Shen Weiguang
Der Informationskrieg — eine neue Herausforderung

Das 20. Jahrhundert ist ein äußerst bewegtes Kapitel in der Geschichte des Militärs: Es brachen zwei Weltkriege aus, es fand eine militärische Revolution statt, die beim klassischen Infanterie- und Kavalleriekrieg begann und beim mechanisierten Krieg endete … Jetzt, am Ende des 20. Jahrhunderts, hatten wir noch kaum Zeit innezuhalten und zurückzublicken, und schon zeichnet sich eine völlige neue Form des Krieges am Horizont ab: der Informationskrieg.

Vom mechanisierten Krieg zum Informationskrieg

Seit dem Zusammenbruch des Eisernen Vorhangs und dem Ende des Kalten Krieges, also seit der Auflösung der zwei großen Machtblöcke, hat sich in der internationalen Militärstrategie eine Wende von historischer Bedeutung vollzogen, die die Gefahr des Ausbruchs eines Weltkrieges im klassischen Sinn reduziert hat. Der Schwerpunkt der internationalen Beziehungen und der Fokus der allgemeinen Aufmerksamkeit hat sich auf die Wirtschaft verlagert, die internationalen strategischen Beziehungen sind nicht mehr durch die Gegenüberstellung der beiden Supermächte und einen Rüstungswettlauf gekennzeichnet, sondern haben sich auf den wirtschaftlichen Wettstreit und eine Auseinandersetzung über Wertvorstellungen verlagert.

In dem Moment, als die Menschen das Ende des Kalten Krieges feierten und begannen, die traditionellen militärischen Werte zu hinterfragen, haben die westlichen Militärmächte unter der Führung der Vereinigten Staaten eine neue militärische Revolution ausgelöst. Jede Analyse des Informationskriegs muß auf dem Hintergrund dieser Militärrevolution stattfinden, denn nur so kann man diese neue Form des Krieges in ihrer ganzen Tragweite erfassen, denn der historische Hintergrund ist die Basis, ohne die Neues nicht entstehen kann.

Jedes neue Zeitalter ist das Produkt einer technologischen Revolution, und eine technologische Revolution ist das Vorspiel eines neuen Zeitalters. Dies ist ein Gesetz, das für alle gesellschaftlichen Veränderungen und Entwicklungen gilt und die Logik sozialer Ereignisse bestimmt. Die militärischen Aktionen der Menschheit, ihre Kriege folgen seit jeher diesem Muster.

Die durch die Eisenschmelze bedingte technologische Revolution hat die Ackerbaukultur und die Entwicklung von Kriegswaffen ermöglicht und die durch die Verwendung von Schußwaffen bedingte Revolution im Kriegswesen ausgelöst.

Die Erfindung der Dampfmaschine markierte den Beginn des Industriezeitalters. Auf dem Schlachtfeld hielten Panzer und Kanonen Einzug. Dies bedeutete den Beginn des mechanisierten Krieges — ein weiterer historischer Quantensprung. Die Mikroelektronik und der Computer führten zur dritten Welle der technologischen Revolution: dem Informationszeitalter mit seinem Krieg der unsichtbaren Geschosse und der jüngsten militärischen Revolution.

Diese militärische Revolution wurde bereits Ende der siebziger Jahre in der früheren Sowjetunion vorausgesagt. Der damalige Generalstabschef der sowjetischen Armee, Marschall Ogarkov, und einige berühmte Militärtheoretiker prophezeiten, daß die Entwicklung neuer nichtnuklearer Technologien zu einer Revolution im militärischen Bereich führen würde. Damals haben sie die Informationstechnologien, deren Herzstück der Computer

war, in den militärischen Bereich inkorporiert und Zielerfassungssystemen wie Präzisionslenkwaffen vermehrt Aufmerksamkeit geschenkt. Sie gingen davon aus, daß man mit Hilfe dieser damals noch in Entwicklung befindlichen neuen Technologien, die die alten wissenschaftlichen Grundsätze von Grund auf in Frage stellten, höchstwahrscheinlich in der Lage wäre, noch wesentlich verheerendere Waffen herzustellen, als es die Atomraketen sind, was eine militärische Revolution auslösen würde. Nach dem Golfkrieg im Jahre 1991 waren nicht wenige amerikanische Generäle der Ansicht, daß der Golfkrieg dank amerikanischer Militärtechnologie kombiniert mit sowjetischem Militärdenken gewonnen werden konnte. Dies ist eine objektive Einschätzung der Tatsache, daß die Militärführung der damaligen Sowjetunion als erste diese neuerliche Militärrevolution erkannt hat.

Die Initiative für die Umsetzung dieser Militärrevolution ging jedoch von den Amerikanern aus. In den USA sind zur Zeit großangelegte Forschungen über die technische Seite des Informationskrieges im Gange, und es werden die verschiedensten Maßnahmen getroffen, um den Informationskrieg tatsächlich Wirklichkeit werden lassen zu können. Dazu zählen:

— Theoretische Forschung im Bereich des Informationskrieges und Festlegung einer Strategie für den Informationskrieg

— Errichtung eines integrierten C4ISR-Systems (Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance) — Geheime Forschungen über einen Angriffsinformationskrieg — Forschungen über Abwehrmaßnahmen — Simulationen für einen Informationskrieg

Auch die chinesischen Militärtheoretiker haben sich bereits früh mit dieser weltweiten Militärrevolution und dem Informationskrieg auseinandergesetzt. 1983 begann die chinesische Forschung, sich mit den durch die neuen Technologien bedingten revolutionären Veränderungen zu beschäftigen. Im Zuge dieser Forschungen entstand der Plan "863", der ein positives Klima für Forschung im Sektor der Hochtechnologie schuf. Parallel dazu erlebte die theoretische Forschung im militärischen Bereich ihren ersten Höhepunkt.

Was den Begriff des Informationskrieges betrifft, so ist er zum ersten Mal in China verwendet worden. Ich habe bereits 1985 begonnen, mich mit dem Konzept des Informationskrieges auseinanderzusetzen und in einem wissenschaftlichen Aufsatz den Begriff des "Informationskrieges" (chin: xinxi zhan) formuliert. Im April 1987 hat die maßgebliche Militärzeitschrift Chinas, Jiefangjun bao ("Zeitung der Volksbefreiungsarmee"), einen Artikel mit dem Titel Xinxizhan de jueqi ("Die Vorboten des Informationskrieges") veröffentlicht und darin die Ergebnisse meiner Forschungen dargelegt. 1990 erschien mein Buch Xinxizhan ("Der Informationskrieg") im Verlag Zhejiang Daxue.

Bald darauf brach der Golfkrieg aus, und die Militärs begannen, sich verstärkt dem High-Tech-Krieg zuzuwenden. In China haben immer wieder verschiedene offizielle militärwissenschaftliche Forschungseinrichtungen, aber auch nichtstaatliche Organisationen sowie Armeestellen Konferenzen über die militärische Revolution abgehalten und auf breiter Basis Bedeutung, Inhalt, Besonderheiten, geschichtlichen Hintergrund und die Auswirkungen, die diese Revolution im eigentlichen militärischen Bereich hat, beleuchtet.

Was den Begriff "Informationskrieg" betrifft, so gibt es weltweit die unterschiedlichsten Definitionen. Wenn man aber von der Grundbedeutung ausgeht, so haben alle Definitionen einige Aspekte gemein: Das Ziel eines Informationskrieges ist die Erlangung der informationellen Vormachtstellung; der Informationskrieg ist eine kriegerische Handlung, die

sowohl Angriff als auch Verteidigung umfaßt; das Ziel einer Attacke ist entweder das Informationssystem und dessen Infrastruktur oder der Prozeß des Informationstransfers an sich. Der Informationskrieg kann deshalb folgendermaßen beschrieben werden: Der Informationskrieg ist eine Auseinandersetzung, bei der beide feindlichen Seiten um die Vormachtstellung im Erwerb, in der Kontrolle und Anwendung von Information kämpfen, wobei die wesentlichsten Mittel dazu informationelle Maßnahmen bzw. Ausrüstungen sind.

