Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 163 (1997)

Heft: 12

Artikel: Information Warfare : strategisches Mittel der Zukunft

Autor: Abegglen, Christoph

DOI: https://doi.org/10.5169/seals-64789

Information Warfare – strategisches Mittel der Zukunft

Christoph Abegglen

Die hervorragende Bedeutung des Wissens im zwischenmenschlichen Handeln stellt keine neue Erkenntnis dar. So rät schon Sun Tzu: «... Know the enemy and know yourself; in a hundred battles you will never be in peril».[1] Ebenso betont Jomini: «... il faut tenter tous les moyens de se bien instruire. ... en multipliant des renseignements, quelque imparfaits et contradictoires qu'ils soient, on parvient souvent à démêler la vérité du sein même de leurs contradiction.»[2]

Die Informationsrevolution und ihre Folgen

Nicht die Bedeutung des Wissens oder die der Informationsbeschaffung stellt den Kern von Information Warfare dar, sondern die Geschwindigkeit, mit welcher Information und Wissen dank der technologischen Revolution gesammelt, verarbeitet, gespeichert, verbreitet und dargestellt werden können. Der Einzug der Digitalisierung, die Einführung des Glasfaserkabels und die Leistungssteigerung von Schaltungen haben nicht nur zur gewaltigen Kapazitätssteigerung in der Telekommunikation geführt, sondern im Zuge des Deregulierungsprozesses fallen auch die Preise.[3] Zudem ist die Anzahl der Medien zur Informationsverbreitung gestiegen: Neben Presse, Radio und öffentlichem Fernsehen sind Privatsender, E-Mail, Mobiltelefone, Satellitenfernsehen/-telefon, Fax, GPS, Internet sowie Videokonferenzen getreten.

Um nicht in der Datensintflut zu versinken, schreitet die Datenverarbeitungstechnologie, welche Datenfusion und -analyse automatisiert sowie die Entscheidungsfindung mit Expertensystemen unterstützt, gleichzeitig voran. So ist es heute jedem jederzeit und überall möglich, eine grosse Menge von nahezu Echtzeitinformation zu erhalten oder zu verbreiten.[4]

Da der Informationsfluss nicht mehr ausschliesslich vertikal verläuft, sondern vermehrt horizontal und durch die zunehmende Interoperabilität vernetzt, ist eine Verflachung von Organisationen und eine zunehmende Dezentralisierung hin zu Organisationsnetzwerken absehbar.[5]

Man wird vom traditionellen, an die Hierarchiestruktur untrennbar gebundenen Informationsfluss von Befehl, Nachrichten und Doktrin wegschreiten. Denn in Zukunft wird durch alle Führungsstufen hinweg dieselbe Information allen gleichzeitig zur Verfügung stehen. Damit die Führung wegen der verbesserten Schlachtfeldtransparenz nicht in die Falle des Mikromanagements tappt, gilt es besonders die Unterstellten im Rahmen der Auftragstaktik zu einer einheitlichen Denkweise zu erziehen. Es muss eine klare Trennung von Aufgaben und Kompetenzen zwischen den Führungsebenen erfolgen.

Eine weitere Folge der Informationstechnologierevolution wird wohl das Verschwinden kostspieliger Waffenplattformen sein.[6] Die Fortschritte in der Übermittlungstechnik machen es möglich, die bis anhin auf einer Waffenplattform vereinten Elemente wie Sensoren, Waffen, Entscheidungsträger und Ausführende physisch voneinander zu trennen. So wird eine teure Waffenplattform, die oftmals durch eine einzige kostengünstige Abwehrwaffe vernichtet werden kann, in ihre Einzelteile physisch zerstreut, welche einzig durch Kommunikation miteinander verbunden bleiben, um so den gegnerischen Mitteleinsatz ebenfalls zu verzetteln. Aus einem grossen Angriffsziel werden viele kleine, die in ihren Einzelteilen günstig sind und somit entbehrlich werden.[7]

Schrumpfende Budgets bei erweitertem Aufgabenspektrum verursachen zudem wachsenden Kostendruck auf die verkleinerten Streitkräfte. Dies wird den Einzug von Informationstechnologie aus Überlegungen der Kosteneffizienz und Produktivitätssteigerung beschleunigen. Auch der Simulation eröffnet sich dank der gesteigerten Rechenleistung von Computern mit der «Virtual Reality» eine neue Dimension. Eine Panzermannschaft kann heute z.B. nicht nur von den USA aus gegen eine von Grossbritannien über die Datenautobahn in einem virtuellen Schlachtfeld antreten, sondern Echteinsätze können für einsatzbezogene Ausbildung in der virtuellen Welt eingeübt werden.[8]

Grundlegende Gedanken

Voraussetzung für eine klare Definition des Begriffes und der Mittel der Information Warfare sind einige grundlegende Gedanken betreffend Information, Entscheidungszyklus und möglicher Ansatzpunkte von Information Warfare.

Information

Unter Information versteht man im allgemeinen den Inhalt oder die Bedeutung einer Mitteilung. Information kann aber ebenfalls aus einer Veränderung des Mitteilungsflusses resp. aus einer Nichtmitteilung geschöpft werden.

