George J. Stein/USAF
InfoWar: Worte zählen

Die hier veröffentlichten Ansichten sind jene des Autors und geben nicht die offiziellen Standpunkte der US-Regierung, des Department of Defense, der US Air Force oder des Air War College wieder.

Einleitung

Die terminologische Grundlage für eine Diskussion über den InfoWar findet man eher in der "wirklichen Welt" als in philosophischen, linguistischen oder etymologischen Spekulationen. So interessant philosophische Betrachtungen auch sein mögen, es läßt sich nicht leugnen, daß "Krieg" — und somit auch der InfoWar — in erster Linie eine vom Staat unter Zuhilfenahme seiner Streitkräfte ausgeführte Aktion ist. Selbstverständlich könnte man "Hacken" und andere "Cyber"-Aktivitäten von Jugendlichen oder kriminellen Organisationen, die sich gegen Privatpersonen, Banken oder öffentliche Versorgungsbetriebe richten, als eine Art "InfoWar" sehen, doch im Rahmen dieser Abhandlung werden sie als "kriminell" eingestuft. In diesem Aufsatz wird der InfoWar als staatliche Aktivität verstanden, die zum größten Teil von den Streitkräften ausgeführt wird. Natürlich wären auch der Geheimdienst oder andere Dienste der Staatssicherheit dazu imstande. Behält Clausewitz recht und "Krieg ist die Fortsetzung der [Staats]Politik mit anderen Mitteln", dann stellt der InfoWar ein weiteres "Mittel" dar, die Ziele der Staatspolitik zu verfolgen.

Die momentane Aufmerksamkeit, die dem InfoWar zuteil wird, ist die Folge der vom US-Militär ziemlich öffentlich geführten Diskussion zu diesem Thema. Diese Abhandlung möchte die Evolution des InfoWar-Konzepts in offiziellen und halboffiziellen Dokumenten der US-Streitkräfte darstellen. Besondere Aufmerksamkeit wird dabei den aktuellen Konzepten der US Air Force gewidmet, da diese die interessantesten Gedanken entwickelt haben, wie es sich für die Teilstreitkräfte geziemt, die die meiste Verantwortung für "strategische" Kriegsführung tragen. Die berücksichtigten Dokumente fallen generell unter die Kategorie "Doktrin". Für die US-Streitkräfte — eigentlich für jede moderne militärische Einrichtung — bestimmt eine Doktrin nicht nur, "wie" sie kämpfen oder andere Operationen wie etwa Hilfseinsätze ausführen, sondern in noch stärkerem Maße, wie die Streitkräfte "organisiert, ausgebildet und ausgerüstet" werden, um ihre Missionen auszuführen. Innerhalb der US-Streitkräfte werden Doktrinen in solche für die einzelnen Teilstreitkräfte und sogenannte "gemeinsame" Doktrinen unterteilt. Jede der Teilstreitkräfte hat ihre eigene Doktrin. Wie die Armee, die Marine und das US Marine Corps und die Luftwaffe in den Kampf ziehen und organisiert, ausgebildet und ausgerüstet werden, hängt von den typischen Eigenheiten des primären Operationsgebiets (Land, See oder Luftraum) ab.

In den USA wird jede der Teilstreitkräfte so organisiert, ausgebildet und ausgerüstet, daß sie den im Ausland stationierten Generalstabschefs — etwa dem Europäischen Kommando (EUCOM) oder dem Pazifischen Kommando (PACOM) — als Truppen zur Verfügung stehen. Die Teilstreitkräfte werden zwar als solche eingesetzt, aber sie "kämpfen gemeinsam" unter einem "Kommandanten der vereinten Streitkräfte", der Kommando und Kontrolle über jede einzelne der Teilstreitkräfte hat. Das heißt, die Army, Navy oder Air Force ziehen nicht los und führen ihren jeweils eigenen Krieg. Da die Fähigkeit, gemeinsame Operationen ausführen zu können, für die US-Streitkräfte im Mittelpunkt steht, entwickelte sich in den letzten Jahren die "gemeinsame" Doktrin. Was noch wichtiger ist: Eine gemeinsame Doktrin ist für die US-Streitkräfte verbindlich und hat Priorität vor einer Doktrin der Teilstreitkräfte. Im Kontext des InfoWar liefert somit die Betrachtung der "offiziellen" gemeinsamen Doktrin die exakteste terminologische Grundlage für jede Diskussion oder Analyse der "wirklichen