Im Jahr 1985 habe ich den Informationskrieg folgendermaßen definiert: Im weitesten Sinn ist der Informationskrieg eine Auseinandersetzung, bei der kampfbereite militärische (aber auch politische, wirtschaftliche, kulturelle und technologische) Einheiten gewaltsam die Infosphäre besetzen und einander Informationsressourcen streitig machen. Damit sind vor allem Aktivitäten gemeint, im Zuge derer ein Staat Information dazu benutzt, seine strategischen Zielsetzungen zu verwirklichen. Ein praktisches Beispiel dieser Art von Informationskrieg ist z. B. das Ende des Kalten Krieges. Im engeren Sinn meint der Begriff die im Zuge eines Krieges stattfindende Konfrontation zweier Gegner in der Infosphäre, was ein wesentliches Merkmal eines modernen Krieges ist. Dabei kann man den strategischen und den taktischen Informationskrieg unterscheiden, wobei es sich bei ersterem um einen Krieg außerhalb des durch Waffengewalt gekennzeichneten "Gefechtsfeldes" handelt, d. h. um Aktivitäten, die in einer konflikterzeugenden politischen Atmosphäre, im neuen "Raum der Kriegsführung" stattfinden. Das Angriffsziel ist der Geist, das Denken des Gegners, vor allem jener Bereich, in dem Entscheidungen gefällt werden. Der taktische Informationskrieg ist der Informationskrieg auf dem Gefechtsfeld, d. h. der Command- und Control-Krieg, der Krieg zur Erlangung der Kontrolle über relevante Informationen, wobei die Information an sich das wesentliche Kriegsinstrument darstellt. Ziel ist es, die gegnerischen Aufklärungs- und Informationssysteme anzugreifen und die Entschlossenheit der gegnerischen Entscheidungsträger und die dadurch bedingten Handlungen zu beeinflussen, zu unterbinden oder zu verändern. Die Erscheinungsformen des Informationskrieges sind äußerst vielfältig: psychologische Kriegsführung, nachrichtendienstlicher Krieg, Strategiekonkurrenz, theoretische Abschreckung, potentielles Kräftemessen, elektronischer Krieg, Waffensysteme zur Vernichtung der gegnerischen Informationsinfrastruktur, Computervirenkrieg, Präzisionskrieg, verdeckter Krieg usw.

Der Schauplatz eines Informationskrieges unterscheidet sich von dem eines konventionellen Krieges vor allem dadurch, daß er in einem "unsichtbaren Raum" liegt. Der Informationskrieg ist ein formloser, unblutiger Krieg.

Der Informationskrieg umfaßt sechs Aspekte, nämlich Beschaffung, Anwendung, Schutz, Nutzung, Fernhaltung und Verwaltung von Information. Die sechs wesentlichen Charakteristika sind: 1) Der Informationskrieg ist ein Krieg, den die Kriegsparteien in der Infosphäre führen; 2) der Informationskrieg hat zum Ziel, die informationelle Vormachtstellung zu erlangen; 3) im Informationskrieg besteht das wesentlichste Angriffsziel darin, das gegnerische C4I-System (Command, Control, Communication, Computer, Intelligence) zu behindern, zu schwächen, zu sabotieren und zu vernichten; 4) im Informationskrieg sind informationelle Waffen und Informationssysteme die wichtigsten Mittel der Kriegsführung; 5) der Informationskrieg ist ein Krieg, der einem Real-time-Krieg sehr nahe kommt; da er sich der Informationssysteme bedient, wird der Kampfraum wesentlich ausgeweitet, während gleichzeitig die Dichte der militärischen Kräfte dementsprechend abnimmt und die Kriegsdauer verringert werden kann; 6) das wesentlichste Mittel des Informationskrieges besteht im Korrumpieren von Information.

Dabei ist die Vorherrschaft im informationellen Bereich einer der wesentlichen Faktoren, die über Sieg oder Niederlage entscheiden; sie ist ein Multiplikator der Stärke. Überlegenheit im informationellen Bereich bedeutet auf dem "Gefechtsfeld" konkret, daß es gelingt, Information rechtzeitig, umfassend und präzise zu nutzen; die überlegene Seite ist also in der Lage, Information frei zu nutzen. Aus dem strategischen Blickwinkel betrachtet, bedeutet dies, daß vor allem Techniken zum Informationstransfer bzw. zur -verbreitung voll ausgenutzt werden, um nicht nur die Kampfmoral des Gegners zu schwächen, sondern vor allem auch um das allgemeine Funktionieren des politischen und wirtschaftlichen Systems des Gegners zu zerstören und ihn zu lähmen.

Eine neue Sichtweise des Krieges

Mit der Informationsgesellschaft verändern sich althergebrachte Formen der Kriegsführung, gleichzeitig wird auch die traditionelle Auffassung vom Wesen des Krieges vehement in Frage gestellt.

Bislang war Krieg die Fortführung der Politik, die höchste Form des Kampfes, die sich gewaltsamer Mittel bedient, um Konflikte zwischen gesellschaftlichen Gruppen zu lösen. Der Informationskrieg ist jedoch nicht mehr nur die Fortführung der Politik, er findet nicht mehr nur zwischen Völkern, Staaten, sozialen Klassen und politischen Gruppierungen statt, sondern liefert die Voraussetzung dafür, daß auch unpolitische Gruppierungen, ja, sogar Einzelpersonen ihre Interessen durchsetzen und ihre Existenz unter Beweis stellen können. Unternehmen, religiöse Gruppen, Terrorgruppen, Stammesguerillatruppen, Drogendealer oder andere kriminelle Banden können einen Krieg auslösen. Jede beliebige gesellschaftliche Gruppe, jede Einzelperson kann ein mit einem Chip ausgerüstetes System angreifen, in eine ans Netz angebundene Anlage eindringen und das Netz benutzen, um einen speziellen Krieg auszulösen. Sie muß nur die zur Kommunikation notwendige Computertechnologie beherrschen, über einen Computer und eine Anbindung ans Netz via Telefonleitung verfügen. Daher muß man die politischen Hintergründe eines Krieges konkret analysieren und untersuchen, bevor man dessen Wesen feststellen kann.

Im Informationszeitalter verändern sich auch die Unterscheidungen das Wesen des Krieges betreffend. Im traditionellen Krieg kannte man zwei große Kategorien: den gerechten Krieg und den ungerechten Krieg. Jede Art von Widerstand gegen Unterdrückung und Ausbeutung oder gegen eine äußere Aggression, jeder Krieg, der den sozialen Fortschritt zum Ziel hat, galt als gerechter Krieg; hingegen galt jeder Krieg, der eine Revolution unterdrückte, auf Aggression und Expansion nach außen hin gerichtet war oder den gesellschaftlichen Fortschritt verhindern wollte, als ungerechter Krieg. Mit dem Informationszeitalter sind jedoch sehr viele Merkmale eines Krieges vage und nebulös geworden, denn es ist oft nicht mehr möglich, gewisse bewaffnete Zusammenstöße, militärische Aktionen oder lokal begrenzte Kriege den Kategorien "gerechter Krieg" bzw. "ungerechter Krieg" zuzuordnen. Das Wesen des Krieges wird also immer komplexer.

Im Informationszeitalter verwischen sich auch die Grenzen zwischen Kriegsvorbereitung und -durchführung. Die nach Hegemonie strebenden Staaten sind praktisch ständig dabei, Kriegsvorbereitungen zu treffen, und könnten daher jederzeit einen Krieg beginnen. Die Beeinflussung der öffentlichen Meinung, nachrichtendienstliche Abwehr und Überwachung des Netzes sind in Wirklichkeit nichts als eine in ihrer Form veränderte militärische Invasion, sie sind bereits Teil der Kriegspraxis.

Im Informationszeitalter stellt die informationelle Abschreckung eine neue Variante der Abschreckung dar. Wie die atomaren, biologischen und chemischen Waffen, die ein extrem hohes Tötungs- und ein beträchtliches Abschreckungspotential aufweisen, bergen auch die neuen Methoden und Möglichkeiten eines Informationskrieges ein hohes Abschreckungspotential und können unter Umständen die Eskalation eines Krieges verhindern.

Im Informationszeitalter ist die Information eine strategische Ressource, die ebenso wichtig ist wie materielle Güter oder Energie, und die Informationsindustrie stellt bereits eine der wichtigsten Industrien eines Staates dar. Der Faktor Information ist ein Produktionsfaktor geworden, der sich in einem exponentiellen Verhältnis zu anderen Produktionsfaktoren entwickelt. Auf die einzelnen Länder bezogen — egal, ob sie sich im Agrar- oder im Industriezeitalter befinden — bedeutet dies, daß sie sich direkt — oder indem sie eine Entwicklungsstufe überspringen — in Richtung Informationszeitalter orientieren müssen. Im militärischen Bereich bringt das Informationszeitalter den Informationskrieg hervor, so wie das Zeitalter der Schwerindustrie den mechanisierten Krieg hervorgebracht hat. Egal, wie man dieser Frage zur Zeit gegenübersteht, es handelt sich um eine unausweichliche historische Entwicklung.

Neue Kriegsformen verändern die Doktrinen

"Information" bedeutet im militärischen Bereich auch "nachrichtendienstliche Information". Obwohl die Militärs früher genausowenig wie heute ohne derartige Informationen ausgekommen sind, waren sie während früherer Kriege bei der Beschaffung und Verarbeitung von Information, im Entscheidungsprozeß, beim Erlassen von Befehlen oder beim Einsatz und der Kontrolle von Streitkräften allein auf das menschliche Gehirn angewiesen. Nur wenn es selbstverständlich ist, daß dieser gesamte Prozeß vom menschlichen Gehirn gemeinsam mit Computern und Netzwerken bewältigt wird, kann man von einem echten Informationskrieg sprechen.

