ein, und weshalb stellt er einen radikalen Umbruch dar? Welche Erfordernisse und Optionen ergeben sich für die Vorbereitung und Durchführung eines Cyberkrieges? Wird dadurch eine neue Form der Machtprojektion möglich? Welche Rolle spielen organisatorische und technologische Faktoren? Welche zusätzliche Faktoren (z. B. psychologische) sollte man berücksichtigen? Wie könnte einem dieses Konzept Überlegungen hinsichtlich C3I, REC (funkelektronische Kampfsysteme) und Psychokrieg — wichtige Faktoren, die normalerweise nicht zusammenhängend betrachtet werden — erleichtern bzw. sinnvoll umlenken? Welche Effizienzmaßnahmen (Measures of Effectiveness, MOE) sollten ergriffen werden? Mit derartigen Fragen, von denen einige in diesem Beitrag angerissen werden, sollte man sich näher auseinandersetzen.

Paradigmenwechsel

Wir gehen davon aus, daß der Cyberkrieg, wie der Krieg im Clausewitz'schen Sinne, ein "Chamäleon" ist. Er wird sich an verschiedene Kontexte anpassen können; er wird nicht aus

einem einzigen strukturierten Ansatz bestehen oder einen solchen erzwingen. Man wird Cyberkrieg als Offensive oder Defensive ausführen können, auf strategischer ebenso wie auf taktischer Ebene. Er wird die gesamte Intensitätsskala umfassen, von Konflikten, die mit schwermechanisierten Truppen auf weitläufigen Kriegsschauplätzen ausgetragen werden, bis zum Kampf gegen Aufständische, bei dem "das Marschieren" die wichtigste Form des Manövers darstellt.

Rufen wir uns kurz den Blitzkrieg ins Gedächtnis. Diese Doktrin für offensive Operationen basierte auf der strikten Koordination von mobilen Streitkräften und Luftwaffe und war für ein relativ offenes Gelände und gutes Wetter gedacht. Ihr Hauptkapital war Geschwindigkeit; es ging darum, rasch Breschen zu schlagen und durch rasche Nachfolgeeinsätze effiziente Verteidigungsmanöver zu verhindern.

Dem Blitzkrieg liegt die Annahme zugrunde, das gegnerische Heer sei eine große und komplexe Maschine, die darauf eingestellt ist, entlang einer vorgegebenen Verteidigungslinie zu kämpfen. Im rückwärtigen Teil der Maschine befindet sich ein empfindliches Netzwerk aus zahlreichen Nachrichtenlinien für Nachschub und Information sowie aus Hauptknotenpunkten, an denen diese Linien zusammenlaufen. Die Zerstörung dieses Zentralnervensystems ist gleichzusetzen mit der Zerstörung des Heeres. Das Hauptziel des Blitzkrieges ist somit strategische Penetration. Der Angreifer versucht, durch eine Lücke in der gegnerischen Front weit hinter die feindlichen Linien einzudringen und so das gegnerische Kommunikationssystem zu beschädigen und die wichtigsten Schnittpunkte des Netzwerks zu zerstören.[29]

Im Vergleich dazu sieht das "Schlachtfeld" im Cyberkrieg ganz anders aus. Der Cyberkrieg hängt weniger von einem geographischen Gebiet als von der Natur des elektronischen "Cyberspace"[30] ab, welcher sich durch die Anwendung moderner Technologie beherrschen lassen sollte. Der Cyberkrieg profitiert von einem offenen funkelektronischen Spektrum und guten atmosphärischen und sonstigen Bedingungen zu dessen Nutzung. Er erfordert unter Umständen einen raschen Informations- und Nachrichtenfluß, aber nicht unbedingt auch rasche oder schwerbewaffnete Offensiven wie etwa der Blitzkrieg. Wenn dem Gegner die Sicht genommen ist, kann er auch gegen einen langsam vorrückenden Angreifer nicht viel tun. Die Frage, wie, wann und wo Kampfcomputer und die dazugehörigen Sensoren, Nachrichtennetze, Datenbanken und REC-Geräte zu positionieren sind, wird in künftigen Kriegen so wichtig werden, wie sie für Panzer, Bomber und die jeweiligen unterstützenden Einrichtungen im Zweiten Weltkrieg war.

Der Cyberkrieg impliziert eine neue Interpretation der Begriffe "Angriff" und "Niederlage". In der Ära der modernen Nationalstaaten, also etwa seit dem 16. Jahrhundert, bestand Kriegsführung hauptsächlich aus Zermürbungskriegen. Die Streitkräfte des Feindes mußten besiegt werden, bevor man die Ziele einnehmen konnte. Das blieb jahrhundertelang so, bis die grotesken Massenschlachten des Ersten Weltkrieges dazu führten, daß man eine Alternative zum Erschöpfungskrieg suchte. Dies wiederum führte zur Entwicklung des Blitzkrieges, welcher die eher rohen Aspekte des Zermürbungskrieges umging. Dennoch erforderte auch diese manöverorientierte Doktrin die Zerstörung feindlicher Armeen als Vorbedingung zur Erreichung von Kriegszielen; es war also ein Zermürbungskrieg "auf Rädern".

Cyberkrieg könnte außerdem heißen (obwohl wir uns in diesem Punkt nicht sicher sind), daß es für einen Sieg nicht mehr unbedingt nötig ist, die gegnerischen Truppen zu vernichten. Der Sieg der Mongolen über Khurasan ist das beste Beispiel für die beinahe völlige Umgehung und praktische Zersprengung feindlicher Truppen. Man kann im Cyberkrieg einen Weg sehen,

die entscheidenden Kämpfe während eines Konfliktes unblutig auszutragen. Daher läßt sich der Cyberkrieg für eine postindustrielle Doktrin heranziehen, die sich vom traditionellen Zermürbungskrieg des Industriezeitalters abhebt und solche Konflikte zu vermeiden sucht.[31] Im günstigsten Fall wird es möglich sein, Kriege zu gewinnen, indem man das strategische Zentrum der gegnerischen Cyberstrukturen, seine Wissens-, Informations- und Kommunikationssysteme, angreift.

Es fällt schwer, sich überhaupt eine menschliche Form des Krieges vorzustellen, aber auf der Basis einer vollausgebildeten Cyberkriegsdoktrin könnte es möglich werden, beim Einsatz von Streitkräften nicht nur die eigenen Kosten möglichst gering zu halten, sondern damit gleichzeitig auch Siege zu erringen, die nicht unbedingt die größtmögliche Zerstörung des Feindes erfordern. Schon wegen seines Potentials, dem Krieg an sich etwas von seiner Grausamkeit zu nehmen, sollte der Cyberkrieg sorgfältig untersucht und weiterentwickelt werden.