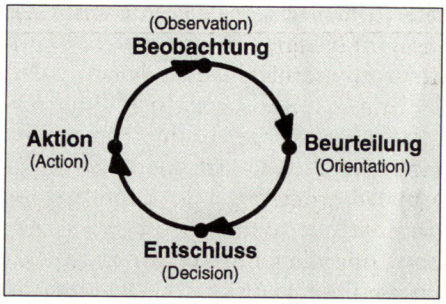


Abbildung 1: OODA-Zyklus.

Wie vorgängig bemerkt, ermöglicht die Informationsrevolution ein immer schnelleres Durchlaufen des Entscheidungszyklus. Abbildung 1 zeigt die Elemente dieser OODA-Zyklus (Observation, Orientation, Decision and Action Loop):[9] Ganz allgemein formuliert versucht Information Warfare, den OODA-Zyklus des Gegners zu beeinträchtigen, währenddem der eigene vor fremder Beein-

flussung geschützt werden soll. Mit anderen Worten besteht das Ziel von Information Warfare darin, in einem Interessenskonflikt den gegnerischen Willen zum Widerstand zu brechen oder zumindest den Gegner in seinem Entscheidungsprozess so zu hemmen, dass er Aktionen nicht rechtzeitig auslösen kann. Zudem sollen einmal ausgelöste Aktionen des Gegners ins Leere schlagen, weil der Gegner seine Beurteilung sowie seinen Entschluss auf irrelevante Informationen von getäuschten Beobachtungssensoren abstützt.

Definition

Sucht man nach einer Definition von Information Warfare, so stösst man auf eine Vielzahl von Varianten.[10]

Einige Definitionen wie diejenige des Verteidigungsministeriums der USA sehen das operative Ziel von Information Warfare in der Erreichung der Informationsüberlegenheit: *«Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based network, while defending ones own information, information based process, information systems and computer-based networks.»*[11]

Doch das Konzept von Informationsüberlegenheit resp. Informationsherrschaft macht wenig Sinn, da die Quantifizierung des Erfolges nicht wie bei der Luftkriegführung möglich ist. In Analogie zur Luftüberlegenheit soll Informationsüberlegenheit dann erreicht sein, wenn «während einer bestimmten Zeit über einem begrenzten Gebiet ... ohne Einschränkung»[12] einer Partei lediglich diejenige Information zukommt, welche die Gegenseite beabsichtigt, ohne dass die eigenen Informationssysteme in irgendeiner Weise vom Gegner beeinträchtigt werden können. Ruft man sich die ganzheitliche Bedeutung von Information in Erinnerung, so leuchtet es ein, dass Informationsüberlegenheit ein Ding der Unmöglichkeit darstellt. Wie es keine «Nicht-Kommunikation»[13] gibt, gibt es keine «Nicht-Information», da auch Ausbleiben von Daten, Befehlen, Aufklärungsergebnissen usw. Information beinhaltet. Zudem kann Information von tradiertem Wissen kaum unterbunden werden.

Hier soll die Variante des «Institute for the Advanced Study of Information Warfare (IASIW)» als Definition dienen: *«Information Warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.»*[14]

Mittel und Einsatzarten

Es werden sieben Formen von Information Warfare unterschieden:[15]

- Command and Control Warfare (C^2W), die gegen die gegnerische Führung und deren Kommunikationsverbindungslinien gerichtet ist.
- Intelligence-based Warfare (IBW), die alle Massnahmen zum Schutze eigener Systeme sowie zur Abwehr gegnerischer Systeme beinhaltet, welche ausreichendes Wissen beschaffen sollen, um den Kampfraum zu beherrschen.
- Elektronische Kriegführung (EW).
- Psychologische Kriegführung (PSYW), die bezweckt, die Gesinnung von Alliierten, Neutralen und Gegnern zu verändern.
- Hacker Warfare (HW), mit welcher Computersysteme angegriffen werden.
- Economic Information Warfare (EIW), die Informationen verwehrt oder kanalisiert, damit die eigene ökonomische Überlegenheit weiter verfolgt werden kann und schliesslich
- Cyberwarfare (CyberW), die einen Sammelbegriff futuristischer Szenarios der Kriegführung darstellt.

In der Anwendung von diesen genannten Formen von Information Warfare wird zwischen zwei Einsatzmöglichkeiten unterschieden. So wird zwischen Netwar und Cyberwar differenziert.[16] Während Netwar schwerwiegend gegen eine Gesellschaft und deren Informationsinfrastruktur geführt wird, zielt Cyberwar auf die gegnerischen Streitkräfte ab und betrifft militärische Operationen.

Netwar unterscheidet sich nicht nur in ihrer Zielgruppe von Cyberwar, sondern auch in ihrer Konfliktintensität. So wird Netwar im Bereich der Gewalt unterhalb der Kriegsschwelle geführt und somit neben Staaten auch von nichtstaatlichen Akteuren getragen.

Dank der Informationsrevolution können sich diese Akteure in Netzwerken transnational organisieren, um durch ihre Dezentralisation weniger verwundbar zu sein. Aber um dennoch ihre Kräfte konzentrieren zu können, bedingt diese Dezentralisation der taktischen Ebene eine einheitliche Doktrin und engen Informationsaustausch. Diese Organisationsform findet ihre Anwendung sowohl im Netwar als auch im Cyberwar.

