Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 163 (1997)

Heft: 12

Anhang: Information Warfare : Beilage zur "Allgemeinen schweizerischen Militärzeitschrift" ASMZ Nr. 12/1997

Autor: [s.n.]

VSN
ASOR
ASUI
Bulletin

VEREINIGUNG SCHWEIZERISCHER NACHRICHTENOFFIZIERE
ASSOCIATION SUISSE DES OFFICIERS DE RENSEIGNEMENTS
ASSOCIAZIONE SVIZZERA DEGLI UFFICIALI INFORMATORI

Nr. 4,
Dezember 1997

Information Warfare

Information Warfare

Niels Möller-Gulland

Information Warfare – strategisches Mittel der Zukunft

Christoph Abegglen

Informationskonflikte sind Chefsache

Walter Altherr

Psychologische Kriegführung im Zweiten Weltkrieg

Toby E. Rodes

Beilage
zur «Allgemeinen Schweizerischen Militärzeitschrift» ASMZ Nr. 12, Dezember 1997

Information Warfare:

An attack on vital computer systems
that control security, emergency response,
financial transactions, transportation, communications, etc.
(CCI Computer Dictionary).

Information Warfare:

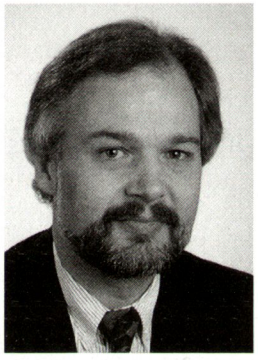
Creating havoc by disrupting the computers
that manage stock exchanges,
power grids, air traffic control and telecommunications.
While the term often refers to warring nations,
it also refers to the disruption of individual organizations
(http://www.zdnet.com/wsources/filters/i/informationwarf.html).

Information Warfare:

Actions taken to achieve information superiority
by affecting adversary information,
information-based processes, and information systems,
while defending one's own information,
information-based processes, and information systems
(CFP 300-1; http://www.marlant.halifax.dnd.ca/acgl.html).

Information Warfare – ein ausschliesslich militärisch-strategisches Mittel?

Wir stehen heute inmitten einer neuen Dimension der Wissensverbreitung. Nie zuvor war das Wissen einer dermassen rasanten Veränderung unterzogen, nie zuvor wurde es dermassen rasch gestreut, und noch nie zuvor stand eine Technologie zur Verbreitung dieses Wissens zur Verfügung wie heute: Printmedien, elektronische Medien, weltumspannende drahtgestützte, drahtlose und satellitengestützte Telekommunikationsmittel, Videokonferenzen, E-Mail und Internet, um nur einige wenige zu nennen. Um nicht vollständig in dieser immensen Datenflut unterzugehen, sondern sie auf eine jeweils überblickbare Datenmenge zu filtern und zu reduzieren, stehen ausserdem unzählige Werkzeuge zur Datenverarbeitung und -selektion zur Verfügung.



Oberstleutnant
Ueli Friedländer
Redaktionsvorsitzender
«VSN Bulletin»

Und die Zahl der Anwender – Anbieter und Benutzer – ist Legion! Firmen wie auch Individuen, zivile Industrie- und Dienstleistungsunternehmen wie auch militärische Stellen sind mittlerweile in diese technologische Revolution miteingebunden und hard- und softwaremässig miteinander quasi in einer Schicksalsgemeinschaft vernetzt.

Es erstaunt daher einigermassen, dass Militär und Zivil trotz offenkundiger Gemeinsamkeiten ihre Aktivitäten in Forschung und Entwicklung nicht besser zu koordinieren suchen, sondern die Bestrebungen der anderen nicht zu beachten scheinen. Typisch für diese Denkweise sind die drei an den Anfang dieser Ausführungen gestellten Definitionen, welche zweimal eine «artrein» zivil-wirtschaftliche sowie eine «artrein» militärische Sichtweise reflektieren. Hier wäre ein gebündeltes Vorgehen angesagt, wobei vermutlich aufgrund des grösseren Erfahrungs- und Leidenspotentials der zivile Partner der Gebende sein dürfte.

Am 20. September 1996 hat Kapitän zur See Niels Möller-Gulland anlässlich der Eröffnungstagung zum 50-Jahr-Jubiläum der Vereinigung Schweizerischer Nachrichtenoffiziere (VSN) in Luzern in seinem Referat «Information Warfare» das Thema analysiert und überblicksweise in Einzelbereiche aufgeschlüsselt. Im unmittelbaren Anschluss daran ist der Gedanke gereift, diesen Komplex der aktiven und passiven elektronischen Einflussnahme nicht nur auf militärische, sondern auch auf wirtschaftliche und dienstleistungsorientierte Ziele vertieft zu untersuchen und ihm ein eigenes Heft zu widmen.

Schon bald zeigte sich, dass der Umfang einer ASMZ-Beilage nicht genügen konnte, und so entschied sich der Vorstand, diesem Heft – quasi einem Kurzabriss der «Informatik-Warfare»-Thematik – ein Buch zum selben Thema folgen zu lassen, welches eine weitere Themenvertiefung bringen soll und ungefähr Mitte 1998 im Buchhandel erhältlich sein wird.

Information Warfare

Niels Möller-Gulland

Die Bundeswehr betritt mit der gedanklichen Auseinandersetzung um Information Warfare Neuland und ist zur Zeit dabei, dieses Thema zu erschliessen. Sie hat noch keine einheitliche Auffassung zu dieser wichtigen Zukunftsfrage entwickelt. Die folgenden Ausführungen sind weder als Positionen des Bundesministeriums der Verteidigung noch als die der Bundesregierung oder des Bündnisses zu betrachten. Hier finden sich lediglich Überlegungen, die im Referat für «Militärstrategie» in der Stabsabteilung «Militärpolitik und Führung» angestellt werden.