Die durch die Entwicklung vom mechanisierten Krieg zum Informationskrieg bedingten Veränderungen schlagen sich in erster Linie in einer Veränderung in der Kriegsform nieder.

Die Operationsfreiheit der Truppen hängt von der Informationsherrschaft ab. Die Operationsfreiheit einer Truppe auf dem Gefechtsfeld ist ein Indikator dafür, in welchem Ausmaß sie die Initiative im Krieg innehat. Initiative ist gleich Operationsfreiheit. Der Informationskrieg eröffnet eine fünfte Dimension, d. h. die Initiative im Krieg verlagert sich weg von der Land-, Luft-, See- und Weltraumherrschaft hin zur Informationsherrschaft. Mit anderen Worten: Nur die Truppen, die die Informationsherrschaft innehaben, genießen Operationsfreiheit. Informationsherrschaft ist jedoch nicht gleichzusetzen mit technischer Überlegenheit und hängt auch nicht vollkommen von dieser, sondern viel mehr von einer neuen Taktik ab und auch davon, ob die Kommandanten zu eigenständigem, kreativem Denken fähig sind. Das Kriegsziel wird im Hinblick darauf gewählt, die gegnerische Entscheidungsfindung zu stören. In früheren, auf die Eroberung von Territorien gerichteten Kriegen galt das Prinzip, die feindliche Effektivstärke zu vernichten, während im Informationskrieg das Prinzip gilt, die Entscheidungsabläufe des Feindes so sehr zu stören, daß er seine Aktivitäten nicht mehr wirksam koordinieren kann. Geht man einen Schritt weiter, so besteht das Hauptziel eines Informationskrieges darin, die Wissens- und Glaubenssysteme des Feindes zu attackieren.

Die Feuerkraft wird nicht mehr flächendeckend angewendet, sondern punktgenau. Der mechanisierte Krieg, der die Produktionsweise des Zeitalters der Schwerindustrie widerspiegelt, ist ein in hohem Maße schematisierter Krieg und ähnelt darin der industriellen Produktion am Fließband, d. h. er verläuft sehr koordiniert, geordnet, aber auch starr und rigide. Die Informationsgesellschaft verändert die traditionellen Formen der Fließbandproduktion, so wie der Informationskrieg die traditionelle schematisierte Kriegsführung verwandelt. Das wesentliche Charakteristikum des Informationskrieges besteht darin, daß er mit Präzision und Geschwindigkeit arbeitet: Präzisionsangriffe auf Ziele außerhalb der Sichtweite werden zum grundlegenden Verwendungsmuster für Feuerkraft. "Carpetbombing", flächendeckende Bombardierung, gehören der Vergangenheit an, "punktgenaue" strukturelle Zerstörung löst die traditionelle Form des schematisierten Krieges ab.

Sonderkommandos und Spezialkriege gewinnen an Bedeutung. Sonderkommandos repräsentieren eine spezielle Form der Kräfteorganisation. Ihre Merkmale sind: Flexibilität, hohe Effizienz, geringe Größe.

Das Kommandosystem geht in Richtung Verflachung. In einem Informationskrieg müssen die Kommandanten extrem effizient arbeiten, und diese Steigerung der Effizienz kann nur durch eine Reduktion der Kommandoebenen erreicht werden. Infolgedessen muß das traditionelle vielstufige, pyramidenförmig angelegte Kommandosystem aufgebrochen werden. Die Informatisierung und Vernetzung der Truppen schafft die traditionelle Kommandospanne ab und läßt anstelle einer pyramidenförmigen eine flache Struktur entstehen. Wie auch die auf die Anforderungen des Informationszeitalters reagierenden Unternehmen sind die Armeen vieler Länder der Welt gerade dabei, die Top-down-Struktur ihrer unbeweglichen Command- und Control-Systeme zu lockern und ein neues System aufzubauen, das die Dynamik einer flachen Kommandohierarchie und der sich auf feindlichem Territorium befindlichen Offiziere und Soldaten zu entfalten vermag.

Auf einem nur schwer abzugrenzenden Kriegsschauplatz muß die Kraft des Volkes voll ausgenutzt werden. Der Informationskrieg ist ein Krieg, der mit Mitteln der Hochtechnologie geführt wird und an dem das gesamte Volk beteiligt ist. Im Zuge der Errichtung des weltweiten Datenhighways können nichtstaatliche Gruppierungen sowie Einzelpersonen die an die weltweiten Datennetze angebundenen Computer- und Informationssysteme nutzen und so am Informationskrieg teilnehmen. Vom strategischen Standpunkt aus gesehen ist der informatisierte Kriegsschauplatz äußerst schwer einzugrenzen. Die Soldaten haben nicht länger die Gelegenheit, im Nahkampf feindliche Stellungen zu erstürmen und sich ihrer Heldentaten zu brüsten. Die Computerprogrammierer ziehen sich vielleicht in ihre Büros oder Häuser zurück, um von dort aus zu kämpfen. In einem Krieg, dessen Grenzen zusehends verschwimmen, kommt der allgemeinen Mobilmachung und dem Ausnützen der Kraft des Volkes besondere Bedeutung zu. Erst der Zusammenhalt des Volkes als Ganzes verleiht dem Krieg seine Macht.

Die von Sunzi vertretene Strategie des "vollkommenen Sieges" kommt erst im Informationskrieg voll zum Tragen. Der Krieg ist die Fortsetzung der Politik, und daß er eine blutige Politik ist, das haben die Menschen schon sehr früh erkannt. Sunzi suchte bereits vor mehr als zweieinhalbtausend Jahren nach einer Möglichkeit, einen unblutigen Krieg zu führen, und formulierte dabei seine berühmten Stratageme "Siegen, ohne zu kämpfen" und "Sind die Truppen unversehrt, dann wird der Sieg umfassend sein". Diese Konzepte kommen erst im Informationszeitalter in vollem Ausmaß zum Tragen. Wir können nicht davon ausgehen, daß ein zukünftiger Krieg ein Kinderspiel sein wird, aber wenn der technologische

Fortschritt die Zivilisierung der Gesellschaft vorantreibt, dann werden sich auch das Konzept von Gewalt und die konkrete Anwendung von Gewalt verändern.

Die Anwendung von Stratagemen wird facettenreicher. Auch wenn der Informationskrieg über verschiedene öffentliche und militärische Telekommunikationsnetzwerke und Medien geführt wird, ist nicht die Technologie der über Sieg und Niederlage bestimmende Faktor, sondern das Entscheidungsverhalten der Menschen. Die am Krieg Beteiligten setzen äußerst konzentrierte dezentrale Handlungen und vollziehen in engster Abstimmung autonom getroffene Entscheidungen. Ein derartiges Vorgehen setzt jedoch voraus, daß der Kommandant über einen höchst kreativen Geist verfügt. Der Fortschritt in der Informationstechnologie hat den menschlichen Faktor nicht nur nicht geschwächt, sondern im Gegenteil verstärkt und noch deutlicher gemacht, daß Kommandieren eine Kunst ist. Da der Kriegsgegner nicht eindeutig festzumachen ist, da sich die Umgebung ständig verändert, der Kriegsrhythmus beschleunigt und die Informationsmenge zunimmt, gewinnt das Kriegsgeschehen in Zukunft an Komplexität und Unfaßbarkeit. Dadurch eröffnet sich auch dem Einsatz von Stratagemen ein weites Feld.

Neue Aspekte des Krieges

Im lautlosen Kampf des Informationskrieges kommt dem geistigen Aspekt größere Bedeutung zu; wenn früher Intelligenz und Mut die entscheidenden Faktoren waren, so ist es heute in erster Linie Intelligenz. Da dieser Krieg ein Kräftemessen auf intellektueller Ebene ist, können strategische Fehler nur sehr schwer durch taktische oder operative Anstrengungen wettgemacht werden, denn bei einem Versagen auf intellektueller Ebene verlieren die Informations- und Kontrollsysteme, also das "Nervensystem" der Truppe, ihre Wirksamkeit.

Ein weiterer Aspekt liegt darin, daß ein "weicher" Schlag wichtiger wird als ein "harter". Da es im Informationskrieg darum geht, Kontrolle über die Informations- und Wissenssysteme des Gegners zu erlangen — vor allem über das Denken der Befehlshaber und Entscheidungsträger — und gleichzeitig die eigenen Bedürfnisse zu schützen, kann man von einem "weichen" Schlag von System gegen System sprechen. Bleibt es bei einem solchen weichen Schlag, kann der Krieg ohne Blutvergießen beendet werden. Deshalb muß es gelingen, den traditionellen Krieg, bei dem "der Gegner vernichtet und die eigene Seite gewahrt" wird, in einen Krieg zu transformieren, bei dem "der Gegner unter Kontrolle gebracht und die eigene Seite gewahrt wird".