Die Netzorganisation ist nicht ein neues Konzept, das Ende des 20. Jahrhunderts hervorgebracht worden ist. Vielmehr bewährte sich dieses schon bei Drogenkartellen und Schmugglerringen, aber auch in der Kriegsgeschichte.[17]

In Abbildung 2 werden die möglichen Ansatzpunkte von Information Warfare im Entscheidungszyklus dargestellt.[18] Diese Darstellung verdeutlicht, dass nicht nur Datenerfassung getäuscht, in deren Verarbeitung manipulativ eingegriffen und deren Verbreitung gestört werden können, sondern dass Information Warfare die Wahrnehmung der Ergebnisse und deren Bewertung durch den Menschen indirekt verändern soll.

Konzept

Information Warfare ist kein neues Konzept. In der Guerillakriegführung von Mao Tse-tung kann ein praktisches Beispiel von Information Warfare gesehen werden. Mit der Informationsrevolution veränderte sich lediglich die qualitative Anwendbarkeit von Information Warfare.

Die ganze Diskussion um Information Warfare unterstreicht etwas mit Bestimmtheit: Allgemein wird im westlichen Denken neu der Schwerpunkt in der Kriegführung deutlich auf die Seite der Täuschung gesetzt. Einerseits ermöglicht die Technologierevolution unter günstigen Bedingungen eine noch nie dagewesene Schlachtfeldtransparenz, andererseits bietet dieselbe Technologie die notwendige Chance, den Gegner auf eine noch kaum erreichte Qualität zu täuschen, so dass Überraschung auch auf dem modernen Schlachtfeld erzielt werden kann.[19] Das Konzept Information Warfare umfasst eine weite Bandbreite, die vom zwischenstaatlichen Krieg im Clausewitz'schen Verständnis als «Fortsetzung der Politik mit anderen Mitteln»[20] d.h. mit physischer Gewalt, bis hin zum Interessenskonflikt

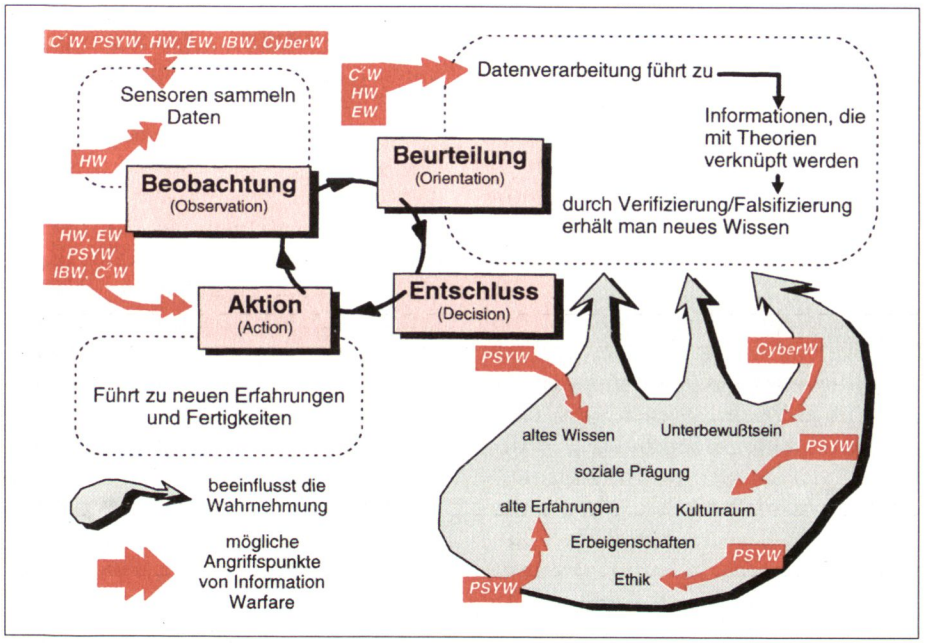


Abbildung 2: Entscheidungszyklus mit möglichen Ansatzpunkten von Information Warfare.

ganz allgemeiner Natur reicht. Darin werden Staaten, sprich deren Streitkräfte, Non-Gouvernmental Organizations (NGOs), Trans-National Corporations (TNCs), Trans-National Criminal Organizations (TCOs) (organisierte Kriminalität), Guerillakämpfer, Verbrecher und Terroristen sowie Abenteuer suchende Jugendliche als mögliche Akteure betrachtet. Dabei umfasst die Konfliktintensität ein Spektrum, das von friedlicher Koexistenz, d.h. Wettbewerb und Konkurrenz, über Gewalt unterhalb der Kriegsschwelle bis hin zum klassischen Krieg reicht.

Die zur Konfliktaustragung eingesetzten Mittel umfassen ein Arsenal, das vom Wort und Bild bis zum nuklear-elektromagnetischen Impuls (NEMP) alles beinhaltet. Die Schwierigkeit, den Urheber einer Information Warfare-Attacke zu lokalisieren, ja selbst eine Attacke als solche zu erkennen, verwischt die Grenzen zwischen Krieg und Frieden, Kriminalität und Krieg sowie zwischen innerer und äusserer Sicherheit.