In diesem Referat wurde vor mehr als zwei Jahren das Thema «Zukunftstechnologien» als ein Gebiet identifiziert, dem unter militärpolitischen und militärstrategischen Aspekten zukünftig besondere Aufmerksamkeit zu schenken sein würde. Mit einer zehnmonatigen Studie, die beim «Amt für Studien und Übungen der Bundeswehr» in Auftrag gegeben wurde, versuchten wir, uns diesem Thema zu nähern.

Während der Bearbeitung stellte sich sehr schnell heraus, dass die Informations- und Kommunikationstechnologie immer mehr zum beherrschenden Technologietrend der Zukunft wird. Daher wurde die Studie im Laufe ihrer Erstellung mit Schwerpunkt auf diese Technologien ausgerichtet. Nach Vorliegen der Studie wurde das Strategiereferat im Zuge der Folgearbeiten beauftragt, eine Position zu diesem Thema zu entwickeln.

Ich möchte voranstellen, dass wir uns bei der Entwicklung unserer Vorstellung noch im Anfangsstadium befinden. Dabei haben wir wie viele andere Nationen – inklusive des Vorreiters USA – das Problem, das gesamte Thema mit allen seinen Facetten in den Griff zu bekommen und sinnvoll zu strukturieren. Dies ist aber erforderlich, um unseren Entscheidungsträgern das Problem in möglichst all seinen Dimensionen verständlich zu machen und nicht zuletzt um fundierte Vorschläge für ein weiteres Vorgehen entwickeln zu können.

Was versteht man unter Information Warfare?

Unter dem Schlagwort «Information Warfare» findet in der letzten Zeit eine besondere Art der «Kriegführung» erhöhte Aufmerksamkeit in den Medien, welche die spezifischen Möglichkeiten und Schwächen der modernen Informations- und Kommunikationstechnologie und ihren Einfluss auf die Menschen nutzt. Bei dieser Art der Kriegführung wird häufig nicht unterschieden, ob es sich um Auseinandersetzungen zwischen Staaten – also um Krieg im hergebrachten völkerrechtlichen Sinne – oder um substaatliche Konfliktparteien handelt.

Die Meinungen und Auffassungen über die Bedeutung dieses Themenkomplexes und der davon ausgehenden Risiken sind mannigfaltig. Die Bandbreite der Ansichten reicht von sehr futuristischen Vorstellungen über den «Cyberwar» oder «Netwar auf der Datenautobahn», der einen Krieg mit Leiden und Tod ersetzen wird, bis hin zu der konservativen Vorstellung, dass die Massnahmen des Information Warfare zur traditionellen Form der modernen Kriegführung zu zählen sind, die lediglich einem Modernisierungsprozess auf Grund der fortschreitenden technologischen Entwicklung unterliegen.

Die Wahrheit dürfte wie bei vielen Dingen auch hier irgendwo zwischen beiden Extremen anzusiedeln sein. Nach unserer Einschätzung liegt sie für die Gesamtgesellschaft näher am futuristischen Ende, für das Militär dichter bei den konservativen Vorstellungen.

In einer durch das US Department of Defence geprägten Definition werden unter Information Warfare sämtliche Massnahmen verstanden, die darauf abzielen, durch Einwirken auf gegnerische Information und Informationssysteme – bei gleichzeitigem Schutz der eigenen Information und Systeme – Informationsüberlegenheit zu erhalten, um eigene nationale und militärstrategische Ziele durchzusetzen.

Diese Einschränkung auf den militärischen Bereich ist mit Blick auf den Ursprung dieser Definition verständlich, greift aber in unseren Augen und auch in der überwiegend amerikanisch geprägten Literatur zu kurz.

Eine weitergehende Definition subsumiert unter Information Warfare «alle Massnahmen, die das Ziel haben, das gesamte Informationswesen eines Staates zu treffen. Dies kann durch Manipulation, Fälschung, Ausspähung bis hin zur Löschung von Datenbeständen gehen».

Bei dieser Definition wird deutlicher, dass es sich bei «Warfare» nicht notwendigerweise um Kriegshandlungen im traditionellen Sinne handeln muss. Aber auch diese Definition ist noch nicht umfassend genug, da nicht nur staatliche Institutionen Ziel derartiger Operationen sein können, auch Organisationen, Firmen sowie Einzelpersonen können im Zentrum derartiger Massnahmen stehen.

Eine oft gebrauchte Definition, die ihren Ursprung bei der US Army hat, versteht unter Information Warfare «alle Massnahmen zur Schaffung von Informationsdominanz durch Beeinträchtigung gegnerischer Informationen, informationsgestützter Prozesse und der Informationssysteme selbst, unter gleichzeitigem Schutz der eigenen Informationen, informationsgestützter Prozesse».

Aus dieser Definition lassen sich die folgenden wesentlichen Dimensionen und Inhalte von Information Warfare ableiten:

- Information Warfare ist nicht nur auf den rein militärischen Bereich zu beschränken, sondern kann die gesamte Gesellschaft, Organisationen wie auch Individuen, als Ziele und Akteure gleichermassen betreffen.

- Information Warfare überlagert traditionelle Konfliktmuster. Er ist nicht nur zwischen politischen bzw. militärischen Gegnern, sondern vielmehr in jeder «Konkurrenzsituation» denkbar.
- Information Warfare beschränkt sich nicht nur auf den Einsatz immaterieller Wirkmittel, sondern umfasst auch die physische Zerstörung gegnerischer Einrichtungen.
- Information Warfare macht sich die enorm gestiegene Bedeutung von Information für den Menschen in hochentwickelten und komplex vernetzten Industriegesellschaften und für durch ihn geschaffene Systeme und Organisationen zunutze. Er zielt darauf ab, die Perzeption eines gegnerischen Individuums, Systems oder aber einer Organisation – also auch der Gesellschaft – zu beeinflussen.