Organisatorische und strategische Überlegungen

Auf strategischer Ebene mag der Cyberkrieg Maos militärisches Ideal von der Kombination strategischer Zentralisierung und taktischer Dezentralisierung implizieren. Das Zusammenspiel dieser Effekte ist eine der komplexeren Facetten der Informationsrevolution. Wir vertreten vorerst die Ansicht, daß die Vorteile der Dezentralisierung noch verstärkt würden, wenn das Oberkommando — quasi als Ausgleich für den möglichen Verlust der zentralen Befehlsgewalt — "Gesamtübersicht" erlangte, ein Begriff, den wir oben eingeführt haben und der uns derzeit am geeignetsten erscheint, um den vollständigen Überblick über einen Konflikt zu beschreiben. Dieser Begriff impliziert, daß von zentraler Seite nicht versucht wird, in das Mikromanagement einzugreifen.

Die neue Technologie produziert eine Informationsflut, die in Echtzeit aufzunehmen, zu filtern und zu integrieren ist. Informationsüberlastung und Informationsstau bezüglich Kommando und Kontrolle sind schon lange ein wunder Punkt zentralisierter, hierarchischer Strukturen.[32] Das Führen eines Cyberkrieges kann entscheidende Neuerungen im organisatorischen Aufbau erfordern, insbesondere einen Wechsel von Hierarchien zu Netzwerken. Das traditionelle Vertrauen in hierarchische Strukturen wird unter Umständen an netzwerkorientierte Modelle angepaßt werden müssen, um größere Flexibilität, laterale Verbindungen und Teamwork über institutionelle Grenzen hinweg zu ermöglichen. Man wird sich nicht mehr wie bisher auf Kommando und Kontrolle, die Hauptstärken der Hierarchie, konzentrieren, sondern eher auf Beratung und Koordination, die Eckpfeiler der Netzwerkstruktur. Dies könnte in der Übergangsphase die Frage aufwerfen, inwiefern institutionelle Traditionen beibehalten werden können, wenn ihre verschiedenen Bestandteile mit anderen Bestandteilen (oder gar anderen Institutionen) auf eine Art und Weise vernetzt werden, die bestehenden Hierarchien "gegen den Strich" geht.

Die Informationsrevolution hat bereits die Frage der Verbindungen innerhalb und zwischen den Teilstreitkräften und, im Fall eines Bündniskrieges, auch der zwischen den Heeren aufgeworfen. Die Cyberkriegsdoktrin kann derartige Verbindungen notwendig machen. Sie kann eine besonders enge Kommunikation, Beratung und Koordination zwischen den für Strategien, Plänen und Operationen und den für C3I zuständigen Offizieren erfordern, ganz zu schweigen von den Einheiten im Feld.

Das operationelle und taktische Kommando im Cyberkrieg mag ungewöhnlich anspruchsvoll sein. Wahrscheinlich werden die Bewertung von Truppenbewegungen und die Ausgabe neuer

Befehle nicht mehr wie bisher den traditionellen Weg durch die Instanzen der Kommandohierarchie nehmen. Von der Korps- bis zur Kompanieebene werden Kommandeure mit großer Handlungsfreiheit operieren müssen. Doch auch wenn sie nun mehr Autonomie als je zuvor genießen, müssen sie gleichzeitig umso mehr in der Lage sein, als Teil integrierter gemeinsamer Operationen zu agieren. Um das zu ermöglichen, wird die Gesamtübersicht aufgeteilt werden müssen. Auch eine radikale Änderung der Form und Zusammenstellung von Kampfeinheiten kann notwendig werden. Statt Divisionen, Brigaden und Bataillonen könnte der Cyberkrieg die Schaffung von kombinierten Einsatztruppen erfordern, ähnlich der derzeitigen Marine Air-Ground Task Force.

In der Geschichte finden sich zahlreiche Beispiele für die innovative Kombination von Kampfeinheiten. Sie reichen zurück bis zum römischen Manipel als Gegenstück zur Phalanx. In der Neuzeit brachte der Zweite Weltkrieg zahlreiche völlig neue Einheiten hervor. So begann die US-Armee, Kampfkommandos oder -teams einzusetzen, die aus einer Kombination von Artillerie, Panzer und Infanterie bestanden. Das deutsche Äquivalent dazu war die Kampfgruppe. Diese Einheiten waren oft in der Lage, Missionen zu erfüllen, bei denen größere Einheiten, sogar Korps, bis dahin versagt hatten. Die US-Marine war in dieser Hinsicht ebenfalls innovativ und schuf die schnelle Einsatztruppe als Grundeinheit für Operationen im Pazifikkrieg. Wir möchten darauf hinweisen, daß Maßnahmen, die bisher großteils als improvisierte organisatorische Anpassungen in Kampfsituationen angesehen wurden, nun als ein Ziel unserer ständigen Truppen in Friedenszeiten betrachtet werden sollten, welches es vor Ausbruch des nächsten Krieges zu erreichen gilt.

Überlegungen zur Truppengröße

Die Doktrin des Cyberkrieges und die dazugehörigen organisatorischen und operationellen Veränderungen werden unter Umständen eine Reduktion der US-Streitkräfte erlauben. Anderen bedeutenden Umwälzungen aus der Geschichte der Kriegsführung nach zu schließen, sind jedoch wesentliche Truppenreduktionen auf lange Sicht problematisch. Revolutionäre Neuerungen in der Kriegsführung haben stets nur vorübergehende Vorteile geschaffen, da erfolgreiche Innovationen rasch kopiert wurden.[33]

Verfügen beide Parteien in einem künftigen Konflikt über substantielle Cyberkriegskompetenzen, so erfordert die Intensität und Komplexität eines solchen Krieges wohl eher mehr als weniger Truppen. Mag sein, daß der besser ausgebildete, geschicktere Praktiker sich durchsetzt, aber wahrscheinlich werden "große Bataillone" weiterhin notwendig sein, besonders, wenn das relative Cyberpotential auf beiden Seiten annähernd gleich ist. Ob die zukünftigen US-Truppen nun größer oder kleiner sind als heute, sie werden auf jeden Fall deutlich anders zusammengesetzt sein.

Operationelle und taktische Überlegungen

Der Cyberkrieg könnte auch auf operationeller und taktischer Ebene radikale Auswirkungen haben. Bisher ließen sich Militäreinsätze in Kategorien des "Haltens und Zuschlagens" einteilen. Ein Teil der Truppe diente dazu, den Gegner festzunageln und so Raum für Flankenangriffe und andere Manöverformen zu schaffen.[34] Taktisch gesehen, bestanden die Hauptaspekte der Kriegsführung bisher aus Beschuß und Bewegung. Feuerschutz ermöglicht Manöver, und Manövereinheiten können dann wiederum weiteren Einheiten bei ihrem Vorrücken Feuerschutz geben. Beschuß schafft also Manöverpotential. Taktisches Vorrücken kann man als eine Art Bockspringen auffassen.