Es liegt deshalb nahe, Information Warfare nicht mit dem eingeschränkten Begriff der Informationskriegführung zu übersetzen, sondern diesen auf die ganzheitliche Betrachtungsweise der Strategie von General Beaufre auszuweiten: «*...la stratégie ne doit pas être une doctrine unique, mais une méthode de pensée permettant de classer et de hiérarchiser les événements, puis de choisir les procédés les plus efficaces.*»[21] Indem Strategie als eine Denkmethode betrachtet wird, löst sie Beaufre von ihren ursprünglich kriegerischen Fesseln und weitet dieselbe in ihrer Anwendbarkeit auf jedes zwischenmenschliche Handeln aus. Grundsätzlich definiert Beaufre Strategie als die Kunst der Dialektik des Willens, indem Macht zur Lösung des Konfliktes von Streitparteien verwendet wird. Ziel der Strategie ist es, den Gegner davon zu überzeugen, dass es zwecklos sei, in einen Kampf einzutreten oder diesen weiterzuführen. Die Entscheidung wird dann fallen, wenn man eine Situation geschaffen hat und diese als Gelegenheit ausnützt, in welcher die moralische Desintegration des Gegners soweit herbeigeführt worden ist, dass er zur Annahme unserer Bedingungen gezwungen werden kann.[22]

Wahl der Mittel

Die Wahl der Mittel dazu hängt sowohl von der Verwundbarkeit des Gegners als auch von den eigenen Möglichkeiten ab. Beaufre unterscheidet dabei zwischen direkter und indirekter Strategie. Während direkte Strategie schwergewichtig militärische Mittel zur Zielerreichung einsetzt, benutzt die indirekte Strategie andere Mittel als militärische Gewalt: So z.B. Diplomatie, politische und wirtschaftliche Sanktionen, aber auch einen revolutionären Aufstand, um eine Intervention von aussen vorzubereiten oder um eine Regierung zu stürzen sowie einen Guerillakrieg in Verbindung mit internationalen Aktionen.[23] Hier ist denn auch die Informationstechnologie – und mit dieser die Informatik – als zusätzlicher Machtfaktor neben Diplomatie, Wirtschaft, Kultur, Ideologie und Streitkräfte dazuzusetzen. Kurz, das Konzept Information Warfare beinhaltet also je nach Anwendungsart Elemente der indirekten wie auch der direkten Strategie.

Alle Handlungen im Bereich Information Warfare, die beabsichtigen, die Informationsinfrastruktur und Informationsprozesse unbemerkt zu seinen eigenen Gunsten auszunützen, sollen unter dem Begriff des verdeckten Vorgehens subsumiert werden. Darunter können u.a. Massnahmen fallen, die darauf abzielen, Annahmen und Wissen der Gegenpartei mittels Psychological Warfare zu beeinflussen. Weiter sollen darunter auch Aktionen im Bereich Hacker Warfare gezählt werden, die als konstruktiv bezeichnet werden. Damit ist die Beschaffung von Geld, Informationen, Hard- und Software gemeint, ohne dass die Informationsinfrastruktur dadurch von Ausfällen beeinträchtigt würde. Sympathisanten sowie Nachrichten und Aufklärungsergebnisse sollen mit Psychological Warfare bzw. mit Intelligence based Warfare ebenfalls vom Gegner unbemerkt beschafft werden können. Auch alle defensiven Massnahmen zum Schutz der eigenen Informationsinfrastruktur und der eigenen Informationsprozesse fallen in den Bereich des verdeckten Vorgehens, falls diese erfolgreich sein wollen.

Vorgehensweise

Unter dem Begriff des offenen Vorgehens sollen alle Massnahmen verstanden werden, welche die Informationsinfrastruktur und Informationsprozesse zu stören beabsichtigen, so dass diese wegen Überlastung, hard- oder softwareinduzierter Systemausfälle oder gar wegen physischer Zerstörung aussetzen. Schon die Androhung solcher Massnahmen soll unter die Bezeichnung des offenen Vorgehens von Information Warfare fallen.

Direkte Bedrohung

Auf strategischer Ebene wird abgewogen, ob resp. wie die Mittel von Information Warfare im Rahmen von Netwar zur Zielerreichung eingesetzt werden können. In der Form von Netwar findet man wahrscheinlich diejenige Möglichkeit, welche Sun Tzu als die höchste Vollkommenheit eines Strategen bezeichnet, nämlich indem dieser die Gegenpartei durch Angriff auf dessen Strategie überwindet. Hier, wie auch auf operativer Ebene, gilt es im besonderen, die Mittel und Vorgehensweisen mit dem Endziel abzustimmen. Denn Netwar nimmt nicht nur Formen des totalen Krieges an, sondern ist in seiner Wirkung mit derjenigen eines Nuklearkrieges zu vergleichen.[24] Die Wirkung einer Netwar-Attacke ist in Kollateral- und Folgeschäden schwer einschätzbar. Dabei wird nicht zwischen Kombattanten und Zivilisten unterschieden.

In einer zunehmend interdependenten Welt lässt sich zudem nicht ausschliessen, dass man selbst von Folgeschäden der eigenen Netwar-Offensive betroffen sein wird. So liegt ein weltweiter Börsenkrach durchaus im Bereich des Möglichen, wenn man beispielsweise die Börse in Tokio durch Hacker Warfare mit imaginären Devisentransaktionen überschwemmt.