Ziel von Information Warfare ist daher, Informationsinhalte zu manipulieren und den Informationsfluss, zum Beispiel durch Ausschalten von Ebenen und Verbindungen, zu stören, um so die Funktionsfähigkeit des Gesamtsystems zu beeinträchtigen oder gänzlich zu unterbinden. Dazu ist es u.a. erforderlich, in Besitz wichtiger Informationen des Gegners zu kommen, sei es durch herkömmliche Spionage oder aber auf elektronischem Wege.

Wichtig für das Gesamtverständnis ist jedoch, sich klarzumachen, dass Information Warfare zwar zunächst auf Soft- und Hardware der Informationstechnologie wirkt, aber tatsächlich gegen die Entscheidungsträger gerichtet ist.

Fragen wir nach den Opfern von Information Warfare, stellt sich automatisch auch die Frage nach den Tätern. Auch hier sehen wir eine breite Palette von Möglichkeiten:

- Versucht etwa ein einzelner «Hacker» aus Lust am Probieren in entsprechende Systeme einzudringen?
- Stecken mafiaähnliche Organisationen hinter Computerkriminalität, die in wirtschaftliche oder staatliche Datensysteme eindringen, um finanzielle Vorteile zu erlangen und Machtstrukturen zu unterlaufen?
- Oder wird etwa mit staatlicher Unterstützung eine organisierte Zerstörung oder Verfälschung der Daten einer industriellen Volkswirtschaft und der dazugehörigen Informationsstrukturen betrieben?

In allen diesen Fällen könnte einem Staat möglicherweise grösserer Schaden zugefügt werden als durch eine Auseinandersetzung mit konventionellen Waffen. Problematisch ist dabei: Angreifer dürften schwer zu identifizieren sein, die Grenzen zwischen krimineller Handlung und militärischer Aktion dürften fliessend verlaufen. Jede mögliche Täter-Opfer-Kombination ist denkbar, und häufig werden sich – je nach Motiv – unterschiedliche Kombinationen ergeben.

Warum stellt sich das Problem gerade jetzt?

Es ist für uns alle fast täglich erfahrbar, dass die hochentwickelten Industrienationen an der Schwelle zum Informationszeitalter stehen. Herausragende Kennzeichen des Informationszeitalters sind, dass

- die Menge der verfügbaren Informationen,
- der fast unbeschränkte Zugriff auf sie und
- die Geschwindigkeit ihrer Verarbeitung

zu den Faktoren werden, die für ein effizientes Zusammenwirken der traditionellen Produktionsfaktoren «Arbeitskraft», «Kapital» und «Boden» ausschlaggebend und damit im wirtschaftlichen Sinne für einen Erfolg entscheidend sind. Ihr eigentliches Wirkmoment entfalten diese an Informationen gekoppelten Kriterien mit Blick auf die Entscheidungsprozesse, die allen Aktivitäten vorausgehen müssen.

Der Wandel, der durch neue Informationstechnologien ausgelöst wird, erfasst zuerst den wirtschaftlichen und erst später andere gesellschaftliche Bereiche. In einer Informationsgesellschaft wird der Kampf um Wissen und Information noch wesentlich ausgeprägter zum Machtkampf als das in unserer Gesellschaft der Fall ist. Dieser Machtkampf wird vor allem mit Hilfe neuer Technologien geführt werden. Neue multinationale und nichtstaatliche Organisationen entstehen und gewinnen an Einfluss. Das Auftreten neuer Akteure sowie neue Formen der Konfliktaustragung erweitern das herkömmliche Konfliktspektrum.

Aufgrund der rasanten Entwicklung auf dem Sektor der Informations- und Kommunikationstechnologie kommt es zu einem Trend der Informationsexplosion. Dieser Trend wird bedingt durch die rapide steigende Verbreitung informationsintensiver Systeme, intelligenter Sensoren sowie der computergestützten Kommunikation. Zugleich werden wir unsere Fähigkeiten, mit Informationen umzugehen, neu ordnen müssen und erheblich steigern können. Im militärischen Bereich wird es möglich sein, Sensoren und Effektoren wesentlich wirksamer miteinander zu verbinden. Nahezu Echtzeitaufklärung kann dann unmittelbar zum präzisen und weitreichenden Waffeneinsatz genutzt werden. Die Unterstützung der Führungs- und Entscheidungsprozesse durch leistungsfähige, übergreifende Informationssysteme wird zu deutlich verkürzten Entscheidzyklen führen.

Eine wesentliche Anforderung an die Informationssysteme wird darin liegen, entscheidungsrelevante von nicht entscheidungsrelevanten Daten zu unterscheiden.

Das anbrechende Informationszeitalter wird mit hoher Wahrscheinlichkeit auch das Bild eines zukünftigen Krieges verändern. Wahrscheinlich wird in einem langfristigen Prozess zunehmend materielle Gewalt durch immaterielle Gewalt ersetzt werden. Die physische Vernichtung von Menschen und Material wird hinter der Zerstörung bzw. Lähmung von kommunikations- und entscheidungsrelevanter Infrastruktur zurücktreten. Vielleicht kann man diese Entwicklung mit dem Bild der Entwicklung von Kindern zu Erwachsenen vergleichen. Als Kinder haben wir unsere Konflikte hin und wieder handgreiflich ausgetragen. Als Erwachsener hat man gelernt, dass die geistige Auseinandersetzung eine wesentlich wirksamere und schärfere Waffe darstellt als die der körperlichen Gewalt.

Das mögliche Kriegsbild des Informationszeitalters wird bestimmt sein durch umfassende, vernetzte Strukturen mit zentralisierten Informationssystemen (für den militärischen Bereich: Stichwort «digitalisiertes Gefechtsfeld»).

Die nicht-physischen Einwirkmöglichkeiten gegen Entscheidungszentren sowie gegen Kommunikations- und Informationsstruktur von Konfliktgegnern werden zunehmen. Überlegene Software wird die Hardware dominieren. Oder anders gesagt:

überlegene Computerprogramme werden wichtiger sein als überlegene Computer. Das Kriegsbild einer Informationsgesellschaft wird auch von zunehmenden Möglichkeiten der Einflussnahme auf die Perzeption eines Gegners mit Hilfe neuer Technologien geprägt sein.