Der Cyberkrieg wird wahrscheinlich andere, vielleicht sogar konträre Prinzipien hervorbringen. Überlegenheit im Bereich Wissen und Informationskontrolle ermöglicht höchstwahrscheinlich eine Strategie des "Zuschlagens ohne Halten" sowie taktische Manöver, die optimale Bedingungen für einen anschließenden Beschuß schaffen.

Überlegungen zum Thema Atomwaffen

Wie sieht es mit Atomwaffen und Cyberkrieg aus? Die Kriege, in die die Vereinigten Staaten in Zukunft verwickelt sein könnten, werden wahrscheinlich aus zwei Gründen nicht-atomarer Natur sein. Erstens deshalb, weil der Zerfallsprozeß in der ehemaligen Sowjetunion mit großer Wahrscheinlichkeit weitergeht und weitere Truppenreduzierungen einen Atomkrieg höchst unwahrscheinlich machen, und zweitens, weil die USA schlecht beraten wären, wenn sie Länder atomar bedrohen, die selbst über keine Atomwaffen verfügen.

Abgesehen vom Fehlen einer zentralen Bedrohung und von den normativen Hemmungen gegen den Einsatz von Atomwaffen für Zwangsmaßnahmen gibt es auch einen praktischen Grund, weshalb man Atomwaffen in diesem Kontext ausklammern sollte: Setzt man einen Gegner unter Druck, so sucht er vielleicht bei einer anderen Atommacht Schutz oder wird dazu veranlaßt, sich ebenfalls Atomwaffen zu beschaffen. Selbst wenn ihm dies gelingt, wird er aber an einer konventionellen Konfliktbereinigung interessiert sein, da die USA weiterhin allen aufstrebenden gegnerischen Nuklearmächten hinsichtlich potentieller Gegenschläge weit überlegen sein werden. In Anbetracht der Tatsache, daß selbst große künftige Kriege aller Wahrscheinlichkeit nach keine Atomkriege sein werden, erscheint der Versuch noch vernünftiger, unsere Kapazitäten für konventionelle und nichtkonventionelle Kriege durch die Entwicklung einer Cyberkriegsdoktrin zu optimieren.

Strategische und operationelle Überlegungen zu Kriegen mit Massenvernichtungswaffen stellen bereits einen Vorläufer des Cyberkrieges dar. Strategien des atomaren Gegenschlags kreisten hauptsächlich um die Zerstörung der Schlüsselzentren gegnerischer Kommunikation, um so die Steuerung und Kontrolle atomarer Langstreckenwaffen zu verhindern.

Das "Abschneiden" der gegnerischen Führungsspitze vom Truppenkörper stellte bereits ein typisches Cyberprinzip dar. Aufgrund der katastrophalen Politik der gegenseitigen Abschreckung war diese Erkenntnis der Kriegsführung jedoch einige Jahrzehnte lang unbeachtet geblieben.

Bevor wir aber das Thema Atomkrieg wieder verlassen, möchten wir noch auf eine Ausnahme für den Bereich des Seekrieges hinweisen. Aufgrund der überwältigenden Überlegenheit der USA zur See ist klar, daß ihre potentiellen Gegner diese nach Möglichkeit zu verringern oder zu beenden suchen. Daher werden Atomwaffen Gegnern, die nur über eine kleine Kriegsmarine verfügen, attraktiv erscheinen, sofern für ihre Ziele die Vernichtung unserer Marinekapazitäten erforderlich ist. Vor hundert Jahren versuchte der Franzose Jeune Ecole durch die Entwicklung wendiger Schiffe, die eine brandneue Waffe, den Torpedo, abfeuern konnten, der Vorherrschaft der Königlich Britischen Marine in internationalen Angelegenheiten entgegenzuwirken. Heute könnten sich moderne Marineexperten großer wie kleiner Mächte dazu veranlaßt sehen, ebenfalls neue Waffen zu entwickeln.[35]

Glücklicherweise verfolgt die US-Kriegsmarine einen Weg, der der Informations- und Kommunkationsdimension des Krieges höchste Bedeutung zumißt. Denn wenn man auf See geortet ist, ist man sofort verwundbar. Tatsächlich ist man im Seekrieg inzwischen bei einer Doktrin angelangt, die schon sehr nach Cyberkrieg aussieht. Die Gründe dafür liegen

vielleicht in der geschichtlichen Entwicklung, denn auch die vorhin genannten Beispiele aus dem Bereich der Marine, selbst die aus der napoleonischen Zeit, weisen starken Cybercharakter auf.

Vorschläge für weitere Forschungen

Unsere Ideen dienen als Einführung und Anregung und lassen viele Themen für weitere Analysen offen. Wir sind überzeugt, daß dies eine aufregende Zeit ist, eine Zeit des Umdenkens in der Theorie und Praxis der Kriegsführung, und daß der Cyberkrieg eines der Themen in diesem Umdenkprozeß sein sollte. Wir gründen das auf die Annahme, daß technologische und dadurch bedingte organisatorische Innovationen weiterhin einen revolutionären Verlauf nehmen werden.

Wir schlagen Fallstudien vor, um festzustellen, was bei der Entwicklung einer Cyberkriegsperspektive zu berücksichtigen ist. Wie bereits erwähnt, sollten sich diese Fallstudien auch mit dem Vietnam- und dem Golfkrieg befassen. Zusammen mit anderem Material — Buchbesprechungen, Interviews etc. — über die potentiellen Auswirkungen der Informationsrevolution könnten solche Studien dazu beitragen, eine theoretische und praktische Grundlage für einen Bezugsrahmen zu schaffen, der nicht nur der Analyse, sondern potentiell auch der Formulierung einer von der strategischen bis zur taktischen Ebene und in Konflikten aller Intensitätsgrade anwendbaren Doktrin dient. Solche Studien könnten auch mithelfen, die technologischen und nicht-technologischen Grundpfeiler des Cyberkrieges zu unterscheiden.