So wirft Netwar gleich wie der Einsatz von Nuklearwaffen Fragen des Kriegsvölkerrechts auf. Neben den legalistischen Aspekten gesellt sich aber auch die Frage der Ethik. Dank der Informationsrevolution sind Angriffe im Bereich der Semantik und Epistemologie in einer noch nie dagewesenen Qualität möglich. So ist das Opfer eines «Netwars» von hoher Intensität letztlich die Wahrheit.

Ob die Androhung von Netwar ähnlich wie Atomwaffenarsenale eine Dissuasionswaffe auf strategischer Ebene sein kann, hängt von zwei Faktoren ab:

- Erstens muss die Wirkung von Netwar in ihrer Durchschlagskraft die Gegenseite so überzeugen, dass diese die Kosten einer möglichen Konfliktaustragung deutlich höher als irgendwelchen Nutzen daraus einschätzt.
- Zweitens muss der Gegenseite mittels einer glaubhaften Einsatzdoktrin bewusst gemacht werden, dass Netwar sie ab einer bestimmten Eskalationsstufe eines Konfliktes treffen würde.

Indirekte Bedrohung

Neben dieser direkten Bedrohung besteht aber durchaus die Möglichkeit einer indirekten Bedrohung. Wenn im Landkrieg unter direkter Bedrohung die Besetzung resp. eine Androhung der Besetzung eines Landes, unter indirekter Bedrohung ein Durchmarsch resp. eine Androhung eines Durchmarsches durch ein Drittland zum Zwecke einer Besetzung des gegnerischen Territoriums verstanden wird, so kann im Bereich Information Warfare unter indirekter Bedrohung das Ausnutzen der Informationsinfrastruktur und Informationsprozesse eines Drittlandes zum Zwecke von Netwar gegen die gegnerische Informationsinfrastruktur und Informationsprozesse verstanden werden.

Staaten, die besonders von diesem Bedrohungsszenario eines Konfliktes betroffen sind, besitzen eine ausgezeichnete sowie vernetzte Informationsinfrastruktur, die durch geringe defensive Massnahmen gekennzeichnet ist und dadurch grosse Sicherheitslücken aufweist.

Das Erkennen einer Netwar-Attacke erweist sich aus technischen Gründen als äusserst schwierig. Bestimmte Vorgehen auf operativer Stufe können diese Tatsache zusätzlich verstärken. Eine vage Identifikation des Aggressors legt aber eine schlechte Basis zur Legitimation eines bewaffneten Vorgehens als mögliche Gegenreaktion auf eine Netwar-Attacke.

Information Warfare auf operativer Ebene durchbricht in der Kriegführung althergebrachte Vorstellungen von Raum und Zeit. Dank verdecktem Vorgehen können Kriegsvorbereitungen monatelang, ja über Jahre hinweg, unbemerkt durchgeführt werden. Taktische Vorausaktionen im Bereich Hacker Warfare wie das Implantieren von Trojanischen Pferden, Zeitbomben oder Bedingungsbomben lassen sich vorgängig ausführen. Die Wirkung dieser Implantate kann dann auf einen bestimmten Zeitpunkt, mit einer spezifischen Operation koordiniert, Monate später ausgelöst werden.

In der räumlichen Dimension umfasst das potentielle Kriegstheater nicht mehr lediglich den Raum, in dem sich Antagonisten physisch angreifen können, also Operationstheater, Operationsbasis inkl. Verbindungslinien sowie im Zeitalter der Interkontinentalraketen den Heimatboden, sondern beinhaltet wegen der indirekten Bedrohung die ganze Welt inkl. Weltraum. Da Bits und Bytes praktisch zeitverzugslos überall hin verschoben werden können, liegt die Annahme nahe, dass im Bereich von Netwar das Ausnutzen der äusseren sowie konzentrischen Linien immer zum Vorteil gereichen wird. Denn diese Operationslinienwahl ermöglicht der offensiven Partei, die Gegenseite aus verschiedenen Richtungen gleichzeitig zu attackieren. So können denn auch die Spuren, die zum Aggressor hinführen könnten, zusätzlich verwischt werden, so dass die Identifikation desselben überaus schwierig sein dürfte.

Phasenverlauf eines künftigen Konfliktes

Der Verlauf von Information Warfare kann in vier Phasen unterteilt werden: Erstens in eine Lernphase, zweitens in Schöpfphase, drittens in eine Eskalationsphase und schliesslich viertens in eine Phase der Friedensfindung resp. Deeskalation.

Die ersten zwei Phasen sind dadurch gekennzeichnet, dass in diesen schwergewichtig verdeckt und mittels indirekter Strategie vorgegangen wird. Denn Lernphase und Schöpfphase bilden zusammen die eigentliche Vorbereitungsphase einer strategischen Offensive, die erst mit der Eskalationsphase eingeleitet wird.

Lernphase

In der Lernphase soll die Informationssystemarchitektur des Zielraumes, d.h. die Architektur der gegnerischen Entscheidungsfindung, auf strategischer, operativer und taktischer Ebene analysiert werden, so dass Information Warfare wirksam geführt werden kann.