Welt". Wenn also "[Info]War die Fortsetzung von Politik mit anderen Mitteln" ist, so bildet die InfoWar-Doktrin der US-Streitkräfte die notwendige, wenn auch nicht ausreichende, terminologische Grundlage für Diskussionen zum Thema InfoWar.

Die Evolution der InfoWar-Terminologie

Die erste offizielle und öffentliche Erwähnung durch die US-Streitkräfte dürfte im Memorandum of Policy No. 30 (1993): Command and Control Warfare erfolgt sein. Command and Control Warfare (C2W)[1] wurde definiert als "die (Hervorhebung durch den Verfasser) militärische Strategie, die den InfoWar auf dem Schlachtfeld (Hervorhebung durch den Verfasser) einführt und die physische Zerstörung mit einschließt. Ihr Ziel ist es, die feindlichen Kommandostrukturen vom Truppenkörper abzuschneiden." MOP 30 verweist den Leser zur Erläuterung von InfoWar auf ein älteres (noch immer klassifiziertes) Dokument: DOD (Department of Defense) TS (Top Secret) 3600.1 — Information Warfare — 1992. Die drei Kernpunkte: (1) daß InfoWar und C2W als gegenseitig relevante Konzepte angesehen werden; (2) daß es sich dabei um eine sehr von der Army (den Landstreitkräften) geprägte Sichtweise der Kriegsführung handelt; und (3) daß die jüngsten Erfahrungen aus dem Golfkrieg als das Wesentliche von C2W angesehen werden. Ich möchte General Colin Powells Bemerkung zum Sieg über die irakische Armee in Erinnerung rufen: "Zuerst haben wir ihr den Kopf abgeschnitten, dann haben wir sie getötet."

Die Ausarbeitung einer gemeinsamen Doktrin der US-Streitkräfte ist recht komplex. Kurz gesagt, wird dabei eine der Teilstreitkräfte als "Führungskraft" bestimmt, die den ersten Entwurf ausarbeitet und die Anmerkungen, Zustimmung und Ablehnung, alternativen Sichtweisen etc. der anderen Teilstreitkräfte durch das Joint Doctrine Center koordiniert. Der Gedanke dahinter ist, zumindest theoretisch zu vermeiden, daß eine gemeinsame Doktrin nur die Sichtweise einer der Teilstreitkräfte widerspiegelt. Idealerweise bedeutet eine gemeinsame Doktrin einen Konsens. Als die verschiedenen Entwürfe der gemeinsamen Doktrin für C2W in den Teilstreitkräften die Runde machten, wurde die ursprüngliche Sichtweise (siehe oben) als zu eng gefaßt angesehen. Ebenso war es ziemlich unsinnig, C2W in einem Umfeld zu erörtern, in dem die Definition des Ausgangskonzepts InfoWar noch streng geheim war. Endlich, nach vielen Entwürfen, entstand 1995 aus den Debatten und Diskussionen die Joint Publication 3—13.1 — Joint Doctrine for Command and Control Warfare. Die JP 3—13.1 ist somit eine verbindliche terminologische Grundlage für die Erörterung von InfoWar innerhalb der US-Streitkräfte — bis das "Basisdokument" JP 3—13 Information Operations (noch im Entwurfsstadium) verabschiedet wird.[2]