Wir schlagen analytische Übungen zur Bestimmung der verschiedenen möglichen Erscheinungsformen des Cyberkrieges im frühen 21. Jahrhundert vor, wenn die neuen Technologien fortschrittlicher, verläßlicher und vernetzter sein werden als heute. In diesen Überlegungen sollten die potentiellen Gegner der Vereinigten Staaten in Konflikten aller Intensitätsgrade berücksichtigt werden. Eine solche Liste mag die Streitkräfte der früheren Sowjetunion ebenso umfassen wie Nordkorea, Irak, Iran und Kuba. Ein Cyberkrieg gegen die Kommandostruktur eines Landes kann unter Umständen dann besonders wirksam sein, wenn dieses Land von einem Dikator angeführt wird, der sich in seinem Land keiner breiten Unterstützung erfreut.[36] Ebenso sollten nichtstaatliche Akteure als potentielle Gegner in Betracht gezogen werden, wie etwa transnationale Millennaristen-, Terroristen- und Verbrecherorganisationen (z.B. Drogenschmuggler). Wir gehen davon aus, daß sowohl der Cyberkrieg als auch der Netzkrieg auf einzigartige Weise zur Bekämpfung nichtstaatlicher Akteure geeignet sind.

Weiters schlagen wir vor, in diese Gedankenexperimente auch ungewöhnliche Gegner und Gegenmaßnahmen einzubeziehen. Die revolutionären Kräfte der Zukunft werden immer öfter aus weitverbreiteten, mehrere Organisationen umfassenden Netzwerken bestehen, die keine bestimmte nationale Identität aufweisen, sondern vielmehr den Anspruch erheben, der zivilen Gesellschaft zu entspringen. Weiters könnten sie aggressive Gruppen und Individuen umfassen, die Experten für moderne Kommunikations- und Munitionstechnologien sind. Wie werden wir damit umgehen? Kann sich Cyberkrieg (oder gar der Netzkrieg) hier zu einer angemessenen, wirksamen Gegenmaßnahme entwickeln? Wird es offiziellen Institutionen weiterhin so schwerfallen, informelle Netzwerke zu bekämpfen, so daß die USA womöglich neue Militäreinheiten und -kapazitäten entwickeln müßten, um für die vernetzte Kriegsführung gerüstet zu sein?

All das könnte einen Forderungskatalog für die endgültige Beurteilung des US-Cyberkriegspotentials im Verhältnis zu dem potentieller Gegner ergeben. Wie groß ist die derzeitige Überlegenheit der USA? Wie lange wird sie bestehen? Dabei sollte nicht nur verglichen werden, inwiefern die verschiedenen Parteien in der Lage sind, einen Cyberkrieg zu führen bzw. einem solchen standzuhalten, sondern auch, inwiefern sie die Schwächen des Gegners zu erkennen, zu identifizieren und für eigene Zwecke zu nutzen imstande sind.

Zwar ist dieser Artikel in einem immanent futuristischen Ton gehalten, doch tun sich derzeit auch in der wirklichen Welt zwei Gefahren auf, denen durch die geschickte Anwendung von Netzkrieg- und Cyberkriegstechnologien begegnet werden könnte. Die eine ergibt sich aus der Weitergabe von Massenvernichtungswaffen. Während man über die spezifischen Gegebenheiten des Erwerbs und die Zeitpläne für die Entwicklung von glaubwürdigen, sicheren Arsenalen offen diskutieren kann, steht außer Frage, daß die Vereinigten Staaten strikt gegen eine Weitergabe von Massenvernichtungswaffen sind. Es gilt also, einer solchen effizient entgegenzuwirken bzw. sie zu verhindern.

Die Möglichkeiten der Proliferation in der Ära nach dem Kalten Krieg schaffen ein angemessenes Anwendungsgebiet für Netzkriegstechniken, da man im Umgang mit den meisten nationalstaatlichen Akteuren (inklusive Deutschland und Japan, sollten diese jemals eigene Atomwaffen besitzen wollen) der Überzeugungsarbeit gegenüber Präventivschlägen[37] den Vorzug geben wird. Ein Netzkrieg, der speziell darauf ausgerichtet ist, potentiellen Proliferatoren vom Erwerb solcher Waffen abzuraten, könnte aus einem "Frontalangriff" über die zahlreichen Kommunikationsnetzwerke bestehen, über die wir mit ihnen verbunden sind, diplomatische, akademische, wirtschaftliche, journalistische und private Verbindungskanäle eingeschlossen. Der konzeptuelle Aspekt des Netzkrieges würde sich darauf konzentrieren, potentielle Proliferatoren davon zu überzeugen, daß sie derartige Waffen gar nicht brauchen. Der Erwerb solcher Waffen würde nur neue Feinde schaffen und ein neue Gefahr für das Überlebens darstellen, während die Vorteile minimal und unbeständig wären.

Die zweite Gefahr, die in der Welt nach dem Kalten Krieg höchstwahrscheinlich auf uns zukommt, betrifft die regionale Sicherheit. Voraussichtlich werden die Ausgaben Amerikas für seine Verteidigung zumindest während der nächsten zehn Jahre weiter sinken. US-Truppen werden reduziert und Übersee-Einsätze gekürzt werden. Die Anzahl der Geschwader und Flugzeugträgerflotten wird sinken. All diese Entwicklungen reduzieren die Fähigkeit Amerikas, eine erfolgreiche Abschreckung gegen konventionelle Aggression zu garantieren. Von Südkorea bis zum südasiatischen Subkontinent, vom Persischen Golf bis zum Balkan und im gesamten Gebiet der ehemaligen Satellitenstaaten der Sowjetunion bis an die Ostsee werden bescheidene oder gar keine amerikanischen Posten stationiert sein. In einer Welt, in der das Aufflammen jahrhundertealter ideologischer, religiöser, ethnischer und territorialer Rivalitäten sehr wahrscheinlich ist, wird regionale Abschreckung eine problematische Praxis darstellen.

Wenn die Wahrscheinlichkeit regionaler Kriege besteht und die amerikanischen Truppen kleiner und von den besagten Regionen weiter entfernt sind als in der Vergangenheit, dann könnte eine Cyberkriegsdoktrin dazu dienen, das Problem der größeren Entfernungen und kleineren Truppen zu kompensieren. Wenn wir bezüglich der Auswirkungen des Cyberkrieges recht behalten und herkömmliche Anforderungen an die Streitkräfte gegenüber unterschiedlich großen und starken Gegnern obsolet werden, dann sollten die USA in der Lage sein, Aggressoren sogar mit relativ kleinen Truppen jederzeit zurückzuwerfen. General Colin Powell faßt die Essenz dieser Überlegung sehr treffend in seiner Analyse des Golfkrieges zusammen:

Truppenreduktionen und ein immer kleineres Verteidigungsbudget führen zu einer immer stärkeren Technologieabhängigkeit, welche den zur erfolgreichen militärischen Abschreckung notwendigen Kräftemultiplikator darstellen muß … Kampfinformationssysteme wurden die Verbündeten des Soldaten. Die Computer lieferten weitaus mehr als eine Dienstleistung. Sie waren Kräftemultiplikatoren.[38]