Der Faktor Information, der schon immer in der Kriegführung einen hohen Stellenwert hatte, wird im Kriegsbild einer Informationsgesellschaft strategische Bedeutung erlangen und als neuer Faktor zu den klassischen Faktoren Raum, Zeit und Kräfte hinzukommen.

In einer Gesamtschau könnten dann die vier Faktoren wie folgt bewertet werden:

Faktor Raum

Präsenz in einem begrenzten Raum wird wahrscheinlich einen geringeren Stellenwert haben als heute, weil die Informationsdichte in einem Raum zunehmend an Bedeutung gewinnt.

Was ist damit gemeint? Wenn man jederzeit über ein lückenloses Lagebild und über Abstandswaffen verfügt, die in diese Räume wirken können, können Räume kaum noch durch Präsenz von Truppen gehalten werden. Tendenziell wird der Raum erweitert durch intensivierte Nutzung des Weltraums sowie die Aufhebung räumlicher Grenzen durch Kampf in Kommunikations- und Informationsnetzen.

Faktor Kräfte

Kräfte mit Fernwirkung werden immer mehr an Bedeutung gewinnen. Es kommt zur Effizienzsteigerung von Kräften durch Vernetzung sowie durch neue, erweiterte Wirkmöglichkeiten. Insgesamt dürften immaterielle Wirkmöglichkeiten zu Lasten materieller Kräfte an Bedeutung gewinnen.

Faktor Zeit

Die Nutzung eines Informationsvorteils macht Zeit zunehmend zu einem kritischen Faktor. Zeitdruck löst immer schnellere Entscheidungszyklen aus. Die Bedeutung von Zeit steigt, da der im Vorteil ist, der als erster die richtigen Massnahmen auf Grund der richtigen Information anwenden kann.

Faktor Information

Verfügbarkeit von Information kann langfristig bis zur völligen Transparenz des Kriegsschauplatzes führen. Die Einsatzmöglichkeiten von Information zur Einflussnahme auf die Willensbildung eines Gegners werden weit subtiler als heute – und damit wesentlich wirksamer sein.

Langfristig kann der Faktor Information einen qualitativen Sprung von der unterstützenden Funktion in der Kriegführung zum entscheidenden Mittel von zentraler Bedeutung machen. In taktischer wie operativer Hinsicht wird Information die Qualität einer Waffe annehmen, indem sie einerseits immer mehr zur Effizienzsteigerung von Waffen und Einsatzmitteln beiträgt und andererseits selbst zerstörerisch, weil manipulativ auf gegnerische Informationssysteme einwirken kann. In diesem Sinn wird Informationsdominanz zu einem Spiel und könnte etwa das bisherige operative Ziel der Dominanz mit physischen Kräften in einem Raum verdrängen.

Strategisch wird der Informationskrieg neben Land-, Luft- und Seekrieg zu einer zusätzlichen Dimension der Kriegführung. Als Folge dieses Qualitätssprungs und des wachsenden Stellenwerts des Faktors Information steigt die Bedeutung von Information Warfare zumindest als Ergänzung zur traditionellen Kriegführung immer mehr. Es bleibt abzuwarten, ob Information Warfare in der Zukunft das Kriegsbild als solches grundlegend verändern wird. Für die absehbare Zukunft ist jedenfalls nicht damit zu rechnen, dass Information Warfare herkömmliche Formen militärischer Auseinandersetzung ablösen wird. Es wird sie jedoch um eine neue Dimension erweitern. Dennoch kann der Faktor Information künftig zum «winning factor» von Auseinandersetzungen werden.

Technologisches Umfeld

Die bereits heute erkennbare Abhängigkeit von Staaten untereinander wird sich als fortschreitende Vernetzung vor allem in ihren wirtschaftlichen, kulturellen, wissenschaftlichen und anderen Bereichen weiter entwickeln. Der Trend zur Globalisierung wird sich vor allem bei den Wirtschaftsbeziehungen fortsetzen.

Für militärische Anwendungen können neue «dual use»-Technologien einen weiter wachsenden Stellenwert erlangen. Vergleichsweise billige kommerzielle Massentechnologien werden zunehmend auch militärisch unmittelbar verwendet und dabei gerade von solchen Staaten genutzt werden können, die sich bisher militärische Hochtechnologie nicht leisten konnten. Damit schafft die allgemeine Verfügbarkeit von informationstechnologischem Know-how selbst für weniger entwickelte Staaten die Voraussetzungen, in «Inselbereichen» militärische Fähigkeiten aufbauen zu können, die denen von Hochtechnologiestaaten ebenbürtig sind.

Wir müssen auch davon ausgehen, dass Technologietransfer im Zeitalter nahezu unbegrenzt verfügbaren Wissens und Information immer schwieriger zu kontrollieren und einzuschränken sein wird. Es wird damit noch schwieriger werden, eine Proliferation von Know-how und damit von Waffen jeder Art zu kontrollieren.

Mit welchen Risiken müssen wir uns auseinandersetzen?

Politische Risiken

Nach einem französischen Atomtest im September 1996 riefen Computerhacker und Friedensaktivisten aus verschiedenen Ländern im Internet dazu auf, die Kommunikationssysteme Frankreichs durch «Sitzblockaden auf der Datenautobahn» (d.h. die gezielte Überflutung eines Datennetzes mit Informationen) lahmzulegen.

Dieser Punkt gibt dem Thema Information Warfare eine zusätzliche Dimension: er zeigt, dass die Waffen des Information Warfare durchaus auch als politisches Druckmittel angewendet werden können. Je mehr private Nutzer Zugang zu grossen Datennetzen haben, desto grösser wird die Gefahr von organisierten Demonstrationen auf der Datenautobahn. Das kann bedeuten, dass Aspekte von Information Warfare sich zu einem politischen Druckmittel von Gleichgesinnten und Interessenverbänden entwickeln könnten, gleichermassen aber

auch von Regierungen genutzt werden können.