Eine Informationsarchitektur umfasst nicht nur die physischen Elemente wie Sensoren und Empfänger mit deren technischen Spezifikationen sowie die Verbindung dieser Teile untereinander. Eine Informationssystemarchitektur beinhaltet auch Massnahmen, die ergriffen werden, damit die Authentizität von Information gewährleistet bleibt. Weiter erklärt die Informationsystemsarchitektur, wie

Daten zu Information werden und wie Information zu Entscheidung führt.

Der Zweck dieser Phase besteht also darin, die zweite Phase vorzubereiten, indem man analysiert, wie im Zielraum Meinungen, Werte, Ideen und Wissen zustande kommen und wie das Resultat an ein bestimmtes Zielpublikum am geeignetsten vermittelt wird. Neben der Analyse der Kultur wird in der Lernphase eine eingehende Schwachpunktanalyse der Informationsinfrastruktur des Zielraumes einen weiteren Schwerpunkt darstellen. Diese Schwachpunktanalyse soll nicht nur Sicherheitslücken aufdecken, sondern gleichzeitig Daten wie Codewörter, Identifikationsprotokolle elektronischer Datenübertragung, Lösungsschlüssel zum Dechiffrieren u.ä. zu deren Ausnützung aggregieren. Den Abschluss dieser Phase bilden Zielkataloge auf strategischer Ebene für den Einsatz der verschiedenen Mittel von Information Warfare.

Schöpfphase

In der zweiten Phase können die in der Lernphase gesammelten Informationen zur Beschaffung von weiteren Informationen, von Geldmitteln sowie von Hard- und Software benutzt werden. In der Schöpfphase soll die eigene Position konsolidiert werden, indem ein ausgedehntes Organisationsnetz aufgebaut wird und die geeigneten Ausgangsbedingungen für die strategische Offensive geschaffen werden. Ziel dieser Phase ist neben der Konsolidierung, Zielkataloge auf operativer Ebene zusammenzustellen sowie den eigenen Zugriff auf authentische Informationen zu gewährleisten.

Je nach strategischer Zielsetzung eines Akteurs kann ein Konflikt über Jahre hinweg in der Schöpfphase verharren. So kann es durchaus sein, dass ein weniger entwickeltes Land oder TCO sich damit begnügt, lediglich von unbemerkt abgezweigten Finanzströmen aus dem Zielraum oder von der eigenen Macht über die Entscheidungsfindung der Gegenseite durch Manipulation zu profitieren.

Eskalationsphase

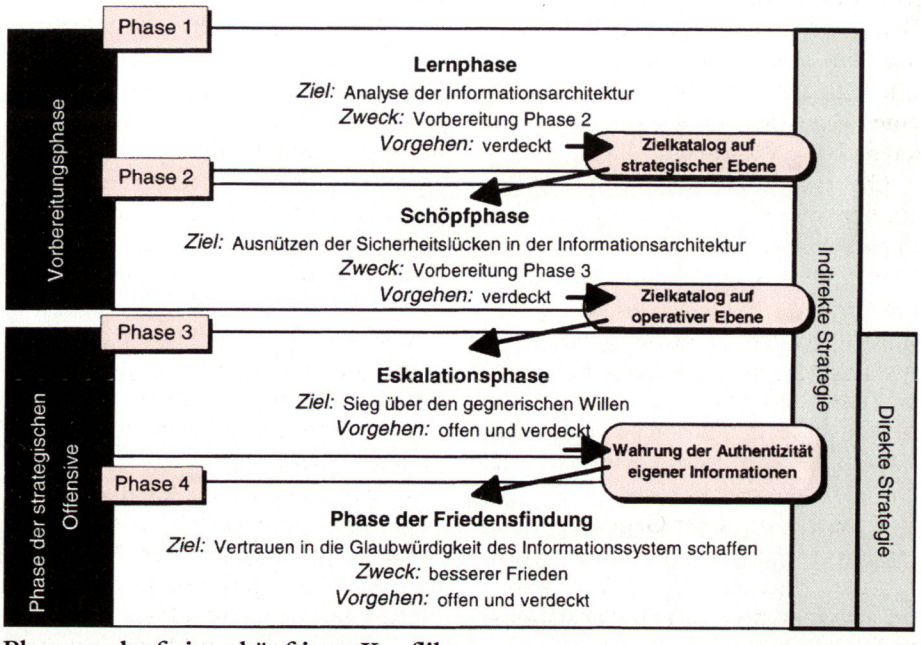
Erst in der Eskalationsphase wird zum offenen Vorgehen sowie zur direkten Strategie übergegangen. Je nach beabsichtigter Konfliktintensität reicht diese strategische Offensive von Dissuasion durch Androhung von Netwar über Erpressung, Terrorismus bis hin zum offenen Krieg mittels Cyberwar. Für diese Phase werden die während der Vorbereitungsphase vorgängig implantierten und zum Teil ausgetesteten Mechanismen zum Eindringen in das gegnerische Informationssystem koordiniert ausgelöst. Ziel der Eskalationsphase ist der Sieg des eigenen Willens über denjenigen der Gegenpartei. Nicht die Vernichtung des Gegners steht dabei im Vordergrund, sondern die Bewahrung der Authentizität der eigenen Informationsbeschaffung und -verarbeitung.