Drittens verlagert sich der Informationskrieg in Richtung Volkskrieg. Die wesentlichsten Unterschiede zwischen einem traditionellen Krieg und dem Informationskrieg sind: Das Ziel kann ein ganz beliebiger Bürger sein, aber jeder Bürger kann auch aktiv am Krieg teilnehmen, und die in einen Informationskrieg involvierten Personen können reguläre Militärs, aber genauso gut auch Jugendliche sein. Außerdem sind viele Ausrüstungsgegenstände, die auf dem "Gefechtsfeld" verwendet werden, also z. B. Computer oder optische Instrumente, im freien Handel erhältlich und sind ursprünglich auch für den zivilen Bereich entwickelt worden. Darüber hinaus findet der Krieg nicht am traditionellen Kriegsschauplatz mit Waffengewalt statt, sondern durchdringt die gesamte Gesellschaft. Der Informationskrieg ist ein Volkskrieg im wahrsten Sinn des Wortes. Viertens stellt der Informationskrieg die traditionellen Konzepte von Angriff und Verteidigung in Frage. Er mißt zwar dem Angriff eine beträchtliche Bedeutung bei, noch wichtiger jedoch ist die Verteidigung. Ein Grund dafür liegt darin, daß, wenn man Angriffs- und Verteidigungs-Informationskrieg vergleicht, der Angriff sich oft nur auf einen einzelnen Punkt konzentriert, während die Verteidigung sich auf die Gesamtfläche bezieht; es handelt sich um eine Verteidigung in alle Richtungen. Was

die Abwehr betrifft, so ist es nicht leicht, im Raum der Computer den Angreifer ausfindig zu machen. Außerdem ist die versteckte Bedrohung, die von einem derartigen Angriff ausgeht, schwer zu fassen, eine rechtzeitige Voraussage ist schwer zu treffen, und das Resultat von Abwehrmaßnahmen ist schwer im voraus abzuschätzen. Darüber hinaus verläßt man sich bei einem Informationskrieg, wie er zur Zeit diskutiert wird, in hohem Maße auf Elektronik, was die Verwundbarkeit der nationalen Netzwerke im Falle eines Informationskrieges verstärkt. Dazu kommt, daß im Informationszeitalter ein Angriff, der Verteidigung ist, effizienter ist als eine reine Abwehr. Fünftens sind im Informationskrieg eindeutige Festlegungen nicht mehr möglich. Im Zuge der sich ständig verbessernden Informationsinfrastruktur verschwimmen die Grenzen zwischen einigen bislang streng von einander abgegrenzten Begriffen (z. B. öffentliches Wohl und privates Wohl, Krieg und Verbrechen). Wenn in einem vernetzten Informationssystem der Informationskrieg ausbricht, verlieren z. B. die Grenzen zwischen Staaten und Regionen ihre Funktion. Es ist schwierig zu eruieren, woher eine Bedrohung kommt, ja, es ist sogar schwierig festzustellen, wer angegriffen wurde und wer die Verantwortung für den Angriff hat. Andererseits ist es sehr schwierig, die einzelnen Ebenen feindlicher Aktion zu unterscheiden, die von einer kriminellen bis zu einer kriegerischen Handlung reichen können. Der Schaden, den Computerkriminalität anrichten kann, könnte in Zukunft größer sein als der Schaden, der aus einem militärischen Angriff resultiert. Dadurch büßt die traditionelle Arbeitsteilung zwischen Regierung und Militär und den einzelnen Ministerien einer Regierung (z. B. Ministerium für innere Sicherheit, Nachrichtendienst, die für die Vollstreckung von Gesetzen zuständigen Stellen usw.) an Wirksamkeit ein.

Sechstens besteht zwischen konventionellem Krieg und Informationskrieg eine Gemeinsamkeit, nämlich daß das Land, das die Schlüsselwaffe beherrscht — wie z. B. im Falle der Atombombe — die Fähigkeit zum Erstschlag bzw. Vergeltungsschlag hat. Das gleiche gilt auch für den Informationskrieg: Auch hier gibt es sowohl im Angriffs- als auch im Verteidigungsbereich eine Reihe von Schlüsseltechnologien. Es ist unmöglich, alle sich von Tag zu Tag verändernden modernen Waffen zu beherrschen, aber zumindest sollte man sie besitzen, um sie praktisch oder zu Abschreckungszwecken einsetzen zu können. Künftig sollte man eine Reihe von Bestimmungen erlassen, die den Informationskrieg regeln und die alle Konfliktparteien respektieren müssen: Der Informationskrieg ist nur ein Kräftemessen und darf nicht dem Wohl der gesamten Menschheit schaden, vor allem nicht der Menschheit selbst. Ich bin der Überzeugung, daß derjenige, der in Zukunft eine die gesamte Menschheit schädigende Entscheidung trifft oder derartige Befehle erläßt, als erster Opfer eines Angriffs wird. Die gesellschaftliche Entwicklung, das Bewußtsein der Menschheit und der technologische Fortschritt sind in der Lage, dies zu verwirklichen.

Veränderungen in der Natur des Angriffs

Im Agrarzeitalter schuf die Armee, die über genügend Menschen verfügte, um das Land zu schützen, eine Infrastruktur, die die militärische Sicherheit des betreffenden Landes garantierte. Im Zuge der schnellen Entwicklungen im Industriezeitalter konnte die militärische Sicherheit eines Landes nicht allein dadurch garantiert werden, daß das Militär ausrüstungsmäßig auf dem letzten Stand war und über Panzer, Kriegsschiffe, atomare Lenkwaffen usw. verfügte, sondern der Staat mußte auch über bestimmte wirtschaftliche Ressourcen und ein schnelles, umfassendes System der militärischen Mobilmachung verfügen. Im Informationszeitalter sieht sich die militärische Sicherheit mit einer bislang ungekannten Herausforderung konfrontiert.

Der Informationskrieg verfolgt andere Ziele als der traditionelle Krieg. Während es im Krieg des Agrarzeitalters darum ging, die feindliche Armee zu zerstören, war man im

Industriezeitalter bestrebt, nicht nur die feindliche Armee zu zerschlagen, sondern auch das militärische Potential zu vernichten, das es dem Gegner ermöglicht, den Krieg weiterzuführen. Im Informationszeitalter sind die Hauptangriffsziele die Computernetzsysteme des gegnerischen Staates, die die politischen, wirtschaftlichen, militärischen Anlagen und die gesamten gesellschaftlichen Einrichtungen verbinden.

Man bezeichnet den Golfkrieg nicht deswegen als Vorform des Informationskrieges bzw. als Krieg der "Dritten Welle", weil dabei informatisierte Waffen benutzt wurden, sondern weil dabei das militärische Denken einen gewaltigen Wandel durchmachte. Die alliierten Truppen sind bei der Auswahl der Ziele anders als früher vorgegangen und griffen vor allem die gegnerischen Informationssysteme mittels Informationswaffen an.

Im Informationszeitalter verschwimmen nach und nach die Grenzen zwischen Kriegsvorbereitung und Kriegsführung. Bis jetzt mußte jeder Angreifer, der einen Krieg beginnen wollte, bzw. jeder Verteidiger, der eine Invasion abwehren wollte, umfangreiche Vorbereitungen treffen, wozu auch die Erziehung des Volkes, der Aufbau eines umfassenden Mobilisierungssystems, die Festlegung einer Kriegspolitik und eines Kriegsplans, die Entwicklung und Produktion neuer Waffen und die Errichtung einer Kriegsinfrastruktur zählten. Der Kriegsprozeß selbst war bislang ein ununterbrochenes Geschieße und Gemetzel. Vor allem im Industriezeitalter ähnelte ein solcher Krieg in gewisser Weise der Produktion am Fließband. Im Informationskrieg verschmelzen Kriegsvorbereitung und -durchführung. Die nach Hegemonie strebenden Staaten sind praktisch täglich mit Vorbereitungsarbeiten beschäftigt, genauso wie sie jeden Tag Krieg führen. Sie bedienen sich dazu der unterschiedlichsten Methoden: Sie bestechen ausländische Waffenproduzenten, sie verkaufen virusverseuchte Chips an die Länder, die sie unter Kontrolle bekommen wollen oder als potentielle Feinde ansehen; oder sie kaufen Waffenfabriken auf und statten die Waffen mit verseuchter Software aus usw. Diese Art der Kriegsvorbereitung hat in Wirklichkeit die formale militärische Invasion verändert und ist Teil der Kriegsführung selbst geworden. Derartige Entwicklungen legen folgenden Schluß nahe: Im Informationszeitalter besteht die militärische Bedrohung im wesentlichen nicht darin, daß feindliche Truppen die Staatsgrenzen bedrohen oder der Feind ein starkes Heer aufmarschieren läßt, sondern sie rührt von einem plötzlichen Angriff aus dem Netz her: Sie ist ein Angriff auf das "Zentralnervensystem" von Staat und Militär, ein Angriff "von Angesicht zu Angesicht". Ja, es geht sogar so weit, daß man weder weiß, wer der Gegner ist, noch woher die Bedrohung kommt und wann der Krieg tatsächlich begonnen hat.