Während eine Cyberkriegsdoktrin uns ein stabiles Rüstzeug für den Kampf gegen die größten regionalen Aggressoren bieten sollte, müssen wir doch eingestehen, daß die geringe Größe und das (eventuell) ungewöhnliche Erscheinungsbild unserer Streitkräfte einen geringeren "Einschüchterungseffekt" auf zukünftige Gegner ausüben werden, was die Stabilität unserer Abschreckung in Krisenzeiten beeinträchtigen könnte. Dieses neue Dilemma läßt sich auf zwei Arten entschärfen. Erstens können uns Netzkriegstechniken in für uns interessanten Regionen frühe Warnsignale liefern und die Möglichkeit geben, einen potentiellen Aggressor von seinem Vorhaben abzubringen, sobald wir seine Absichten kennen. Die zweite Möglichkeit, die regionale Abschreckung zu fördern, besteht darin, stillschweigend Entschlossenheit zu signalisieren. Das kann bedeuten, bereits zu einem frühen Zeitpunkt einer Krise Militärstreitkräfte einzusetzen oder "vorzuführen", und könnte sogar den Einsatz unserer Militärpotentiale zur Statuierung von Exempeln involvieren.[39] Wenn derartige Signale auf die von der Cyberdoktrin empfohlenen Ziele gerichtet wären, wie z.B. auf wichtige Kommunikationsknotenpunkte, so wären die Kapazitäten des Aggressors für offensive Handlungen von Anfang an praktisch gleich Null.

Wie mag nun ein Cyberkrieg gegen einen regionalen Aggressor aussehen? In den meisten Fällen wird er wahrscheinlich nach dem "Pusan-Inchon"-Schema ablaufen.[40] Zuerst müßte man den "KO-Schlag" des Gegners abfangen. Dann würden die amerikanischen Streitkräfte zum Gegenangriff übergehen. Die Hauptverantwortung dafür, daß die USA nicht bereits zu Beginn eines Krieges vom Gegner überrannt werden, würde mit Sicherheit auf der US-Luftwaffe lasten und davon abhängen, inwiefern diese in der Lage ist, die Kommunikation und Logistik des Gegners auszuschalten. Je nach Region werden sich die Einzelheiten unterscheiden, da einige Angreifer weniger gut gegen eine strategische Blockade gerüstet sind als andere. Zukünftige Aggressionen seitens des Irak gegen die arabische Halbinsel würden z.B. davon abhängen, ob der Irak eine Handvoll Straßen und zwei Brücken über den Tigris benützen kann. Andererseits hat z.B. Nordkorea zahlreiche Möglichkeiten, in den Süden vorzudringen.

Die zur Abwendung von Aggressionen nötigen Streitkräfte wären wahrscheinlich von bescheidener Größe. Da dem Angreifer längst vor Eintreffen der US-Bodentruppen die Sicht genommen ist, werden die USA zuschlagen können, wo und wann sie wollen. Auf der arabischen Halbinsel etwa wäre auch eine Invasion mit einer Armee von einer Million Mann nicht in der Lage, gegen einen amerikanischen Cyberkrieg zu bestehen, insbesondere, wenn eine defensive Position beibehalten wurde. Da der Angreifer nicht weiß, wo die Amerikaner angreifen könnten, müßte er seine Truppen über einen Kampfschauplatz verteilen, der sich in jede Richtung mehrere hundert Kilometer erstrecken würde. Die amerikanische Luftwaffe würde ihn blenden und seine Truppen während ihrer Manöver zerstören. Dann käme es dort, wo man am wenigsten damit rechnet, zum Gegenangriff, und die Fähigkeit des Angreifers, als zusammenhängende Streitmacht zu kämpfen, würde zunichtegemacht. So wie die Mongolen im Feldzug gegen Khurasan eine Armee schlagen konnten, die mehr als zehnmal so groß war wie ihre eigene, sollten moderne Cyberkrieger in der Lage sein, viel größere Streitmächte im Feld zu besiegen. Natürlich werden die Einzelheiten von Region zu Region verschieden sein. Wieder wäre das Beispiel Korea etwas komplizierter, obwohl auch auf dieser Halbinsel der Mangel an strategischer Tiefe durch das unverwüstliche südkoreanische Verteidigungspotential mehr als aufgewogen wird.

Es scheint offensichtlich, daß eine Cyberkriegsdoktrin dem geschickten Anwender die Fähigkeit verleiht, konventionelle regionale Aggression zwischen Nationalstaaten mit geringem Blutvergießen und Materialverlust niederzuschlagen. Aber wird sie gegen nichtkonventionelle Gegner ebensogute Dienste leisten? Dies ist eine äußerst wichtige Frage,

da vielfach, insbesondere von Van Creveld[41], behauptet wurde, der Krieg würde von nichtstaatlichen Akteuren und kleineren Staaten verändert, die ständig neue Methoden ersinnen müssen, um überlegene Gegner bekämpfen und besiegen zu können. Daher würden sich zukünftige, aus religiösem, ethnischem oder durch Stammesfehden bedingtem Eifer motivierte Krisen dadurch auszeichnen, daß große, gutbewaffnete irreguläre Truppen ein ihnen bekanntes Terrain optimal nutzen. Derartige Truppen könnten sich weiters problemlos innerhalb und zwischen den "Membranen" zersplitterter Staaten bewegen.

Der Cyberkrieg stellt vielleicht kein Allheilmittel für alle Konflikte dieses Typus dar, aber er schafft zumindest einen neuen, nützlichen Rahmen zu deren Bewältigung. Im Falle Ex-Jugoslawiens, wo alle der obengenannten Faktoren in Erscheinung getreten sind, sollten die AirLand Battle des US-Heeres oder auch die "Operation Wüstensturm" nicht als Analysemodelle herangezogen werden. Ein derartiger Bezugsrahmen würde dazu verleiten, eine gesamte Feldarmee (400.000—500.000 Mann) als das geeignete Instrument für einen Entscheidungskrieg in einer derartigen Umgebung anzusehen. Statt dessen könnte eine Intervention einfach nach dem im Cyberkrieg verwendeten "Pusan-Inchon"-Ansatz für regionale Konflikte ablaufen. So könnten z.B. die einheimischen Verteidiger in Bosnien und in anderen Gebieten des ehemaligen Jugoslawien mit den richtigen Waffen ausgestattet werden, um jeden Versuch, sie zu überrennen, zunichtemachen zu können (das "Pusan" des Feldzugs). Dann könnte als nächster Schritt eine kleine kombinierte amerikanische Einsatztruppe aus nicht mehr als einer Division Bodentruppen[42] in opportunistischer Manier zuschlagen, wann und wo sie wollen (das "Inchon"). Die feindlichen Streitkräfte wären aus der Luft durch Abfangen von Funkmeldungen und durch unbemannte Bodensensoren leicht lokalisierbar, insbesondere, wenn sie versuchen, vorzurücken oder zu kämpfen. Die Tatsache, daß die Aggressoren weit verstreut sind, macht es einfacher, sie einzeln zu schlagen. Und sobald sie sich konzentrieren, fallen sie der enormen amerikanischen Feuerkraft zum Opfer.