Der bedeutendste Schritt von MOP 30 zu JP 3—13.1 ist die Erkenntnis, daß C2W eine "Anwendung von InfoWar im Rahmen militärischer Operationen (Hervorhebung durch den Verfasser)" ist. C2W findet "in allen Bereichen militärischer Operationen und in allen Konfliktsituationen" Anwendung. C2W ist sowohl für die Offensive als auch die Defensive gültig. Die Doktrin ist natürlich kurz und bündig formuliert. Die Implikationen einer Militärdoktrin werden dem Leser überlassen — Lesern mit militärischem Denkvermögen und einem weitreichenden militärischen und politischen Hintergrund. Ist C2W "eine Anwendung von InfoWar im Rahmen militärischer Operationen", so würde ein Leser mit militärischem Denkvermögen schließen, daß es, abgesehen von der offensichtlichen Notwendigkeit für Defensive und Offensive, (a) andere Anwendungsformen von InfoWar im Rahmen militärischer Operationen und (b) Anwendungsformen von InfoWar auch im Rahmen nichtmilitärischer Operationen geben kann. Genauso findet C2W "in allen Bereichen militärischer Operationen und in allen Konfliktsituationen" Anwendung. Es ist somit nicht mehr nur darauf beschränkt, auf dem Schlachtfeld den Befehlsfluß des feindlichen

Kommandos zu unterbrechen. Die Joint Doctrine for Command and Control Warfare ist insgesamt wahrscheinlich die geeignetste Ausgangsbasis, um die Evolution des InfoWar zu verfolgen. Sie ist der Leitfaden für jede der Teilstreitkräfte beim "Organisieren, Ausbilden und Ausrüsten".

Zwei wichtige Definitionen aus der JP 3—13.1 beinhalten folgende Aspekte: C2W ist der

integrierte Einsatz von psychologischen Operationen, militärischer Täuschung, operationaler Sicherheit, elektronischer Kriegsführung und physischer Zerstörung mit gegenseitiger Unterstützung durch den Nachrichtendienst, um dem Gegner Informationen vorzuenthalten, sein C2-Potential zu beeinflussen, zu schwächen oder zu zerstören, während das eigene C2-Potential gegen solche Aktionen geschützt wird.

Im offiziellen Sprachgebrauch umfaßt InfoWar

Aktionen, die der Erlangung von Informationsüberlegenheit dienen, indem Informationen, informationsbasierte Prozesse sowie Informationssysteme und Computernetzwerke des Gegners getroffen und die eigenen verteidigt werden.

Erwähnenswerte Kernbereiche sind folgende: C2W zeichnet sich nur insofern aus, als es den "integrierten" Einsatz von fünf bereits bestehenden "organisierten, ausgebildeten und ausgerüsteten" militärischen Fertigkeiten darstellt. C2W ist ein neuer Denkansatz, traditionelle Militärtaktiken — z. B. elektronische Kriegsführung oder operationale Sicherheit — umzusetzen. C2W ist nicht so sehr technologieabhängig, sondern viel mehr ein Potential, verschiedene Eigenschaften zu "integrieren", um "dem Gegner Informationen vorzuenthalten und sein C2-Potential zu beeinflussen, zu schwächen und zu zerstören." C2W ist eine Kampfmethode und keine Kampftechnologie. Es geht dabei nicht bloß um einen "Cyber-" oder computerbasierten Kampf.

InfoWar wird trotz seiner militärischen Relevanz ganz klar als ein wesentlich weiterreichendes Konzept verstanden. Obwohl die Streitkräfte Fachkenntnisse, Gerätschaften und Personal für "Aktionen zur Erlangung der Informationsüberlegenheit …" beisteuern können, steht nirgends geschrieben, daß der InfoWar eine zentrale militärische Mission sei, noch daß die Streitkräfte eine führende Rolle dabei spielen. Meiner Meinung nach ist dies der Hauptgrund, warum die US-Streitkräfte seit 1997 anstatt "InfoWar" den weniger beunruhigend klingenden Begriff "Information Operations" (Info-Operationen) verwenden. Auch im Entwurf des "Basisdokuments" JP 3—13 Information Warfare ist bereits von "Information Operations" die Rede.