Politische Sicherheit und Medien

Wenn es um die Sicherheit eines Staates geht, muß man auch die politische Sicherheit berücksichtigen. Die Politik ist die Gesamtheit aller Aktivitäten der verschiedenen Klassen, politischen Parteien und gesellschaftlichen Gruppierungen, deren Ziel es ist, das grundlegende Wohl sicherzustellen, die Staatsgewalt zu organisieren und zu festigen und mittels staatlicher Macht das Land zu regieren. All dies ist ohne Information nicht denkbar. Information stärkt die Kohäsion innerhalb eines Staates und die Macht des Staates, ist aber auch eine Waffe, die die Kohäsion eines Staates untergraben und ein Regime bedrohen kann.

In der Agrargesellschaft mit ihrer unterentwickelten Produktivkraft, in der die einzelnen Teile eines Landes nicht in Kontakt miteinander standen und nur ein geringfügiger Austausch unter den Menschen stattfand, war die Verbreitung von Information im wesentlichen eine Sache von mündlicher Kommunikation und Poststationen. Daher war auch der Informationsfluß vom Schlachtfeld zur Gesellschaft äußerst begrenzt und langsam, was es den staatlichen

Machtorganen erleichterte, Kontrolle auszuüben, sich abzuschotten, Monopole zu bilden und eine in höchstem Maße zentralistische Führung zu etablieren. So konnte ein Regime über eine relativ lange Zeit hinweg Stabilität und Sicherheit aufrechterhalten.

Im Industriezeitalter ist die Lage eine völlig andere. Im Zuge der Entwicklung der Informationsmedien und der Vergrößerung der Informationsmenge und der Beschleunigung des Informationsflusses ist die Zahl jener Menschen, die die Politik beeinflussen können, extrem gewachsen. Dieser Aspekt wirkt sich zwar günstig auf die politische Demokratisierung aus, andererseits nehmen die politischen Konflikte zu, und die politische Unsicherheit steigt dementsprechend. Da die Kommunikationsmedien heutzutage im wesentlichen von der herrschenden Klasse kontrolliert werden, manifestieren sich die von außen und innen kommenden feindlichen umstürzlerischen Aktivitäten in erster Linie in Form eines Ringens um die Herrschaft über die öffentliche Meinung.

In der Informationsgesellschaft wird das gesamte gesellschaftliche, politische und wirtschaftliche Leben in die Computernetzwerke transferiert, was einerseits die politische Transparenz erhöht und das Demokratisierungsniveau steigert, andererseits aber sieht sich die politische Sicherheit einem nie gekannten Druck ausgesetzt. Die Entwicklung einer Informationssymbolwirtschaft führt dazu, daß die Anzahl der Kanäle zwischen den verschiedenen Klassen und gesellschaftlichen Gruppen, zwischen den verschiedenen Regionen und Staaten dramatisch zunimmt.

Die Globalisierung von Mediensystemen schwächt radikal den Einfluß der früheren monomedialen Medien, Publikationen oder Technologien. Infolgedessen wird das Informationsmonopol der staatlichen Gruppen zerschlagen, und die gesellschaftlichen Gruppen und der einzelne Bürger erhalten die Gelegenheit, direkt an den politischen Aktivitäten irgendeines Landes auf der Welt oder des eigenen Landes teilzunehmen. In dieser Dezentralisierung unterliegt die politische Macht einer fast unbemerkten Verschiebung.

Darüber hinaus verwischen sich im Informationszeitalter die Grenzen zwischen staatlicher und internationaler Politik. Die politische Sicherheit eines Staates unterliegt in unterschiedlichem Ausmaß dem Einfluß und Druck der internationalen Politik. Gleichzeitig bietet die rasante Entwicklung der Informationstechnologie den nach Hegemonie strebenden Staaten wirtschaftlichere und praktischere Mittel und Wege, ihre Machtpolitik zu betreiben. Die politische Sicherheit von Dritte-Welt-Staaten sieht sich dadurch mit einer neuen Herausforderung konfrontiert.

Eine Bedrohung des Wirtschaftssektors

Die Politik ist die konzentrierte Manifestation der Wirtschaft, die Wirtschaft ist ihrerseits die Grundlage für die Existenz von Klasse, Nationalität, Staat und politischer Gruppe. Unter dem Motto "Friede und Entwicklung" wurde die wirtschaftliche Sicherheit zur Kernfrage der staatlichen Sicherheit.

In einer autarken Agrargesellschaft war die Wirtschaft einer Gesellschaft im wesentlichen in sich geschlossen und unabhängig. Außer klimatischen gab es kaum äußere Einflüsse auf die wirtschaftliche Sicherheit. Im Industriezeitalter kam es zu einer intensivierten Produktion im großen Maßstab und zu einer sehr genauen sozialen Arbeitsteilung. Mit den Handelsgütern hat sich dann schließlich und endlich das bis zu diesem Zeitpunkt verschlossene Tor der Staaten geöffnet, und die zwischenstaatlichen wirtschaftlichen Beziehungen wurden immer enger. Für ein Auto wird unter Umständen der Plan in Amerika gezeichnet, in Europa wird

vielleicht die Karosserie hergestellt, während Asien den Motor beisteuert und das Ganze in Afrika zusammengebaut und dann auf den Markt gebracht wird. Einerseits wird dadurch die Zusammenarbeit gefördert, andererseits ist die wirtschaftliche Sicherheit der einzelnen Staaten einer gewissen Bedrohung ausgesetzt.

In der Informationsgesellschaft sieht sich die wirtschaftliche Sicherheit der einzelnen Staaten einer noch größeren Herausforderung gegenüber. Die entwickelten Länder befinden sich bereits mitten in der Informationsgesellschaft bzw. in der postindustriellen oder Prä-Informationsgesellschaft. Im wirtschaftlichen Wettbewerb gilt die Regel, daß "hohes Geopotential das niedrige entmachtet". Es ist daher eine historische Pflicht, die kurz- und langfristige wirtschaftliche Sicherheit eines Staates grundlegend zu gewährleisten, indem der betreffende Staat schnell und zügig Produktionsstrukturen schafft, deren Rückgrat die Informationsindustrie bildet.

Die Integration und gleichzeitige Regionalisierung der Weltwirtschaft führt zu einer extremen Abhängigkeit und Fragilität der Wirtschaft der einzelnen Staaten. Im erbitterten Wettkampf der Informationsindustrie können sich auch innerhalb der entwickelten Staaten beträchtliche Unterschiede auf technologischem Gebiet auftun, wodurch die gegenseitige Abhängigkeit noch verstärkt wird. Diese Interdependenz der staatlichen Wirtschaften bedeutet eine Bedrohung der Wirtschaft der einzelnen Staaten. Je größer die Abhängigkeit, desto größer die Bedrohung. In der Informationsgesellschaft führen Computerisierung und Telekommunikation dazu, daß bislang getrennte Sektoren wie Finanzen, Markt, Waren, Technik, Arbeit, Industrieanlagen, Dienstleistungen, Freizeit und Produktion zu einem Ganzen verschmelzen. Vom heutigen Stand der Technik aus gesehen, sind diese informatisierten Netzwerke äußerst empfindlich und können leicht von Hackern angegriffen werden. Wenn ein gegnerischer Staat organisierte, gezielt kriminelle Handlungen im Netz setzt, dann kann das im betroffenen Staat zum Zusammenbruch der Wirtschaft führen. Dieses Szenario ist keineswegs aus der Luft gegriffen. Es ist bekannt, daß es bereits heute Staaten gibt, die an der Entwicklung sogenannter Superviren und elektromagnetischer Impulse arbeiten, die zum gewünschten Zeitpunkt Systeme wie Banken, Börsen, Luftverkehr, Telefon, Fernsehen, Kraftwerke, Stromversorgung usw. angreifen und zur Lähmung der Wirtschaft eines Staates führen können. Die Frage der "wirtschaftlichen Sicherheit" eines Landes umfaßt die verschiedensten Gefahren von außen oder von innen, denen das Wirtschaftssystem ausgesetzt ist, ja, diese Gefahren können sogar aus dem Wirtschaftssystem selbst herrühren.

Kulturelle und ökologische Aggression

Auf das engste mit der politischen und wirtschaftlichen Sicherheit verbunden ist die soziale Sicherheit.

Die Kultur ist der "Klebstoff" der Gesellschaft, die Basis, die die soziale Stabilität gewährleistet. Die vom Menschen geschaffene Kultur durchdringt sämtliche Bereiche des sozialen Lebens, bringt soziale Normen und soziale Systeme hervor. Die Menschen einer bestimmten Zeit und eines bestimmten Volkes leben alle in einem bestimmten kulturellen Modell.