Politische Entscheidungen basieren in der Regel auf einer Vielzahl komplexer, aggregierter Einzelinformationen. Grundsätzlich ist das Risiko einer politischen Fehleinschätzung durch Verfälschung oder Manipulation der zugrunde liegenden Daten und Fakten vorstellbar. Die Gefahr der gezielten Beeinflussung der politischen Meinungsbildung ganzer Bevölkerungsteile mit den Mitteln des Information Warfare verbindet die bekannte Praxis der Propaganda mit modernem technologischen Rüstzeug, das unkontrollierbar und grenzüberschreitend einsetzbar ist.

Wirtschaftliche Risiken

Die Abhängigkeit verschiedener Wirtschaftszweige von der Verfügbarkeit ihrer Informationssysteme ist heute sehr gross. So wird die Information bereits als vierter Produktionsfaktor einer Volkswirtschaft verstanden. Mehr denn je entscheiden Wissensbesitz und schneller Wissenstransport über den Vorsprung und die Wettbewerbsfähigkeit von Unternehmen auf den Weltmärkten.

In den USA spricht man inzwischen sogar schon von der «Informations- und Wissensrevolution», die dabei ist, die Sozial- und Wirtschaftssysteme grundlegend zu verändern.

In diesem Zusammenhang kommt dem ungehinderten Zugang zu Informations- und Kommunikationstechnik eine besondere Bedeutung zu. Untersuchungen haben ergeben, dass die «Überlebenszeit» von Unternehmen nach einem Totalausfall der Datenverarbeitungsanlage nur noch wenige Tage beträgt. So rechnet man beispielsweise mit maximalen Überlebenszeiten bei Totalausfall der Datenverarbeitungen bei

- Versicherungen von 5½ Tagen,
- Herstellern von 5 Tagen,
- Händlern von 2½ Tagen und
- Banken von 2 Tagen.

Mit diesen Zeiten wird deutlich, wie verwundbar moderne Unternehmen und damit die Industriegesellschaft heute sind. Der wirtschaftliche Schaden, der jetzt schon durch Hacker und Viren in der Bundesrepublik jedes Jahr entsteht, lässt sich kaum abschätzen. Auch im Bereich gezielter Wirtschaftsspionage dürfte eine halbwegs zuverlässige Abschätzung des Schadens kaum möglich sein. Die Dimension lässt sich jedoch erahnen, wenn man an die bereits heute enorm hohen Forschungs- und Entwicklungskosten besonders bei Produkten der Hochtechnologie denkt.

Gesellschaftspolitische Risiken

Manipulation und Propaganda stellen kein neuartiges Instrument zur Beeinflussung der Willensbildung der Bevölkerung dar. Dennoch muss man diese, sofern sie gezielt und grossflächig eingesetzt werden, auch als Waffen des Information Warfare sehen.

Die Nutzung der neuen Medien und Kommunikationstechniken erweitert die bisher bekannten Möglichkeiten enorm. Die gezielte Ausstrahlung von Rundfunk- und Fernsehprogrammen ist ein solches klassisches Mittel der Manipulation. Aber auch hier ergeben sich durch die Informationstechnologie neue Ansatzpunkte.

Der Computer bietet die Möglichkeit, ganze Fernsehsendungen zu fälschen. So wollten die USA im Golfkrieg angeblich das Gesicht des irakischen Diktators Saddam Hussein digital nachbilden und diesen eine Rede halten lassen, die ihn in den Augen der Gläubigen diskriminiert hätte. Dies zeigt, dass man mit Hilfe des Computers glaubhafte, virtuelle Realitäten schaffen kann.

Durch Anbindung eines Landes an internationale Netze – beispielsweise die Volksrepublik China im Internet – oder durch weltweit über Satelliten ausgestrahlte Fernsehprogramme ist heute kaum mehr die vollständige Isolation der Bevölkerung eines Landes möglich. Langfristig wäre eine solche Isolation aber der einzig mögliche Schutz vor aggressiver Manipulation von aussen. Dies würde aber zur Isolation auf allen anderen für einen Staat wichtigen Gebieten führen. Grenzen hätten damit ihre frühere Bedeutung weitgehend eingebüsst.

Weltweit gibt es derzeit 1,2 Milliarden Fernsehgeräte und 180 Millionen Personal Computer. Dies stellt ein ungeheures Manipulationspotential dar, das im positiven wie im negativen Sinne politisch und propagandistisch genutzt werden kann. Die Werbung beispielsweise macht sich unterschwellige Beeinflussung zunutze.

Militärische Risiken

Im rein militärischen Sinne könnte man Information Warfare als eine neuartige Form der Kriegführung interpretieren. Gegenüber konventionell geführten militärischen Auseinandersetzungen bietet der unterstützende Einsatz von Information Warfare folgende entscheidende Vorteile:

Zunächst sind Mittel des Information Warfare durchwegs billiger als konventionelle Waffen. Dazu bietet Information Warfare den Vorteil, ausserordentlich abstandsfähig zu sein und Personen in der Regel nicht direkt zu gefährden.

Eine weitere Eigenheit des Information Warfare ist, dass seine Wirksamkeit weniger von der Zahl und Grösse von Waffen, sondern vielmehr von der Intelligenz der eingesetzten Mittel und Verfahren abhängig ist. Angriffe durch Mittel des Information Warfare werden durch den Gegner häufig erst erkannt, wenn es für Gegenmassnahmen zu spät ist, d.h. wenn lebenswichtige Datenbestände und Informationsinfrastrukturen bereits geschädigt wurden oder die Beeinflussung bereits erfolgt ist. Es lassen sich auch Programmteile (z.B. Viren) implementieren, die zwar im Konfliktfall die Leistungsfähigkeit von Führungs- und Waffeneinsatzsystemen beeinträchtigen, aber nicht zu deren Totalausfall führen. Solche Manipulationen sind kaum erkennbar. Sie können bereits in Friedenszeiten vorbereitet werden, ohne dass es bemerkt werden kann.