JP 3—13.1 behält weiterhin seine Bedeutung für das Verständnis der konzeptuellen und terminologischen Grundlage des InfoWar. Es wird nämlich behauptet, daß "effiziente C2W den Befehlshaber der Vereinten Streitkräfte in die Lage versetzt, das Bild des feindlichen Kommandierenden von der Situation am Kriegsschauplatz zu formen." Oder anders gesagt, durch den integrierten Einsatz von elektronischer Kriegsführung, Täuschung etc. die Fähigkeit des Feindes, zu wissen, was vor sich geht, zu beeinflussen. Im wahrscheinlich interessantesten Statement des gesamten Dokuments steckt JP 3—13.1 das höchste Ziel von C2W ab — quasi den Heiligen Gral des InfoWar. JP 3—13.1 behauptet, daß es "sogar möglich sei, den Feind davon zu überzeugen, daß die USA noch vor Einsetzen der Kampfhandlungen ‚gewonnen' haben, was eine Abhaltewirkung von Feindseligkeiten zur Folge hat." Das ist der Angelpunkt der gesamten Diskussion. Damit wird impliziert, daß durch die richtige Integration bestehender militärischer Fähigkeiten, die für den "operationalen" oder "taktischen" Einsatz auf dem Schlachtfeld konzipiert waren, diese über das Schlachtfeld hinausgehen können und den "strategischen" Effekt der Abhaltewirkung von

Feindseligkeiten haben. Richtig eingesetzt, können militärische C2W-Operationen als wichtige Entwicklung gesehen werden, die die Tofflers mit "Anti-Krieg" oder dem Vermeiden von "Kampfhandlungen" bezeichnet haben.[3] Auch wenn es seltsam anmutet, so haben im Zuge der Operationen in Bosnien Militärs der Presse gegenüber erklärt, daß ihre "Informationsüberlegenheit" und die Fähigkeit, das "Bild des feindlichen Kommandierenden von der Situation zu formen" ihre wichtigsten verfügbaren "Hilfsmittel" zur Wahrung des "Friedens" waren.

Vereinfacht gesagt, können "Organisation, Ausbildung und Ausrüstung" für C2W von den Streitkräften weit über die herkömmlichen Zielsetzungen hinaus für "Info-Operationen" oder den InfoWar eingesetzt werden. Gerade darin liegt das Potential von Info-Operationen oder InfoWar, nämlich daß sie an den Fugen zwischen den Bestandteilen der Clausewitz'schen "wunderlichen Dreifaltigkeit" von Staat, Streitkräften und Zivilbevölkerung eingesetzt werden können, womit sich die Frage erhebt, ob der InfoWar eine echte Revolution im militärischen Bereich darstellt oder nicht. InfoWar kann nicht nur den Kommandierenden von seinen Truppen trennen, sondern auch die politische Führung von den Streitkräften oder, ebenso revolutionär, die Bevölkerung vom Staat.