Phase der Friedensfindung

In der Phase der Friedensschliessung gilt es, der Gegenpartei Vertrauen in die Glaubwürdigkeit in ihre eigenen Informationssysteme wieder zu vermitteln. Der Aufwand dazu ist direkt von der Intensität und den Vorgehensweisen von Information Warfare während der Eskalationsphase abhängig. Dies führt deutlich vor Augen, dass schon auf strategischer Ebene die Mittel und Vorgehensweisen im Hinblick auf die Zielerreichung, nämlich das Schaffen eines besseren Friedens, wohl überlegt sein muss.

Zusammenfassung

- Unter dem Konzept Information Warfare darf nicht wie zu Beginn von dessen intellektueller Durchleuchtung lediglich der Kraftmultiplikator Command and Control Warfare verstanden werden, sondern es umfasst das ganzheitliche strategische Denken wie von Beaufre beschrieben. Je nach Einsatzart fallen die Mittel von Information Warfare in die direkte wie auch in die indirekte Strategie.
- Die Informationsrevolution eröffnet auch in einem Schlachtfeld, das durch wachsende Transparenz und Lagebewusstsein gekennzeichnet ist, neue Chancen der Täuschung. Dabei bildet der Entscheidungszyklus der Gegenseite in seiner Gesamtheit das Angriffsziel. Nicht nur Sensoren sollen getäuscht werden, sondern Datenverarbeitung und -übermittlung, ja die Wahrnehmung und das Beurteilungsvermögen des Gegners mittels Beeinträchtigung seiner althergebrachten Annahmen und seines tradierten Wissens. Das allgemein zugängliche Know-how sowie die dazugehörenden geringen Einstiegskosten eröffnen staatlichen und nichtstaatlichen Akteuren die Möglichkeit, Information Warfare zu führen.
- Durch Information Warfare sind kleine und grosse, mächtige wie auch schwache, wenig entwickelte sowie entwickelte Staaten (Akteure) gleich verwundbar. Dabei umfasst die Konfliktintensität sämtliche Eskalations-



Phasenverlauf eines künftigen Konfliktes.

stufen, die vom Frieden bis zum Krieg reichen. Netwar wird auf strategischer Ebene geführt, wobei dessen Einsatzwirkung mit derjenigen eines Nuklearkrieges vergleichbar ist und somit ähnliche Fragen betreffend Dissuasion, Einsatzdoktrin, Ethik und Legalität aufwirft.

- Auf operativer Ebene wird Cyberwar als praktische Umsetzung von Information Warfare gesehen. Die Mittel, welche verdeckt oder offen eingesetzt werden, sind sowohl bei Netwar als auch bei Cyberwar dieselben, ihre Zielräume hingegen unterscheiden sich. Netwar wird schwergewichtig gegen eine Gesellschaft als ganze, Cyberwar schwergewichtig gegen Streitkräfte geführt.
- Wegen der technischen Möglichkeiten, gepaart mit geschicktem operativen Vorgehen, erweist sich die Identifikation des Aggressors in einem Netwar als ein äusserst schwieriges Unterfangen. Die strategische Offensive gereicht dem Aggressor nicht nur aus diesem Grund zum Vorteil, sondern auch weil sich eine kollektive Massnahme oder eine Koalition gegen diesen kaum einleiten resp. formen, geschweige denn nachhaltig unterhalten lässt.
- Auf der Seite der Organisationsform verflacht die Informationsrevolution Hierarchien, weil Informationen allen Hierarchiestufen gleichzeitig zur Verfügung stehen. So werden sich Organisationsnetzwerke durch ihre Interoperabilität, Flexibilität, Redundanz und Dezentralisation gegenüber starren Hierarchien, welche leicht durch «Guillotinieren» (Ausschaltung der Führung) oder «Strangulation» (Unterbrechen der Verbindung der Führung mit deren Unterstellten) zu neutralisieren sind, durchsetzen.
- Die künftige Konfliktaustragung lässt sich in vier Phasen unterteilen. Die Lern- und die Schöpfphase dienen zur Vorbereitung der Eskalationsphase, die durch ihre Anwendung von Information Warfare und deren Intensität direkt die abschliessende Phase, die der Friedensfindung, beeinflusst.
- Die gute, aber moderat geschützte Informationsinfrastruktur macht die Schweiz in Kombination mit ihren aussenwirtschaftlichen Verstrickungen besonders im Banken- und Versicherungsbereich zu einem natürlichen Ziel für verdeckte Hacker Warfare. Ebenfalls ist die indirekte Bedrohung durch Information Warfare für die Schweiz nicht zu unterschätzen.
- Die Konsequenzen aus der Informationsrevolution und aus Information Warfare sind nun auf strategischer, operativer und taktischer Ebene umzusetzen. Eine Anpassung der Organisationsstrukturen der Streitkräfte wird dabei eine der notwendigen Umsetzungen dieser Konsequenzen darstellen. Ausbildung und Erziehung der Soldaten, insbesondere der Führungskräfte, müssen ebenfalls den neuen Anforderungen genügen. Sammeln und Verwerten authentischer Informationen wird die prominente Rolle in Konflikten einnehmen. Dabei erhalten die Nachrichtendienste schon in Friedenszeiten eine neue, gewichtigere Bedeutung.
- Information Warfare verdeutlicht, dass die Grenzen zwischen Krieg und Frieden nicht klar zu ziehen sind. Das Leben stellt vielmehr einen ununterbrochenen Interessenskonflikt dar. Die Interessenskonflikte unterscheiden sich lediglich in den Mitteln ihrer Austragung, wobei auch diese im Bereich Information Warfare dieselben sind. Krieg unterscheidet sich dennoch von anderen Interessenskonflikten durch die bewusste Inkaufnahme des Tötens und des Getötetwerdens zur Verteidigung bestimmter Werte und Normen.