Die Balkankrise mag zu einem prägenden Ereignis für künftige nichtkonventionelle Konflikte werden. Außerdem stellt sie einen wichtigen Beispielfall für die Entwicklung einer Cyberkriegsdoktrin für ein derartiges Szenario dar. Wir möchten jedoch darauf hinweisen, daß diese Überlegungen keinesfalls implizieren, daß wir in diesem Fall eine Intervention unterstützen würden.

Während es der Cyberkrieg erlaubt, daß wir uns bezüglich der Aufrechterhaltung der regionalen Sicherheit in einer Zeit der Reduktion und des Rückzugs von US-Truppen relativ sicher fühlen, bringt das neue Kriegsführungspotential doch auch eine neue Sorge mit sich. Sollten die USA sich für zukünftige regionale Kriege Bündnispartner suchen? Dieser Schritt erscheint logisch, da sowohl internationale als auch innenpolitische Probleme bereits dadurch entschärft werden könnten, daß eine Gruppe von Nationen Arm in Arm, wenn nicht gar im Gleichschritt, gegen den Aggressor aufmarschiert. Dennoch sollten wir uns Gedanken darüber machen, ob wir die Streitkräfte anderer Nationen in einen Cyberfeldzug miteinbeziehen sollten. Abgesehen von den Schwierigkeiten einer sochen Integration, sollten die USA ihren neuen Ansatz nicht überstürzt mit anderen teilen, besonders nicht mit Verbündeten, die womöglich ad hoc rekrutiert wurden. Es ist eine Sache, einen langjährigen Verbündeten wie etwa Großbritannien ins Vertrauen zu ziehen, aber bei Syrien sieht die Sache schon ganz anders aus. Vielleicht kann man diese neue Spannung dadurch lösen, daß wir unsere Verbündeten die Stellung halten, d.h. die "Pusans" verteidigen lassen, während wir uns um die "Inchons" kümmern. Es ist eine Ironie des Schicksals, daß unser Vermögen, Kriege im Einklang mit den Prinzipien der Informationsrevolution zu führen und zu gewinnen, es erfordern könnte, daß wir unsere neuen Erkenntnisse sogar vor unseren Freunden und Verbündeten geheimhalten.

*Titel des amerikanischen Originaltextes: "Cyberwar is Coming!". Erstmals veröffentlicht in: "Comparative Strategy", Volume 12, no.2, pp. 141—165.©Taylor & Francis, 1993.

Abdruck mit freundlicher Genehmigung

Fußnoten:

[1] Delbruck beschreibt die Kriegsführung als ein duales Phänomen; man kann dabei entweder "Erschöpfung" oder "Vernichtung" im Sinn haben, In: Delbruck, Hans: History of the Art of War. 3 Bd., Westport, CT, Greenwood Press 1985.

[2] Dieses Konzept versteht sich in Anlehnung an ein älteres sowjetisches Konzept für eine wissenschaftliche Technologierevolution (STR).

[3] Van Creveld, zitiert von Weigley. In: Weigley, Russell F., "War and the Paradox of Technology". In: International Security. Fall 1989, 192—202

[4] Vgl. Bell, Daniel, "The Social Framework of the Information Society". In: Forester, Tom (Hg.): The Micro Electronics Revolution: The Complete Guide to the New Technology and Its Impact on Society. The MIT Press, Cambridge, Mass., 1980, 500—549; Beniger, James: The Control Revolution. Harvard University Press, Cambridge, Mass., 1986; und Toffler, Alvin: Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century. Bantam Books, New York 1990

[5] Sproull, Lee; Kiesler, Sara: Connections: New Ways of Working in the Networked Organization. MIT Press, Cambridge, Mass. 1991

[6] Zu diesen Themen gibt es umfangreiche Literatur. Zu den neuesten Beiträgen zählen: Bankes, Steve; Builder, Carl; RAND: The Etiology of European Change. Santa Monica 1991; Malone, Thomas W.; Rockart, John F.: "Computers, Networks and the Corporation". In: Scientific American. September 1991, 12—36; Ronfeldt, David; RAND: Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution. Santa Monica 1991; Sproull, Lee; Kiesler, Sara: Connections: New Ways of Working in the Networked Organization. Cambridge: MIT Press 1991, und "Computers, Networks and Work". Scientific American. September 1991, 116—123; Toffler, Alvin: Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century. Bantam Books, New York 1990

[7] Ronfeldt, David: Institutions, Markets, and Networks. in Vorbereitung.

[8] Begriffe mit der Vorsilbe "Cyber" — z. B. Cyberspace — sind derzeit bei einigen Visionären und Technologen en vogue, die Namen für neue, mit der Informationsrevolution zusammenhängende Konzepte suchen. Die Vorsilbe stammt von der griechischen Wurzel kybernan (steuern, beherrschen) und dem damit verwandten Wort kybernetes (Kapitän, Herrscher oder Steuermann). Das Präfix wurde in den vierziger Jahren von Norbert Wiener in seinen klassischen Werken zur "Kybernetik" eingeführt (welche wiederum auf den älteren französischen Terminus cybernetique zurückgeht, der die Kunst des Regierens bezeichnet). Einige Leser mögen die neuen Begriffe, die wir dem Lexikon hinzufügen, nicht gutheißen, aber wir ziehen sie Alternativen wie etwa dem Begriff "Informationskrieg" vor, womit in gewissen Kreisen eine auf C3I-Kapazitäten ausgerichtete Art der Kriegsführung bezeichnet wird. Was unserer Ansicht nach für die Verwendung dieses Präfixes spricht, ist die Tatache, daß es die Bereiche Information und Kontrolle besser als andere zur Verfügung stehenden Präfixe oder Begriffe bezeichnet. In der Tat ist kybernan auch die Wurzel des Wortes "to govern" (herrschen, regieren) und aller davon abgeleiteten Wörter. Vielleicht wäre es hilfreich, den Begriff auch auf Deutsch wiederzugeben. Ein möglicher Begriff wäre Leitkrieg , was sich frei als "Kontrollkrieg" übersetzen läßt. (Wir danken Denise Quigley für diesen Vorschlag.)

[9] Wir danken Carl Builder für den Hinweis, daß sich die Informationsrevolution auf Kontext und Durchführung von Kampfhandlungen gleich stark auswirken könnte und daß in diesbezüglichen Analysen zuerst mögliche Kontextänderungen identifiziert werden müßten, bevor man Empfehlungen für Änderungen im militärischen Verhalten abgibt.