Die Entwicklung der Informationstechnologien und der Medien beschleunigt die Verbreitung von kulturellen Vorstellungen und die gegenseitige kulturelle Absorption und Verschmelzung. Gleichzeitig gibt es aber auch Menschen, die die moderne Netzwerktechnologie nutzen, um z. B. eine "pornographische Kultur" zu verbreiten. Dies stellt zweifellos einen Angriff auf die moralischen und kulturellen Normen und

Wertvorstellungen der traditionellen Kultur dar. Das Chaos auf kultureller Ebene kann letzten Endes auch die soziale Sicherheit beeinträchtigen. Im Übergang zur Informationsgesellschaft kann ein Land auch soziale Erschütterungen durchmachen, wobei derartige Erschütterungen in Entwicklungsländern noch größere Ausmaße annehmen können. Aber egal, ob die Produktivität eines Landes noch auf der Ebene der Agrargesellschaft oder der Industriegesellschaft steht — im Informationszeitalter kann kein Land sich in stiller Abgeschlossenheit weiterentwickeln. Nur in einer Atmosphäre der Öffnung nach außen hat ein Land eine Überlebenschance.

Nach der Theorie von der Selbstorganisation von Systemen, die sich nicht im Gleichgewicht befinden, muß sich ein in Entwicklung befindliches System, wenn es sich im stabilen Stadium des quantitativen Wandels befindet, notwendigerweise in der kontrollierenden Position befinden; wenn sich das System jedoch dem kritischen Punkt des qualitativen Wandels annähert, dann befindet es sich zufälligerweise in der kontrollierenden Position. Das heißt: Je tiefer eine Reform geht, desto zahlreicher sind die Zufallsfaktoren.

Im Informationszeitalter häuft sich Reichtum schneller an als im Industriezeitalter, wodurch die Kluft zwischen arm und reich sich stetig vergrößert und die soziale Sicherheit gefährdet.

Wenn man von sozialer Sicherheit spricht, so darf man auch die Ökologieproblematik nicht unterschätzen.

Mit der Informationsgesellschaft sind nicht nur die durch eine Industriegesellschaft verursachten Verschmutzungen und Bedrohungen nicht gewichen, ganz im Gegenteil: Es kommen neue Verschmutzungsquellen dazu, denn die Entwicklung der Informationstechnologien bringt neue Formen der Umweltverschmutzung mit sich — etwa die Verseuchung mit elektromagnetischer Strahlung. Jene westlichen Länder, die ein hohes Industrieniveau erreicht haben und in denen sich die Informationsindustrie rasch entwickelt, haben aufgrund notwendiger Umstrukturierungsmaßnahmen Industriezweige mit hohem Verschmutzungspotential aus dem eigenen Land in die Entwicklungsländer verlagert und dadurch schwere Umweltschäden in diesen Ländern verursacht. Die harten Fakten der wirtschaftlichen Entwicklung lassen uns schon sehr genau spüren, daß die Entwicklung eines Staates und die ökologische Sicherheit aufs engste miteinander verknüpft sind. Sicherheit ist die Garantie für Entwicklung, aber Entwicklung liefert ihrerseits die Bedingungen für Sicherheit. Mit der wissenschaftlich-technischen Entwicklung und dem Beginn des Informationszeitalters wird die ökologische Unversehrtheit zu einem Kernpunkt für die soziale, ja, die nationale Sicherheit.

Der Krieg des Geistes

Jeder Krieg hat seinen Ursprung im Geist. Diejenigen, die Kriege planen und Befehle geben, und die, die sie in die Praxis umsetzen, sind allesamt nur Erdbewohner, die unter der Kontrolle der Denkprozesse im menschlichen Gehirn stehen. Vergangene und zukünftige Kriege entspringen alle dem Geist des Menschen. Wenn wir Kriege eindämmen und abschaffen wollen, dann müssen wir einerseits eine Antwort in der objektiven Welt suchen, andererseits müssen wir auch die Ursache in subjektiven menschlichen Faktoren suchen, d. h. wir müssen zuallererst die Ursachen eines Krieges im Denken erforschen und ausmerzen.

Das Gehirn des Menschen macht den Krieg — egal, ob bewußt oder unbewußt, egal, ob aus eigener Initiative oder nicht, egal, ob aktiv oder passiv, aber immer nach einem heftigen Kampf — dem Krieg des Denkens im Gehirn. Zum Krieg des Denkens gehört sowohl der

Krieg im Inneren eines individuellen Gehirns als auch der Kampf zwischen verschiedenen Gehirnen. Die Grundeinheit im Krieg des Denkens ist: Menschliches Gehirn + äußeres Gehirn (Gedankenspeicher) + elektronisches Gehirn (Computer).

Wenn man davon ausgeht, daß der umfassende Informationskrieg die höchste Stufe des Informationskrieges darstellt, dann ist der Krieg des Denkens die niedrigste Stufe des Informationskrieges und gleichzeitig auch die kleinste Einheit in der Struktur des Informationskrieges. Jeder Informationskrieg setzt sich aus unzähligen größeren und kleineren Kriegen des Denkens zusammen.

Ein zukünftiger Weltkrieg — der totale Informationskrieg — beginnt zuallererst mit einem Krieg des Denkens. Die Dauer eines derartigen Krieges, wer gewinnt, wer verliert — dies alles hängt davon ab, wie hoch der Sieg bzw. wie vernichtend die Niederlage im Krieg des Denkens sind.

Bei einem zukünftigen Krieg ist die erbittertste, interessanteste und entscheidendste Phase die des Krieges des Denkens. Könnte man den Krieg auf diese Domäne beschränken, so könnten die Kriegsparteien bereits hier entscheiden, wer gewinnt und wer verliert.

Wird Krieg jemals aussterben? Die Antwort heißt nein. Da Umfang und Inhalt des Begriffs "Krieg" sich unablässig wandeln, wird der Krieg ein ständiger Begleiter der Menschheit bleiben. Solange die Menschen denken, solange sie einen Geist besitzen, so lange wird der Krieg nicht aussterben. Natürlich werden sich Inhalt und Form ständig wandeln, und die traditionellen Kriegsformen werden ständig durch neue ersetzt werden, so wie der mechanisierte Krieg vom Informationskrieg abgelöst wird, wobei die Halbwertszeit auch hier immer kürzer wird.

Das 21. Jahrhundert wird das Jahrhundert sein, in dem der Krieg des Denkens, der "Geistkrieg", voll zum Tragen kommen wird.

Firewall und Information Frontier

Alles, was mit Information zu tun hat, ist eine äußerst lebendige, kraftvolle Domäne. Die Regionalisierung der Wirtschaft und das gleichzeitige schnelle Voranschreiten der Globalisierung bedingen eine rapide Zunahme der Informationsmenge. Täglich werden weltweit an die zehn Milliarden Informationseinheiten übermittelt, die jährliche "Informationsproduktion" beträgt ungefähr 72 Milliarden Einheiten. Und jedes Jahr steigt sie um 15 bis 20 Prozent.

Aus dem Blickwinkel der nationalen Sicherheit gesehen, verblaßt mit der weltweiten Verbreitung von Netzwerken allmählich das Konzept der Nationalgrenzen. Diese Aufhebung der Grenzen hat direkt Auswirkungen auf die nationale "Kommunikations-" bzw. "Informationssouveränität" sowie auf die Geheimhaltung von Staatsgeheimnissen. Das Internet — jenes weltumspannende Netzwerk, das den größten Einfluß hat, die größte Anzahl an Usern verzeichnet und über die reichsten Inhalte verfügt — ist ein neuer Kontinent, der weder Grenzen noch Verträge kennt; es ist eine Welt, die erst langsam Gestalt annimmt und deren endgültige Form noch nicht feststeht. Auf diesem unbekannten Gebiet ist der Informationskrieg noch etwas ganz Neues, das sich zwar schnell entwickelt, aber noch nicht in allen Einzelheiten definiert ist. Im Informationszeitalter zielt der Krieg in erster Linie auf die Computernetzwerke eines Landes ab, die Politik, Wirtschaft, Militär und andere gesellschaftliche Bereich miteinander verbinden, die dank der neuen Technologien auf vielen

Kanälen gleichzeitig und auf unterschiedlichste Weise schnell und unsichtbar angegriffen werden können; der Gegner wird "kampflos besiegt". Wenn man also traditionelle Theorien, die auf einen Raum, der Form hat, abgestimmt sind, hernimmt, um das "Territorium der Information" und die "Information Frontier" zu definieren, so wird man auf viele vage Fragen stoßen, denn es bedarf einer neuen Form des Denkens, einer neuen Theorie, eines neuen Blickwinkels, um die Bedeutung des Begriffs der Information Frontier annähernd wissenschaftlich zu definieren.