Die US Air Force und der InfoWar

Die US Air Force hat gerade ihre neue Grundsatzdoktrin ausgegeben: Air Force Basic Doctrine: Air Force Doctrine Document 1 (September 1997).[4] Alle zukünftigen USAF-Doktrinen werden von der AFDD-1 abgeleitet werden. AFDD-1 geht völlig konform mit der gemeinsamen Doktrin, nimmt aber, wie auch bei allen anderen Teilstreitkräften, Rücksicht auf die Besonderheiten der Kriegsführung in der Luft und ergänzt sie den Erfahrungen der USAF gemäß. Die wichtigste Ergänzung in der neuen Grundsatzdoktrin besteht darin, daß die "Informationsüberlegenheit" dem traditionellen Herzstück, der Überlegenheit in der Luft und im Weltraum, gleichgesetzt wird. "Informationen zu dominieren ist im Konfliktfall heute genauso bedeutsam wie die Kontrolle über den Luft- und Weltraum, oder wie die Okkupation von Land in der Vergangenheit (Hervorhebung durch den Verfasser), und wird als unverzichtbare und synergetische Komponente der Luft- und Weltraummacht eingestuft." Vom Standpunkt der USAF aus — die ja der Hauptlieferant und -betreiber von globalen Luft- und Weltraumaufklärungs-, Überwachungs- und Nachrichtensystemen sind, und die durch die "globale Reichweite" der Luft- und Weltraumsystemen eine bei weitem kürzere Reaktionszeit als die traditionellen Land- und Seestreitkräfte zulassen — ist es nur natürlich, daß die "Informationsüberlegenheit" mit der Luftüberlegenheit gleichgesetzt wird. Offen gesagt, ist die Erlangung der Informationsüberlegenheit ein sehr ambitioniertes Ziel. Andererseits hat man erkannt, daß sie für einen modernen Einsatz im Luft- und Weltraum unabdingbar ist und für die Umsetzung der in der zugrundeliegenden gemeinsamen Doktrin Joint Vision 2010 neu definierten "operationalen" (oder Schlachtfeld-) Konzepte von überlegener Manöverfähigkeit, präzisem Einsatz, konzentrierter Logistik und multidimensionalem Schutz genauso bedeutsam ist.[5] Für die USAF bedeutet Informationsüberlegenheit die "Fähigkeit, Informationen zu sammeln, zu steuern, auszunützen und zu verteidigen, während dem Feind diese Fähigkeit verwehrt bleiben soll." Sie schließt, gleich wie in der traditionellen Zielsetzung der Luft- und Weltraumüberlegenheit, die "Erlangung der Kontrolle über den Informationssektor sowie gänzliche Ausnutzung der militärischen Informationsfunktionen" ein. AFDD-1 anerkennt und übernimmt erneut die Standarddefinitionen von Command and Control Warfare (C2W) und von Info-Operationen. Es wird hinzugefügt, daß InfoWar Info-Operationen sind, die "während eines Konflikts oder einer Krise eingesetzt werden, um bestimmte Ziele gegen einen spezifischen Feind oder Feinde zu erreichen" und wahrt damit die Erkenntnis, daß InfoWar eine Untergruppe der Info-Operationen ist.

Doktrinen sind, obgleich deutliche Weisungen, nicht die einzigen verbindlichen Quellen über die Nomenklatur und offizielle Denkweise zum InfoWar in den USA. Jede der Teilstreitkräfte hat ihren offiziellen "Kommentar" publiziert, um einen Beitrag zur doktrinellen Rivalität zwischen den Teilstreitkräften und der politischen Debatten zu leisten. Die Argumente für die Bündelung der Ressourcen auf das "Organisieren, Ausbilden und Ausrüsten" und die Diskussionen zwischen Traditionalisten und Innovatoren innerhalb einer der Teilstreitkräfte erfolgen sehr oft unter der Federführung des (zivilen) zuständigen Staatssekretärs und des (militärischen) Oberbefehlshabers. Das für die USAF vom Staatssekretär und Oberkommandierenden ausgegebene Dokument, Cornerstones of Information Warfare, ist insofern das interessanteste, als es sich in seiner Sichtweise des InfoWar deutlich von den (wenn man so sagen darf) "traditionellen" Sichtweisen der übrigen Teilstreitkräfte abhebt.[6]