[1] Griffith, S. B.: **Sun Tzu – The Art of War.** Oxford University Press, London (1971), S. 84.

[2] Jomini, A. H.: **Précis de l'art de la guerre.** Edition Ivrea, Paris (1994), S. 290.

[3] Cairncross, F.: **Das Ende der Distanz** in NZZ Folio, Nr. 2 (1996), S. 42-47.

[4] Alberts, D. S.: **The Unintended Consequences of Information Age Technologies.** *<http://www.ndu.edu/ndu/inss/booksuc/uchome.html>* (Oktober 1996).

[5] Arquilla, J. und Ronfeldt, D.: **Cyberwar is Coming!** in Comparative Strategy, Nr. 12 (1993), S. 143 f.

[6] Waller, D.: **Onward Cyber Soldiers** in Time International (21. Okt. 1995), S. 26-32; Stix, G.: **Fighting Future Wars** in Scientific American (Dezember 1995), S. 74-80; Libicki, M. C.: **What is Information Warfare.** *<http://www.ndu.edu/ndu/inss/actpubs/act003/a003ch04.html>* (Oktober 1996).

[7] Stix, G.: **Fighting Future Wars** in Scientific American (Dezember 1995), S. 74-80.

[8] Economist: **The Software Revolution** in A Survey of Defence Technology (10. Juni 1995), S. 10.

[9] Economist: **The Software Revolution** in A Survey of Defence Technology (10. Juni 1995), S. 5.

[10] Vgl. dazu Institute for the Advanced Study of Information Warfare (IASIW). **What is Information Warfare.** *<http://www.seas.gwu.edu/student/reto/infowar/what.html>*; Magsig, D. E.: **Information Warfare in the Information Age** (Oktober 1996), *<http://www.seas.gwu.edu/student/dmagsig/infowar.html.>* (Dezember 1995).

[11] Manthrope, W. H. J.: **From the Editor** in W. H. J. Manthrope (Hrsg.), **Information Warfare,** S. 3-12; **Defense Intelligence Journal,** Vol. 5, Nr. 1 (1996), S. 9.

[12] Stahel, A. A.: **Luftverteidigung – Strategie und Wirklichkeit.** Verlag der Fachvereine, Zürich, S. 63.

[13] Steiger, R.: **Lehrbuch der Diskussionstechnik.** Huber, Frauenfeld, S. 145,

[14] Institute for the Advanced Study of Information Warfare (IASIW) in **What is Information Warfare** (Oktober 1996), S. 1, *<http://www.seas.gwu.edu/student/reto/infowar/what.html>*.

[15] Libicki, M. C.: **What is Information Warfare** (Oktober 1996), *<http://www.ndu.edu/ndu/inss/actpubs/act003/a003ch00.html>*.

[16] Arquilla, J. und Ronfeldt, D.: **Cyberwar is Coming!** In Comparative Strategy, Nr. 12 (1993), S. 141-165.

[17] Arquilla, J. und Ronfeldt, D.: **The Advent of Netwar.** Santa Monica: RAND (1996).

[18] In Anlehnung an Rona, T. P.: **Information Warfare: An age-old Concept with new Insights** in W. H. J. Manthrope (Hrsg.), Defense Intelligence Journal, Vol. 5, Nr. 1 (1996), S. 57; Boyd, nach Szafranski, R.: **A Theory of Information Warfare – Preparing for 2020** (1987), S. 3, *<http://www.cdsar.af.mil/apj/szfran.html>* (Oktober 1996).

[19] Isbell, B. R.: **The Future of Surprise on the Transparent Battlefield** in B. H. Reid (Hrsg.): **The Science of War:** Back to First Principles. Routledge, London (1993), S. 162 ff.

[20] Clausewitz von, C.: **Vom Kriege** (16. Auflage). Dümmlers Verlag, Bonn (1952), S. 108.

[21] Beaufre, A.: **Introduction à la stratégie.** Librairie Armand Colin, Paris (1963), S. 11.

[22] dito, S. 16 ff.

[23] dito, S. 19.

[24] Stein, G. J.: **Information War – Cyberwar – Netwar,** *<http://www.cdsar.af.mil/battle/chp6.html>* (Oktober 1996).

Hauptmann Christoph Abegglen (1969), ist diplomierter Berufsoffizier der Infanterie im Bundesamt für Kampftruppen. Dieser Artikel ist ein Auszug aus seiner im November 1996 an der Eidg. Technischen Hochschule (ETH) Zürich, Abteilung für Militärwissenschaften, im Rahmen des Fachstudiums an der Militärischen Führungsschule (MFS) verfassten Diplomarbeit. ■