Ich bin der Meinung, daß die Information Frontier eine formlose, ungeregelte, die "Informationsterritorien" der einzelnen Staaten oder politischen Gruppierungen voneinander trennende Grenze ist. Ein "Informationsterritorium" kann nicht nach traditionellen geopolitischen Konzepten wie Hoheitsgebiet, Luftraum, Territorialgewässer, ja, sogar "Weltraumterritorien" unterteilt werden, sondern nur nach dem unter politischem Einfluß stehenden "Informationsstrahlungsraum". Die Grenzen des Informationsterritoriums, die Sicherheit der Information Frontier betreffen das Gedeihen eines Volkes, eines Staates im Informationszeitalter. Die einzelnen Staaten der Erde sind alle miteinander dabei, sich ihr Informationsterritorium zu erschließen und diese unsichtbare Grenze zu schützen. Es ist also gerade ein erbitterter Kampf um die Vorherrschaft auf dem Territorium der Information im Gange. Die zukünftige Stärke der Wirtschaft eines Staates hängt davon ab, ob er sich dieses Territorium erschließen und die Sicherheit der Grenzen wahren kann.

Die Welt ist gerade dabei, sich in eine Welt des "Netzkapitalismus" zu verwandeln — siehe Liberalisierung des Marktes im Internet —, wodurch der Schutz der Grenzen des Informationsterritoriums zu einer Sache der nationalen Sicherheit wird.

Von der Grenze des Nationalstaates zur "Grenze der fünften Dimension"

Das Informationsterritorium ist ein unvermeidliches Produkt der Informationsgesellschaft, die "Information Frontier" ist das Resultat des Wandels in der Kriegsform und -entwicklung.

Zusätzlich zu den vier Räumen des Krieges — Land, Luft, See und Weltraum — tut sich nun mit dem Informationskrieg als neue Form des Krieges eine fünfte Dimension auf. Da aber der Krieg der vier Dimensionen gegenüber dem Krieg, der aus der fünften Dimension kommt, offen ist, sind wir gezwungen, die Form dieses neuen Kriegsschauplatzes, dieses neuen Territoriums zu erforschen und die Bedeutung des Begriffs "Frontier" zu hinterfragen.

Die Geschichte des Krieges hat immer wieder gezeigt, daß bei jeder Entwicklung einer neuen Kriegsform ein neuer Kriesgsraum erschlossen wurde, und die Entstehung einer neuen Kriegsdimension hat immer auch zur Entstehung einer Grenze für diese neue Dimension geführt. Die Dimension des Krieges bedingt die Dimensionalität des Territoriums eines Staates. Die Fähigkeit eines Staates, in einer Kriegsdimension Widerstand zu leisten, bestimmt den Grad der Sicherheit der dieser Dimension entsprechenden Grenze. Fehlt die Fähigkeit, im Krieg in einer bestimmten Dimension Widerstand zu leisten, so führt das in Wirklichkeit zum Verlust der entsprechenden Grenze, ja, sogar zum Verlust der entsprechenden Verteidigungsfähigkeit. Die Vorherrschaft in einer hohen Dimension bestimmt die mehrdimensionale Sicherheit, und die Sicherheit der hochdimensionalen Territorien entscheidet über die Sicherheit der nieder- oder mehrdimensionalen Territorien.

Verteidigungsmaßnahmen — wo und wie? Der Aufbau einer starken geistigen Verteidigungslinie

In der informatisierten Gesellschaft drohen wir alle — egal ob Individuum, Staat oder politische Gruppierung — im Meer der Information zu versinken. Und wenn wir die Kunst des "Schwimmens" nicht beherrschen, werden wir darin ertrinken. Es reicht nicht, den Raum zu erschließen, in dem Information gewonnen wird, und die eigenen Informationen zu verbreiten, sondern man muß Maßnahmen treffen, um die erworbene Information aussieben und ordnen zu können, um schädliche bzw. unerwünschte Information aussortieren und zurückweisen zu können, um die eigene Informationssicherheit zu wahren und die nützliche Information mit höchster Effizienz zu nutzen.

Auch auf dem Gefechtsfeld wird Information zur wichtigsten Waffe, und da der Angriff letzten Endes dem Wissen und Vertrauen gilt, wird der Gegner dazu gebracht, seinen Widerstand aufzugeben. Die geistige Verteidigungslinie ist die erste, die in Mitleidenschaft gezogen wird, sie ist erstes Ziel eines Angriffs. Deswegen muß jeder — der Staat genauso wie der einzelne Bürger — von sich aus eine unsichtbare "geistige Verteidigungslinie" errichten. Der Staat hat die Aufgabe, Gesetze und moralische Normen, die dieses Informationsterritorium regeln, zu entwickeln und durch positive Beeinflussung der öffentlichen Meinung die geistige Kultur des Landes zu fördern und die Unabhängigkeit des Staates sowie die kulturelle Eigenständigkeit zu erhalten. Der einzelne Bürger hingegen sollte lernen, Information selektiv aufzunehmen und sich gegen schädliche Informationsangriffe zur Wehr zu setzen.

Errichtung einer wirksamen Net Frontier

Mit der hochgradigen Vernetzung der Gesellschaft werden auch die Schwächen des Netzes sichtbar. Diejenigen Länder, die bei der Netztechnologie einen Schritt voraus sind und voll auf Vernetzung setzen, weiten ihre Information Frontier auf andere Länder aus und stellen dadurch eine Bedrohung der "Informationshoheit" anderer Länder dar. Andererseits gibt es wieder Fälle von "Netzsabotage" — siehe Hacker, die illegal in Netze eindringen —, was im schlimmsten Fall die Zerstörung der verschiedenen Netzwerke bedeutet. In einigen Ländern wird zur Zeit versucht, in theoretischer Forschung und mittels Simulationen den "NetWar" zu erforschen. Da die Entwicklung dahin geht, daß immer mehr Information über Netzwerke transportiert wird, werden in Zukunft auch Wettbewerbskonflikte im Netz ausgetragen werden, und Konflikte im Bereich der nationalen Sicherheit werden sich nicht nur in Form eines Informationskriegs innerhalb des militärischen Bereichs, sondern in Form eines allgemeinen Konflikts im Netz manifestieren, der sämtliche gesellschaftlichen Bereiche — Politik, Wirtschaft, Diplomatie, Wissenschaft und Technik, Kultur, Bildung und Ideologie — umfaßt. Konflikte im Bereich der Information und an der Information Frontier sind damit vorprogrammiert.

Konflikte an der "Net Frontier" werden sich dank netzbasierter Täuschung in Zukunft in Form von Störung, Bedrohung und Zerstörung des Feindes manifestieren. Man wird versuchen, mit unterschiedlichsten Mitteln in das gegnerische Netz einzudringen und Information zu "erbeuten"; andererseits wird man bestrebt sein, mittels Täuschung und anderer Maßnahmen zu verhindern, daß der Gegner ins eigene Netz eindringen kann. Über das Netz werden einschüchternde Informationen verbreitet, die ebenfalls einen gegnerischen Angriff unterbinden sollen. Durch all diese Maßnahmen soll die Net Frontier des Gegners angegriffen und zerstört werden und ein Angriff seinerseits unmöglich gemacht werden.

Staaten mit entwickelter Informationstechnologie haben in diesen Bereichen bereits erfolgreiche Arbeit geleistet. Im Politischen sind sie davon abgekommen, ausschließlich Wert auf die Leistung von Computern und -netzwerken zu legen, und haben sich Fragen der

Sicherheit, Unversehrtheit, Userfreundlichkeit, Präzision und Kontinuität zugewandt. Viele westliche Länder haben allein oder gemeinsam Regeln und Normen festgelegt, die langfristig die Sicherheit im Netz steigern sollen, und haben große Summen in die Entwicklung von neuen Technologien zum Schutz des Netzes gesteckt, z. B. in Antivirentechnologien, Technologien, die das "Aussickern" von Information verhindern sollen, und andere Security-Technologien. Aber trotz allem warnen westliche Spezialisten vor enormen Schwachstellen in den Netzwerken. Es wäre wichtig, parallel zur Entwicklung von Computernetzwerken auch die Errichtung einer Net Frontier zu überlegen. Einerseits sollten wir die weltumspannenden Netzwerke wirksam und in ihrer ganzen Fülle nutzen und dementsprechende positive Informationen ins Netz stellen. Darüber hinaus sollten wir unseren eigenen Informationsraum errichten und den Einfluß der eigenen Information stärken. Wenn aber andererseits eine wirksame Net Frontier errichtet werden soll, dann müssen auch jene Backbone-Informationsnetzwerke, die direkt die politische, wirtschaftliche und militärische Sicherheit eines Staates betreffen, einer einheitlichen staatlichen Regelung unterliegen, einheitlich aufgebaut sein und nach Möglichkeit in einem gewissen Umfang Local Area Networks bilden. Dadurch könnte verhindert werden, daß aus Gründen der leichteren Benutzbarkeit die Sicherheit des Netzes sinkt. Was die anderen Netzwerke betrifft, so muß man auch hier geeignete Maßnahmen treffen, wie z. B. die Installation von Firewalls, "Schutzsperren" oder Plattformen, die die Information vorselektieren, um so die Verbreitung staatsschädigender Information zu verhindern und einen gegen das eigene Land gerichteten Angriff abzuwehren. Außerdem müssen auch bei anderen mit Computern ausgestatteten Netzen (Strom-, Telefon-, Fernsehnetz usw.) dementsprechende Vorkehrungen getroffen werden.