Cornerstones erörtert, beinahe schon gegen jede Intuition, daß InfoWar entweder "indirekt" oder "direkt" gesehen werden kann. Indirekter InfoWar besteht darin, Informationen für den Feind zu verändern, indem Ereignisse oder Erscheinungen geschaffen werden, die vom Feind beobachtet oder wahrgenommen werden müssen, um wirksam zu werden. Ein getürkter Funkspruch, der vom Feind nicht abgehört wird, oder ein falscher Blip auf dem Radarschirm, der von der feindlichen Fliegerabwehr nicht entdeckt wird, sind eine Vergeudung von Elektronen. Für die USAF ist laut Cornerstones das, was für die anderen Teilstreitkräfte Command and Control Warfare bedeutet, im besten Fall indirekter InfoWar, der bloß durch den "integrierten" Einsatz höchst traditioneller militärischer Techniken wie psychologischer Operationen, elektronischer Kriegsführung, Täuschungsmanövern etc. geführt wird. Ja, es handelt sich um InfoWar, ist aber nicht tatsächlich neu und hängt zu sehr von den Beobachtungen und Reaktionen des Feindes ab. Auf den Punkt gebracht: Die USAF hat die globale Infrastruktur der Information erkannt. Jeder ernstzunehmende zukünftige Gegner hat Zugang zu "unendlichen" alternativen, ja, sogar multispektralen Informationsquellen, um seine Wahrnehmungen gegenzuprüfen. Der "CNN-Effekt" und die globale Infosphäre könnten die traditionellen Maßnahmen zum Schutz "freundlicher" oder zum Absetzen falscher Informationen zu einer Vergeudung knapper Ressourcen werden lassen. Das beste für die USAF wäre wohl, für den "direkten" InfoWar zu "organisieren, auszubilden und auszurüsten".

Direkter InfoWar besteht darin, "die Informationen des Feindes zu ändern, ohne dessen Beobachtungs- und Analyseprozesse zu bemühen". Das heißt, die Information wird verändert, ohne daß dem Gegner dabei bewußt wird, daß er die falsche Information "wahrgenommen" hat. Direkter InfoWar wird in erster Linie mittels "Informationsattacken", wie sie in Cornerstones betitelt werden, geführt. Das heißt, "die Information direkt zu korrumpieren, ohne dabei die physikalische Entität, in der sie enthalten ist, sichtbar zu verändern." So würde z.B. ein Computervirus, der den Algorithmus für die Zielberechnung von Fliegerabwehrkanonen beeinflußt, genau auf diese Definition zutreffen. Das bedeutet, daß der Computer für die Kanonen weiterhin wie am Schnürchen läuft — nur daß die Geschoße zwanzig Meter zu hoch fliegen. Wie oder ob eine derartige "Informationsattacke" gegen ein vergleichsweise einfaches Gerät wie ein Fliegerabwehrsystem geführt werden kann, wird in den Mantel strengster Geheimhaltung gehüllt, der von den US-Militärs "Black World" genannt wird. Es ist unbestritten, daß eine derartige Fähigkeit einen Trumpf im "direkten" InfoWar darstellt. Beeinflußte man die Weltanschauung, nach der gegnerische Staatsführer, Streitkräfte und die Bevölkerung Wahrnehmungen interpretieren, würde das "direkten" InfoWar in seiner höchsten Form bedeuten. Daß dies von äußerstem "strategischen" Wert wäre, wird wohl niemand bestreiten.

Phantasie oder Zukunft des Krieges?

Klingt "die Änderung der Informationen des Feindes ohne dessen Beobachtungs- und Analyseprozesse zu bemühen" auch nach Science-fiction oder nach einem alten Forschungsprojekt des KGB über reflexive Kontrolle, so kann man es auch als logische Implikation einer wichtigen "Epistemologie der Kriegsführung", die in den US-Streitkräften weite Verbreitung gefunden hat, sehen. Der verstorbene Luftwaffen-Colonel John Boyd (1997) war ein exzellenter Kampfpilot und, nach seiner Pensionierung, strategischer Denker, der eine neue Sichtweise von Konflikten entwickelt hat, die unter US-Militär- und Wirtschaftsstrategen als "O-O-D-A Loop" bekannt wurde.[7] Jede Konfliktsituation kann in vier Komponenten zerlegt werden: Beobachtung, Orientierung, Entscheidung und Handlung (observation, orientation, decision and action). Ob Kampfpilot oder Wirtschaftsstratege, zuerst muß das Umfeld genauestens wahrgenommen werden. Die zweite Phase, die der "Orientierung" ist der mentale Vorgang, bei dem das Beobachtete mit dem bereits Bekannten verglichen bzw. kontrastiert wird. Piloten würden das "Situationsbewußtsein" und Philosophen "implizites Wissen" nennen. Auf der Grundlage der "Analyse" des Beobachteten und des Bekannten "entscheidet" und "handelt" man — O-O-D-A. Für John Boyd ist es das Ziel des Kampfpiloten, "in die Schleife" des Gegners zu gelangen, und schneller und präziser als dieser zu beobachten, zu orientieren/bewerten, zu entscheiden oder zu handeln. Dieser einfache Gedanke wurde zur "Epistemologie der Kriegsführung", die in der Denkweise der US-Militärs weit verbreitet ist. Man könnte Dutzende von Zitaten in den Doktrinen oder Schulungshandbüchern anführen.[8] Besonderen Einfluß hat sie für das US Marine Corps erlangt. Das Ärgerliche für den Forscher ist, daß Boyds Ideen nur als Photokopien von Folien existieren, die er anläßlich seines Vortrags Discourse on Winning and Losing ("Diskurs über Sieg und Niederlage") erstellt hat. Diesen Vortrag hat er zwar Hunderte Male an Militärakademien und im Pentagon gehalten, doch gibt es keine "gedruckte" Fassung von Boyds Gedanken.