[10] Der schwierige Begriff ist "Information"; ihre Definition bleibt ein Schlüsselproblem der Informationsrevolution. Obwohl keine der gängigen Definitionen zufriedenstellend ist, neigen doch viele

Analytiker dazu, sich eine Hierarchie vorzustellen, auf deren unterster Stufe die Daten angesiedelt sind, gefolgt von Informationen in der Mitte, und Wissen auf der obersten Stufe (einige würden darüber noch die Weisheit stellen). Wie viele Analytiker verwenden auch wir den Begriff Information (oder informationsbezogen) oft, um die gesamte Hierarchie zu bezeichnen, manchmal jedoch auch, um etwas zu bezeichnen, das mehr als Daten, aber weniger als Wissen darstellt. Schließlich gibt es noch die immer populärere Ansicht, neue Information sei "jeder Unterschied, der einen Unterschied macht".

[11] Van Creveld, Martin: The Transformation of War. Free Press, New York 1991, 197

[12] Die Bedeutung von "Gesamtübersicht" erkennt bereits David Gelernter, wenn er feststellt: "Wenn du als Software-Ingenieur monumentale Komplexitäten nicht meistern und bewältigen kannst, dann bist du tot: deine Maschinen arbeiten nicht. Sie laufen eine Zeitlang und kommen dann stockend zum Stillstand, oder sie laufen gar nicht. Daher muß ‚Komplexitätsmanagement' dein Ziel sein. Genau dasselbe Ziel können wir auch in etwas positiverem Licht sehen. Wir können es das Streben nach 'Gesamtübersicht' nennen. 'Gesamtübersicht' — das Verständnis des Gesamtzusammenhangs — ist das wesentliche Ziel eines jeden Software-Ingenieurs. Es ist außerdem die wertvollste intellektuelle Ware, die wir kennen." (in: Mirror Worlds, or the Day Software Puts the Universe in a Shoebox … How It Will Happen and What It Will Mean: Oxford University Press, New York 1991, 52)

[13] Vgl. Rona, Thomas P.: Weapon Systems and Information War. Boeing Aerospace Co., Seattle, Juli 1976, 2

[14] Vgl. Arnett, Eric H.: "Welcome to Hyperwar". In: The Bulletin of the Atomic Scientists. Bd. 48, Nr. 7, September 1992, 14—21

[15] Van Creveld formuliert das folgendermaßen: "Von Platon bis zur NATO besteht die Geschichte des Kriegskommandos im wesentlichen aus dem endlosen Streben nach Gewißheit …" In: Van Creveld, Martin: Command in War. Harvard Press, Cambridge 1985, 264

[16] Vgl. Caven, Brian: The Punic Wars. St. Martin's Press, New York 1980

[17] Vgl. Brodie, Bernard: A Guide to Naval Strategy. Princeton University Press, Princeton 1944; Grimble, Ian: The Sea Wolf: The Life of Admiral Cochrane. Blond; Briggs, London 1978

[18] Für diesen Beitrag war James Chambers unsere wichtigste Quelle für die mongolische Militärdoktrin. Jeremiah Curtin hat die mongolischen Sagas übersetzt und sie mit Eloquenz und Kohärenz wiedergegeben. Harold Lamb lieferte wichtige Erläuterungen über den strategischen Ansatz Dschinghis-Khans.

[19] Vielleicht töteten die Mongolen deshalb die Streitkräfte (und deren zivile Helfer) der belagerten Städte, wenn sie sich ihnen widersetzten. Sobald sich diese Brutalität herumgesprochen hatte, leisteten immer weniger Städte Widerstand. (Ein düsteres Beispiel für Netzkrieg.)

[20] Innenpolitische Unruhen innerhalb des mongolischen Reiches spielten mit eine Rolle, wenn Militäreinsätze zum Stillstand kamen.

[21] Vgl. Chambers, James: The Devil's Horsemen. Atheneum, New York 1985

[22] Kilawan war sich durchaus auch der Bedeutung von Kommando und Kontrolle auf taktischer Ebene bewußt. Vor der Schlacht von Hims z. B. sandte er einen seiner Offiziere, der Fahnenflucht vortäuschte, zum mongolischen Heerführer Mangku-Temur. Als er nah genug war, schlug der Mameluckenoffizier Temur mit dem Schwert ins Gesicht. Im selben Augenblick griffen die Mamelucken an. Die mongolischen Stabsoffiziere, die sich um Temur kümmerten, waren während der entscheidenden Eröffnungsphase der Schlacht dermaßen abgelenkt, daß dies zu einer Niederlage führte. Vgl. Chambers, James: The Devil's Horsemen. 160—162

[23] Vgl. Liddell Hart, Sir Basil H.: Great Captains Unveiled. Putnam's, New York 1931, 160—162. In seinen frühen Abhandlungen zur Rolle des Panzermanövers in der Kriegsführung werden die Mongolen als mögliches Vorbild für den Blitzkrieg genannt.

[24] In den Memoiren von Heinz Guderian und F.W. von Mellenthin finden sich zahlreiche Beispiele, wie die Kommunikation über Funk es den deutschen Panzern ermöglichte, das Feuer so lange zu konzentrieren, bis ein

Ziel zerstört war, und dann zu einem neuen Angriffsziel überzugehen. Das Feuer wurde zuerst vor allem auf die Kommandowimpel gerichtet, da die Deutschen über die unzulängliche Funkausrüstung ihrer Gegner Bescheid wußten. Obwohl die Russen für ihre Unterlegenheit in punkto Kommunikation mit großen Opfern büßen mußten, mußte auch Frankreich mit seinen zahlenmäßig überlegenen und schwerer bewaffneten Panzern 1940 Verluste verzeichnen, da zwar alle Panzer über Funkempfänger verfügten, jedoch nur Kommandofahrzeuge Funksprüche absetzen konnten. Außerdem war es für die Franzosen nachteilig, daß sie ihre Panzer gleichmäßig entlang der Front einsetzten, anstatt sie zum Gegenangriff zu konzentrieren. Ein weiteres interessantes Detail ist, daß Guderian seine Karriere als Nachrichtenoffizier begann. Vgl. Guderian, Heinz: Erinnerungen eines Soldaten. Vowinckel, Heidelberg 1951; Mellenthin, F. W.: Panzerschlachten. Vowinckel, Neckargmünd 1963

[25] Stolfi behauptet, daß der "Schwenk" der Deutschen in Richtung Ukraine die einzige Chance Hitlers zunichtemachte, den Krieg gegen die Sowjetunion durch einen Angriff auf das Zentrum ihrer strategischen Kommunikation zu gewinnen. Vgl. Stolfi, R.H.S.: Hitler's Panzers East: World War II Reinterpreted. University of Oklahoma Press, Tulsa 1992.