Aufstellung einer Informationsschutztruppe

Als es Hoheitsgewässer gab, wurden Marinetruppen aufgebaut; als es den Luftraum gab, wurden die Luftstreitkräfte aufgebaut; und auch der Aufbau von Weltraumstreitkräften wird zumindest theoretisch in Erwägung gezogen. Wenn man eine Informationsdimension, eine Informationsgrenze errichtet, dann bedarf es auch einer dementsprechenden Informationsschutztruppe, d. h. einer sich von den traditionellen Truppen vollkommen unterscheidende spezialisierte, wissens- und technologieintensive Truppe, die sich aus Wissenschaftlern, Informationsspezialisten und Militärs, also aus Spezialisten für den Informationskrieg, zusammensetzt. Ihre Hauptaufgabe besteht darin, die Sicherheit der Informationsgrenze zu gewährleisten, auf den eigenen Informationsraum abzielende Angriffe seitens anderer Staaten, politischer Gruppierungen oder Einzelpersonen abzuwehren und diesbezügliche kriminelle Handlungen aus dem eigenen Land zu verhindern. Sie leistet also einem unsichtbaren Gegner im Raum der Information informationellen Widerstand. Sie ist auch dasjenige Sonderkommando, das den Informationskrieg führt, sie ist die Elitetruppe, die einen Informationsangriff abwehrt und bei einem Informationszwischenfall in Aktion tritt. Eine derartige Informationsschutztruppe wäre ein deutliches Symbol für die Errichtung einer dem Informationszeitalter angemessenen Streitkraft. Je rückständiger ein Staat punkto Informationstechnologie ist, desto mehr sollte er an die Errichtung einer Informationsschutztruppe denken, um den Informationsschutz und damit die gesamte Sicherheit des Staates zu garantieren.

Unsere Überlegenheit wiedererlangen

Eine digitalisierte Truppe zu schaffen und einen Informationskrieg zu führen — all das scheint für uns noch in weiter Ferne zu sein, aber die theoretischen Vorbereitungen sind bereits weit gediehen.

Bei all den sprunghaften Entwicklungen, die die Streitkräfte durchmachen, hat nicht unbedingt jenes Land, das einen technologischen Vorsprung aufweist, auch die tatsächliche Vormachtstellung inne, sondern jenes, das einen Vorsprung im Denken aufweist. Dies bietet sowohl eine Chance als auch eine Herausforderung; wem es gelingt, die Chance zu nutzen, der kann auch die Herausforderung annehmen. Wenn wir Überlegenheit erlangen wollen, müssen wir die gewohnte Vorstellung über Bord werfen, daß zuerst die Technologie, danach die Strategie und an letzter Stelle die Theorie kommt. Damit die Theorie auch wirklich eine Vorläuferrolle einnehmen kann, muß sie ihrer Zeit voraus sein. Der Sieg in einem zukünftigen Krieg hängt von den Anstrengungen ab, die wir heute aufbringen; um eine Vormachtposition einnehmen zu können, müssen wir uns einem neuen Lernen zuwenden. "Wissen ist Macht" — im Informationskrieg gewinnt dieser Slogan eine vollkommen neue Bedeutung.

Wissen und Information sind unsere Waffen. Der Unterschied zwischen diesen immateriellen Waffen und den traditionellen, materiellen Waffen liegt darin, daß jene leichter zu verbreiten sind, daß niemand ein Monopol darauf hat, daß jeder daran teilhaben kann. Wenn der andere darüber verfügt, dann kann auch ich sehr schnell darüber verfügen und sie mir zu eigen machen und anwenden. Außerdem ist es wesentlich kostengünstiger, Wissen einzusetzen, als moderne Waffensysteme zu erwerben. Abgesehen davon ist auch der Einsatz moderner Waffensysteme nur dann möglich, wenn das Bedienungspersonal über adäquates Wissen verfügt. Das herkömmliche Militär muß die Einschränkungen, die die Macht der Gewohnheit mit sich bringt, durchbrechen, es muß seine althergebrachten Vorstellungen über Bord werfen und sich neues Wissen aneignen, denn nur dann wird es ihm möglich sein, es mit dieser neuen Herausforderung aufnehmen zu können. Findet dieser Erneuerungsprozeß nicht statt, kann es sich den neuen Gegebenheiten nicht anpassen. Da diese Veränderungen zuallererst im Menschen stattfinden, muß man also zuerst den Menschen "transformieren".

Der Informationskrieg ist ein Produkt der Revolution im militärischen Bereich, und er wird mit Sicherheit alte Militärtheorien, alte Methoden der Kriegsführung und alte organisatorische Strukturen in Frage stellen. Nach dem in der Geschichte wirksamen Gesetz der "Verneinung der Verneinung" wird der Informationskrieg in erster Linie den für die Industriegesellschaft charakteristischen mechanisierten Krieg verneinen. Umgekehrt wird er unter Umständen einiges von der Kriegskunst der Agrargesellschaft übernehmen können. Wir können davon ausgehen, daß die "Kunst des Krieges" eines Sunzi oder die Strategien eines Guerillakrieges, so sie sich mit der Technologie dieses neuen Zeitalters verbinden, ein unabsehbares Potential entfalten werden. Unsere vorrangige Aufgabe besteht daher darin, diese beiden Ansätze zu vereinen.

Technologie kann nicht ohne Theorie auskommen, und Theorie ist nicht losgelöst von Technologie zu sehen. Ein wesentliches Prinzip des Informationskrieges ist das "Differentialprinzip". Stehen sich in einem Krieg eine informatisierte Truppe und eine nicht-informatisierte Truppe gegenüber, so wird im allgemeinen erstere überlegen sein, wobei es auf dem Kriegsschauplatz unter Umständen zu einer einseitigen Transparenz kommt. Um hier eine Veränderung herbeizuführen, darf man sich nicht allein auf strategisches Denken oder den Einsatz von Stratagemen verlassen. Die Kommandierenden müssen über ein technisches Verständnis verfügen und von sich aus die Zusammenarbeit mit Technikspezialisten suchen, um ihr strategisches Denken zu "technologisieren". Selbst auf technologischem Gebiet kann nicht eine Seite allein die Vormachtstellung innehaben, und auch wenn dies der Fall wäre, stünde sie nicht ein für alle Male fest. Sowohl Überlegenheit als auch Unterlegenheit sind relativ, keine Seite kann vollkommene Überlegenheit bzw. vollkommene Unterlegenheit innehaben. Es ist eine Illusion zu glauben, den starken Kräften des Gegners aus dem Weg

gehen und nur seine Schwachpunkte angreifen zu können. Genauso wenig kann man sich nur auf die eigenen Stärken konzentrieren und die eigenen Schwächen ignorieren.

Die Geschichte zeigt uns, daß sich neue Technologien einerseits positiv auf den Menschen auswirken können, andererseits aber auch ihre Schattenseiten haben. Die neuesten Computer- und Informationstechnologien sorgen dafür, daß Gesellschaft und Militär immer stärker vernetzt und integriert werden und dadurch eine extrem hohe Leistungsfähigkeit erreichen. Andererseits weisen eine hochgradig vernetzte Gesellschaft und Armee auch beträchtliche Schwächen auf. Deswegen muß mit der Vernetzung und Digitalisierung eine neue Ordnung etabliert werden. Der Informationskrieg durchbricht die Ordnung des mechanisierten Krieges und bedarf daher selbst einer neuen technologischen Ordnung. Im Falle von Konflikten wären diese dann wesentlich leichter beizulegen. Unsere Forschungen auf dem Gebiet der Kriegsführung, der technologischen Verbesserung sollten an diesem Punkt ansetzen; wir sollten nicht andere imitieren und dabei unsere eigenen Fähigkeiten außer acht lassen.

Um Überlegenheit zu erlangen und diese zur Geltung zu bringen, müssen wir besonderes Augenmerk auf die Entwicklung einer militärischen "Soft Science" legen. Ein Informationskrieg ist ein "sanfter" Angriff, eine sanfte Verletzung und braucht die "Soft Science" als Basis und auch als Garantie.

Die militärische Soft Science beschäftigt sich mit Militärtheorie, Strategie, Planung und Organisation. Die Forschung in diesem Bereich umfaßt die verschiedensten Waffengattungen, ist abteilungs- und fächerübergreifend. Der Informationskrieg ist nicht nur ein Virenkrieg, ein elektronischer oder ein psychologischer Krieg, ein Abschreckungskrieg oder ein Politpropagandakrieg. Er umfaßt einen viel weiteren Bereich und kann mit keiner der früheren Varianten von Krieg verglichen werden. Er bedarf daher nicht nur der herkömmlichen "harten" Technologien, sondern viel mehr einer Garantie durch die "sanften" Technologien.