Für viele in der InfoWar-Gemeinde der US-Streitkräfte basieren Info-Operationen, InfoWar und C2W auf dem Gedanken, daß IW oder C2W im wesentlichen Mittel sind, um die O-O-D-A-Schleife oder den Entscheidungszyklus des Gegners zu beeinflussen, zu unterbrechen, zu verzögern oder in sie einzudringen. Das Endprodukt jeder militärischen Operation ist eine "Handlung". Diese "Handlung" ist die Folge eines Befehls oder einer "Entscheidung" von höherer Ebene, den eine militärische Einheit erhalten hat. Wird also das Kommando- und Kontrollsystem durch die Störung der Übertragung dieser "Entscheidung" zum "Ausführenden" geschwächt, so wird die Effizienz dieser Einheit (oder besser: deren militärische Relevanz) geringer. Attackiere also das feindliche Kommunikationssystem. Schieß die Brieftaube ab oder störe den Funkverkehr.

Es wird auch in Zukunft noch immer nützlich sein, die Verbindungskanäle zwischen "Entscheidung" und "Handlung" zu stören, und dies wird daher auch weiterhin versucht. Auch die bisherige Form der elektronischen Kriegsführung wird fortgeführt werden. Vor allem in der USAF sind viele Militärstrategen der Meinung, daß die zukünftige globale Infosphäre, vor allem die extrem komplexen, sicheren und redundanten Telekommunikationsnetze, jeden Versuch, "die Brieftaube abzuschießen", zu einer Vergeudung knapper militärischer Ressourcen werden läßt. Es wird einfach zu viele alternative Kanäle zur Übermittlung von Entscheidungen an Untergebene geben. Ebenso ermöglicht die Dichte der sich entwickelnden und den Globus umspannenden Kommunikation einen "verteilten" Entscheidungsfindungsprozeß, der wesentlich schwieriger zu beeinflussen oder zu stören sein wird. Der "indirekte" InfoWar hat ein Problem.

Erinnern wir uns, daß der "Heilige Gral" des InfoWarrior darin besteht, "die Einschätzung der Lage auf dem Schlachtfeld des feindlichen Kommandierenden so zu beeinflussen", daß der

"Feind davon überzeugt ist, daß die USA gewonnen haben und dadurch eine Abhaltewirkung von Feindseligkeiten erzielt wird." Im Sinne der militärischen Epistemologie der O-O-D-A-Schleife "zielt" der InfoWarrior auf alle Einrichtungen, Denkprozesse und Handlungen, die es dem Gegner erlauben, die Situation korrekt "zu beobachten", richtig einzuschätzen ("Orientierung"), was diese Beobachtungen bedeuten, aufgrund dieser Einschätzungen rasche, präzise und effiziente Entscheidungen zu treffen und diese Entscheidungen als Kommando und Kontrolle für effektive und rasche Aktionen zu übermitteln.