Was sind mögliche, militärisch geprägte Erscheinungsformen?

Der Begriff Kriegführung muss auch hier im erweiterten Sinn verstanden werden, es handelt sich nicht nur um eine militärische Kriegführung. Die US National Defence University sieht Information Warfare als einen Sammelbegriff, unter dem man sieben unterschiedliche Arten der Kriegführung verstehen kann:

Command and Control Warfare

Vom militärischen Standpunkt aus gesehen die dominierende Komponente im Information Warfare. Com-

mand and Control Warfare beinhaltet alle Massnahmen gegen gegnerische Kommandozentralen und Führungseinrichtungen auf allen Ebenen, inklusive der physischen Zerstörung. Ziel ist es, einen Gegner führungslos zu machen, d.h. einen Zustand zu erwirken, in dem die militärische Führung eines Gegners keine oder unvollkommene Informationen über die eigene Lage hat und die Truppe nicht weiss, was die eigene Führung will.

Information-based Warfare

Bei Information-based Warfare – in anderen Quellen auch Intelligence-based Warfare genannt – handelt es sich um alle Massnahmen, die dem optimalen Erfassen und Verarbeiten aller für die eigene Lagebearbeitung erforderlichen Informationen zum effektiven eigenen Kräfteeinsatz dienen.

Dieses beinhaltet in der passiven Form eine Vernetzung aller möglichen Sensoren und Informationsquellen. Diese passive Form ist die traditionelle Art von Information Warfare, zu der auch alle seit Urzeiten eingesetzten Methoden der Informationsgewinnung und Spionage zählen.

Zur aktiven Form werden alle Massnahmen gezählt, die gegnerische Sensoren manipulieren, täuschen oder zerstören können.

Electronic Warfare

Umfasst alle Massnahmen der elektronischen Kriegführung gegen die gegnerischen Führungsmittel und Führungswege bei gleichzeitigem Schutz der eigenen Fähigkeiten auf diesem Gebiet. Traditionell wird hier nur die Vorherrschaft im elektromagnetischen Spektrum gesehen, die um die Aspekte der Führungs- und Informationssysteme sowie der informationsverarbeitenden Systeme erweitert werden müssen.

Psychological Warfare

Bezieht den menschlichen Aspekt von Information Warfare mit ein und zielt auf die Willensbildung und den Willen eines Gegners. Sie kann auf die gesamte Bevölkerung zielen, aber auch nur auf die Streitkräfte beschränkt werden. Dazu können u.a. fremde, aber auch eigene Medien durch gezielte oder selektive Information genutzt werden.

Hacker Warfare

Zielt darauf ab, in zivile oder militärische Informationssysteme einzudringen und Daten zu manipulieren oder zu zerstören oder den Datenfluss zu unterbrechen. Hierbei handelt es sich grundsätzlich um einen nicht militärischen Anteil von Information Warfare, der im allgemeinen den wirksamsten Effekt in den Medien erzielt.

Es lässt sich unterscheiden zwischen dem Hacker und dem Cracker. Der Hacker dringt in ein System ein, ohne Schaden anzurichten und hinterlässt nur seine «Visitenkarte», um auf sicherheitsrelevante Schwachstellen hinzuweisen. Der Cracker will in einem System Schaden anrichten, beispielsweise durch Infizieren des Systems mit einem Virus.

Economic Information Warfare

Beinhaltet alle Massnahmen der wirtschaftlichen Einflussnahme. Beispielsweise könnte die Manipulation von Börsen- oder Wechselkursen den Zusammenbruch eines nationalen Bankensystems zur Folge haben. Börsentransaktionen per Computer könnten den monetären Abfluss derart schnell veranlassen, ohne dass Banken oder Aufsichtsbehörden rechtzeitig schützende Massnahmen ermöglicht wären.

Netwar/Cyberwar

Unter diesem Begriff – auch virtueller Krieg genannt – werden alle Vorstellungen zusammengefasst, bei denen Teile von Kampfhandlungen in die virtuelle Welt von Computersystemen oder -netzen verlegt und dadurch der Einsatz von physischer Gewalt zunehmend verdrängt wird. Bei vielen Dingen, die unter diesem Namen diskutiert werden, ist nicht abzusehen, wieviel davon realisiert werden kann oder was auf Dauer Science Fiction bleiben wird. Anwendungsbeispiele könnten in etwa Roboter mit künstlicher Intelligenz als Ersatz für Menschen oder satellitengestützte Aufklärung von Datenverarbeitungs-Verbindungen sowie das oft zitierte digitale Gefechtsfeld mit der virtuellen Realität sein.

Ich verzichte hier, auf Einzelheiten des «Wie» des Information Warfare einzugehen, d.h. auf Viren, Trojanische Pferde usw. Dennoch möchte ich an einigen plakativen Beispielen Möglichkeiten des Information Warfare anführen, z.B. angewandter offensiver und defensiver Information Warfare:

– 1996 gelang es Experten der US Luftwaffe in einem Versuch, über das Internet unbemerkt in einen Computer an Bord eines Ägis-Kreuzers der US Navy im Persischen Golf einzudringen. Da dieser Computer zugleich mit dem Schiffsführungssystem vernetzt war, wäre es jederzeit möglich gewesen, dem Schiff beispielsweise falsche Navigationsdaten einzugeben.

– Im Mai 1997 wurde durch einen Makro-Virus das gesamte Datenverarbeitungssystem eines NATO-Stabes gelähmt. Neben der Benutzung privater Software – was natürlich einen Sicherheitsverstoss dargestellt hätte – ist auch denkbar, dass dieses Virus per elektronischer Post eingeschleust wurde.