Liddell Hart bezeichnet die Debatte darüber, ob man Moskau direkt angreifen oder zuerst die sowjetische Feldarmee vernichten hätte müssen, als eine "Schlacht der Theorien", die von den "Vertretern der militärischen Orthodoxie" gewonnen wurde. Vgl. Lidell Hart, Sir Basil H.: History of the Second World War. Putnam's, New York 1970, 175—170

[26] Mao Zedong stützt seine Theorie des Guerillakriegs auf seine Erfahrungen im Kampf gegen die Japaner, die sich, ebenso wie später die Amerikaner in Vietnam, hauptsächlich auf die Unterbrechung der taktischen Kommunikation konzentrierten.Milton Miles wiederholt Maos Standpunkt in seiner Analyse desselben Konfliktes. Vgl. Miles, Milton E.: A Different Kind of War. Doubleday, New York 1968. Die Analyse Desert Revolt von Thomas E. Lawrence bestätigt diese Ansicht ebenso. Vgl. Lawrence, Thomas E.: Seven Pillars of Wisdom. Doubleday, New York 1938

[27] Powell, Colin L., "Information-Age Warriors". In: Byte. Juli 1992, 370

[28] Vgl. obiges Zitat von Sproull und Kiesler

[29] Posen, Barry R.: The Sources of Military Doctrine. Cornell University Press, Ithaca 1984, 36

[30] Auch das ist ein neuer Begriff, den einige Visionäre und Praktiker aufgegriffen haben. Vgl. z.B. Benedikt, Michael (Hg.): Cyberspace: First Steps. MIT Press, Cambridge 1991. Der Begriff stammt ursprünglich aus dem "Cyberpunk"-Science-fiction-Roman Neuromancer von William Gibson (1984). Es ist der umfassendste aller derzeit zur Bezeichnung des neuen Bereich des elektronischen Wissens, der elektronischen Information und Kommunikation erprobten Begriffe. Teils existiert dieser Bereich and festen Standorten in Form von Hardware oder Software, teils aber auch in Übertragungen über Kabel, oder in der Luft bzw. im Weltraum. General Powell (1992) weist in dieselbe Richtung, wenn er behauptet, der "Kampfraum" verfüge über eine "Infosphäre".

[31] Chris Bellamy befaßt sich in seiner Analyse des zukünftigen Landkrieges mit einigen dieser Themen. Vgl. Bellamy, Chris: The Future of Land Warfare. Helm, London 1987

[32] Wir möchten darauf hinweisen, daß der gefeierte US-Geheimdienst während der Operation "Wüstensturm" kaum bis zu den Divisionskommandanten vorgedrungen ist; für diese kam jeder größere Zusammenprall mit den feindlichen Truppen erwiesenermaßen überraschend. Vgl. Grier, Peter: "The Data Weapon". In: Government Executive. June 1992, 20—23

[33] Für Kenneth N. Waltz stellt das Phänomen der "Imitation" einen wesentlichen Faktor für die Herstellung des "inneren Gleichgewichts" dar, welche für alle Nationen von ständigem Interesse ist. Sobald man davon überzeugt ist, daß eine militärische Innovation funktioniert, werden bald alle dem Beispiel des Erfinders folgen. Ein gutes Beispiel dafür ist, daß die gesamte Marine weltweit ihre Holzschiffsrümpfe mit einem Schlag durch solche aus Metall ersetzte, nachdem man im Amerikanischen Bürgerkrieg erstmals mit Eisenverkleidungen experimentiert hatte. Vgl. Waltz, Kenneth N.: Theory of International Politics. Random House, New York 1979

[34] Ein klassisches Beispiel ist die Schlacht in der Normandie 1944. Feldmarschall Montgomerys Truppen nagelten das VII. Deutsche Regiment fest und ermöglichten General Pattons III. Regiment, die deutsche Verteidigung auf breiter Front zu überrennen.

[35] Die Autoren danken Gordon McCormick für seine Beiträge zu diesem Thema. Vgl. weiters Arnett, Eric H.: Gunboat Diplomacy and the Bomb: Nuclear Proliferation and the U.S. Navy. Praeger, New York 1989

[36] Dieser letzte Punkt wurde durch die Überlegungen des RAND-Kollegen Ken Watman angeregt.

[37] Es gibt eine Sorte Proliferatoren, denen gegenüber wir nicht länger vor Gewaltmaßnahmen zurückschrecken werden. Irak, Iran, Nordkorea, Libyen und Kuba zählen zu den Nationen, die durch ihre Drohung, Massenvernichtungswaffen zu erwerben, eine Intervention rechtfertigen würden. Die Vorstellung, daß die Vereinigten Staaten die Doktrin einer "selektiven Präventivmacht" gegen "vogelfreie" Staaten annehmen sollte, wird näher erläutert in Arquilla, John: "Nuclear Proliferation: Implications for Conventional Deterrence". In: Arquilla, John; Niblack, Preston (Hg.); RAND: American Grand Strategy in the Post-Cold War World. Santa Monica 1992

[38] Vgl. Powell, Colin L.: "Information-Age Warriors". In: Byte. July 1992, 370

[39] Dieses Thema wird bei Arquilla detailliert behandelt, vgl. Arquilla, John: "Louder Than Words: Tacit Communication in International Crises". In: Political Communication. Bd. 9, 1992, 155—172

[40] Dieses Konzept stammt aus dem Koreakrieg, wo es während der ersten Phase des US-Einsatzes darum ging, zu verhindern, daß die koreanische Halbinsel in den ersten Kriegsmonaten überrannt wurde. Die Pusan-Grenze hielt einen Teil Südkoreas frei und diente dazu, nordkoreanische Truppen anzuziehen. Der mit Amphibienfahrzeugen durchgeführte Gegenangriff bei Inchon, weitab von der Kriegsfront, brachte die Aggressoren völlig aus dem Konzept.

[41] Van Creveld, Martin: The Transformation of War. Free Press, New York 1991

[42] Kenney und Dugan rufen zu einem "Balkansturm" auf, bei dem überhaupt keine amerikanischen Bodentruppen zum Einsatz kommen würden. Wir stimmen mit diesem Ansatz nicht überein, da er in Theorien der "beschränkten Haftung" und des "Luftmacht-Exeptionalismus" wurzelt. Dennoch werden hier zahlreiche Schlüsselformen von luftkampfgestützten Cyberkriegtaktiken aufgezeigt, die sehr wohl zur Anwendung kommen könnten, auch wenn der Wegfall einer amerikanischen Bodentruppe alle Kampferfolge entschieden schmälern würde. Vgl. Kenney, George; Dugan, Michael J.: "Operation Balkan Storm: Here's a Plan". In: The New York Times. 29. November 1992