Die USAF ist, wie schon erwähnt, aufgrund ihrer Kenntnisse im Bereich der globalen nachrichtendienstlichen Tätigkeit, Aufklärung, Überwachung und Kommunikation zu der Erkenntnis gekommen, daß der InfoWar immer schwieriger durchzuführen und von immer weniger Erfolg gekrönt sein wird, wenn er sich primär auf den Angriff der "Beobachtungs"-Komponente der O-O-D-A-Schleife eines Gegners konzentriert. Eine kurze Überlegung macht deutlich, daß die traditionellen Komponenten von C2W größtenteils von der Schaffung einer "Wahrnehmung" oder "Beobachtung" abhängen. Dies wurde in Cornerstones als "indirekter" InfoWar bezeichnet, da der Effekt ohne die "Beobachtung" nicht möglich ist. "Direkter" InfoWar zielt jedoch — vor allem mit seinen Informationsattacken — auf die Orientierungs-Phase bzw. -komponente der O-O-D-A-Schleife.

Die wahren Ziele eines guten InfoWarrior sind somit (konzeptuell) die "Mittler". Das heißt, es gibt immer einen Prozeß, ein System, Personen, Maschinen oder Technologien, die Daten (Beobachtungen) in Informationen umwandeln, die die Entscheidungsfinder zur Orientierung/Bewertung benötigen, bevor sie eine effektive Entscheidung treffen können (Kommando und Kontrolle). Es gibt also immer jemanden oder etwas, das die riesige flirrende Infosphäre von Daten für den Entscheidungsträger in Informationen "umwandelt" bzw. übersetzt. Das kann ein Computerprogramm sein oder das "Bild", das dieser von den amerikanischen Absichten in seinem Kopf trägt, um seine Beobachtungen zu interpretieren. Aus dem Blickwinkel eines InfoWarrior, der die Herausforderung des direkten InfoWar annimmt, liegt das Hauptaugenmerk, auch im Hinblick auf seine Schlüsselrolle für die Intelligence Community, im Auffinden sowie im logischen und empirischen Einordnen dieser "Mittler". Diese Mittler umfassen zumindest: (a) Führungsköpfe der USA, der Verbündeten und der Feinde, (b) die zivile Infrastruktur zur Übermittlung der Informationen, (c) die militärische Infrastruktur für Kommando und Kontrolle und nicht zuletzt (d) die technischen, elektromechanischen und digitalen Systeme, die die Wirksamkeit von Waffen ausmachen.

Wenn die globale Infosphäre Täuschung, Propaganda und Desinformation zur Schaffung der gewünschten "Beobachtungen" immer mehr ausschließt, kann das einzig (logische) Ziel für den InfoWar nur die "Orientierung" sein, auf deren Grundlage die Beobachtungen für die Entscheidungsfindung bewertet werden. Somit würde die exakteste Übersetzung ins Deutsche nicht "Informationskrieg" sondern, frei nach Hegel, "Geistkrieg" lauten.

Fußnoten:

[1] CJCS, MOP-30 Command and Control Warfare, 1993

[2] Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare, 1995

[3] Toffler, Alvin; Toffler, Heidi: Überleben im 21. Jahrhundert. Deutsche Verlagsanstalt, Stuttgart 1994

[4] Department of the Air Force, Air Force Doctrine Document 1: Air Force Basic Doctrine, September 1997

[5] CJCS, Joint Vision 2010, 1996

[6] Department of the Air Force, Cornerstones of Information Warfare, (n.d.).

[7] Von John Boyd gibt es keine Veröffentlichung, aber eine frühe und äußerst getreue Erörterung seiner Gedanken zur O-O-D-A-Schleife findet sich in: Orr, George E.: Combat Operations C3I: Fundamentals and Interactions, Air University Press, Maxwell AFB, AL 1983. Vgl. auch: Stein, George: US Information Warfare: Jane's Special Report, Jane's Information Group, VA 1996

[8] Vgl. Joint Vision 2010