– Weitere denkbare Angriffsmöglichkeiten bieten sich in den Bereichen der Energieversorgung sowie beim Transport- und Verkehrswesen, beispielsweise durch Störung des Luftverkehrskontrollsystems oder die Lähmung bzw. Beeinträchtigung von Eisenbahnstellwerken.

Weitere Entwicklung

Derzeit liegt der Schwerpunkt der Weiterentwicklung von Information Warfare - auch in den USA - bei den defensiven Aspekten von Information Warfare. Es gilt, Datenverarbeitungsanlagen auf ihre Verwundbarkeit zu untersuchen, Schwachstellen zu identifizieren und Forderungen für Gegenmassnahmen zu entwickeln. Es wird nach Möglichkeiten gesucht, Datennetze über blosse Passworte und Kryptierung hinaus zu schützen.

Die Palette denkbarer Möglichkeiten reicht von automatischer Sperre bei unautorisiertem Zugriff bis hin zur ferngesteuerten Vernichtung sensitiver Daten. Dabei ist zu berücksichtigen, dass sich ein Nutzer nur dann auf übertragene Informationen verlassen kann, wenn auch die Übertragungswege sicher vor fremden Einflüssen sind und in dem Gesamtsystem entsprechend geschützt sind.

Im militärischen Bereich könnte der grösste Nutzen der Informationstechnologie, nämlich die Fähigkeit, riesige Datenmengen direkt an die kämpfenden Truppen zu übermitteln, zugleich auch ihre grösste Schwäche werden. Das Erbeuten auch nur eines einzigen Endgerätes könnte auch dem Gegner den Zugang zum Gesamtwissen eröffnen und ihm gleichzeitig Möglichkeiten für eigene Aktivitäten bieten.

Ausserdem nutzen riesige Mengen von Informationen nur dem, der die für ihn relevanten Informationen rasch ausfiltern kann. Gelingt dies nicht, führt eine Informationsflut leicht zur Lähmung des Entscheidungsprozesses.

Welches sind die Risiken für die eigenen Streitkräfte?

Wenn wir uns die vorgängig genannten Einsatzarten von Information Warfare ansehen, werden wir erkennen, dass davon einiges seit langer Zeit zu den Aufgaben der Streitkräfte gehört. Der Kampf gegen die gegnerische Führungsfähigkeit, Nachrichtengewinnung und Aufklärung, elektronische und psychologische Kampfführung sind traditionelle Aufgabengebiete der Streitkräfte, die in mehr oder weniger Intensität schon immer Teil einer Operationsführung waren.

Wirklich neue Qualitäten an Kriegführung erwachsen durch die Einsatzarten der Hacker Warfare, insbesondere in Verbindung mit Economic Information Warfare. Ziel derartiger Angriffe dürften jedoch in den wenigsten Fällen die Streitkräfte unmittelbar sein. Die zivile Infrastruktur eines Staates, die aber für die Streitkräfte von höchster Bedeutung sein kann, bietet für derartige Attacken lohnenswerte Objekte.

Für die Streitkräfte kommt es darauf an, sich der Möglichkeiten von Angriffen mit Mitteln des Information Warfare bewusst zu sein, dementsprechende Sicherheitsvorkehrungen zu treffen, einfache Rückfallpositionen und Redundanzen zu haben und neue Technologien bewusst und vorsichtig zum eigenen Nutzen einzusetzen.

Der Cyberwar mit dem total vernetzten Soldaten liegt für uns noch sehr weit hinter dem Horizont. Militärische Konflikte werden auch in absehbarer Zeit noch hauptsächlich mit der Hardware durchgeführt werden, die derzeit auf den Kasernenhöfen steht oder im Beschaffungsgang ist.

Der Krieg, der nur virtuell, ohne Verluste von Menschenleben, in den Datennetzen geführt wird, scheint uns in der Zeit von realen, blutigen Kriegen auf dem Balkan, in Afrika und Tschetschenien und dem Streben vieler Staaten nach Massenvernichtungswaffen sehr weit in der Zukunft zu liegen.

Die grössere Gefährdung durch Angriffe mit Mitteln des Information Warfare wird durch uns in den anderen Bereichen eines Staates gesehen. Die neuen Risiken des Information Warfare betreffen die Kommunikations- und Informationsstruktur von Staaten als Ganzes. Wirtschaft, innere Sicherheit und zwischenstaatliche Organisationen sind viel abhängiger von den neuen Technologien als die Streitkräfte und verfügen über so gut wie keinen Schutz.

Für uns ergibt sich ein gesamtstaatlicher Sicherheitsaspekt. Wir sehen den Schutz gegen diese Arten von Angriffen nicht als Aufgabe der Streitkräfte. Es ist erforderlich, dass alle staatlichen Organe und wirtschaftlichen Bereiche, die von diesen Aktionen betroffen sein könnten, ihren Beitrag zum Schutz und für das Funktionieren des Staates leisten.

Dazu dürfte es erforderlich sein, in einem ressortübergreifenden Ansatz zu definieren, welche potentielle Bedrohung von Massnahmen des Information War ausgehen könnten, um auf dieser Basis eine umfassende Strategie zur Abwehr dieser potentiellen Bedrohung zu entwickeln.

Das ist leichter gesagt als getan. Tatsächlich kann man nicht davon ausgehen, dass in allen Sektoren der Privatindustrie und der staatlichen zivilen Verwaltung das Problembewusstsein über die potentiellen Gefahren von Information War vorhanden ist. Der erste Versuch auf unserer Ebene, die Verantwortlichen in den zuständigen Ministerien problembewusst zu machen, verlief ernüchternd. Wahrscheinlich muss ein solches Problembewusstsein von oben nach unten durchgesetzt werden. Ein Weg, den übrigens auch die USA derzeit gewählt haben.

Einschätzung der Risiken

Dies führt uns zu folgendem Fazit hinsichtlich unserer Einschätzung der Risiken:

- Der Schutz der zivilen und militärischen Informationsinfrastruktur wird zu einer vorrangigen und dringenden Aufgabe. Kräfte und Mittel zur Abwehr von Angriffen gegen die Informationsinfrastruktur müssen gebündelt und koordiniert werden.
- Defensive Massnahmen müssen erste Priorität haben.

Nach unserem Wissen vollzieht man derzeit in den USA einen ähnlichen Prozess, ist aber schon weiter fortgeschritten. Präsident Clinton hat kürzlich eine hochrangige Kommission beauftragt, eine Analyse über die Verwundbarkeit des Staates zu erstellen und Wege zur Lösung der identifizierten Probleme aufzuzeigen.

Die Bedeutung des Information Warfare wird von den US-Streitkräften besonders betont. In seiner «Joint Vision 2010» führt der «Chairman of the Joint Chiefs of Staff» hinsichtlich der technologischen Entwicklung aus, dass technisch überlegene Ausrüstung auch weiterhin der Schlüssel für den Erfolg im Einsatz sein wird. Priorität wird in diesem Zusammenhang der Verknüpfung von Informationssystemen und der daraus erwachsenden Fähigkeit einer «dominant battlespace awareness» eingeräumt.

Besonderheiten des militärischen Nachrichtenwesens

Das militärische Nachrichtenwesen steht vor der Aufgabe, verfügbare Informationen durch intensive Analysen zu ergänzen, fehlende Teile gedanklich zu rekonstruieren und daraus entsprechende Schlüsse zu ziehen. Trotz des Einsatzes aller verfügbaren Datenverarbeitungstechnik bedarf es hier in besonderem Masse des Menschen, der als intelligenter Analytiker die verfügbare Information nicht nur sammeln, sondern auch vor allem bewerten muss, um anschliessend Schlussfolgerungen für zukünftiges Handeln zu ziehen. Schon heute ist es eines der Hauptprobleme, in der Fülle vorhandener Informationen die Daten zu finden, die gebraucht werden.

Der Golfkrieg liess hinsichtlich der Informationsfülle und ihrer Nutzung deutliche Schwächen des Nachrichtendienstes erkennen:
– Obwohl Informationen in einem nie gekannten Umfang bereitstanden, gelangten sie oft nicht zu dem, der sie benötigte. Der Nachrichtendienst bewährte sich zwar hervorragend in der Informationsgewinnung und -auswertung, versagte jedoch oft bei der bedarfsgerechten Verteilung ihrer Produkte. Die Truppe erstickte in einer Vielzahl von Detailinformationen.
– Information wurde zeitaufwendig und meist strikt nach Bedarfsträgern, d.h. nach Teilstreitkräften aufbereitet.
– Die einzelnen Teilstreitkräfte betrieben eine Unmenge meist nicht kompatibler Aufklärungssysteme. Es ging viel Zeit damit verloren, Informationen zwischen den Teilstreitkräften auszutauschen.

In der Informationsflut eines Information Warfare darf der Nachrichtendienst – aktiv und selektiv – nur genau die Information zum Bedarfsträger steuern, die dieser zu einem bestimmten Zeitpunkt an seinem momentanen Standort auch benötigt. Kritische Informationen müssen dabei sogar im Einzelfall innerhalb von Sekunden verfügbar sein.

Gleichzeitig hat der Nachrichtendienst – passiv – das Gesamtlagebild in Echtzeit auch für die unterste Führungsebene. Wichtig wird unter diesen Prämissen nicht mehr so sehr die Plattform sein, die eine Information einbringt, sondern wer diese Information erhält, wer sie nutzt.

In den USA ist man sich einig, dass dies völlig neue nachrichtendienstliche Strukturen erfordert, dass eine Quasi-Vernetzung aller Quellen und Sensoren unausweichlich wird. Alle nichtöffentlichen Informationsaspekte müssen zusammengefasst werden, offene Daten mit verschlüsselten Daten korreliert werden. Die Grenzen zwischen taktischer, strategischer und nationaler Aufklärung werden zunehmend verschwimmen.

Dem militärischen Nachrichtenwesen wird in verstärktem Masse eine Bewertung von gegnerischen Fähigkeiten abverlangt und immer weniger die Bereitstellung blosser Potentialvergleiche. Darüber hinaus wird es sich immer mehr der ganzheitlichen und ressortübergreifenden Analyse widmen müssen. Zielobjekte werden nicht länger nur Streitkräfte oder staatliche Strukturen sein, sondern darüber hinaus auch überstaatliche Institutionen, z.B. internationale Konzerne, organisierte Kriminalität und Terrorismus. Das militärische Nachrichtenwesen wird sich den grenzüberschreitenden und ressortübergreifenden Strukturen der Informationstechnologie anpassen müssen.

Viele der erforderlichen Mittel sind kommerziell ohne grossen Aufwand zu beschaffen, und der Fakt, dass sich das Land X vermehrt darum bemüht, bestimmte Computertechnologie zu beschaffen, deutet natürlich nicht darauf hin, dass hier eine zukünftige Quelle von Information Warfare zu erwarten ist.

Es gilt vielmehr zu definieren, welche Parameter für ein Information Warfare-Programm erforderlich sind und mögliche Indikatoren zu definieren, die auf ein solches Programm hindeuten könnten. Alle diese Indikatoren für sich allein dürften unverfänglich sein. Erst die Gesamtschau kann einen hinreichenden Eindruck vermitteln.

Zusammenfassung

- Unter Information Warfare werden eine Vielzahl von unterschiedlichen, teilweise militärischen Massnahmen sowie auch andere, teilweise kriminellen Massnahmen subsumiert, bei denen die besonderen Möglichkeiten der modernen Informations- und Kommunikationstechnologien genutzt werden.
- In einer Informationsgesellschaft kann es langfristig zu einer Veränderung des Kriegsbildes kommen. Es werden neue Akteure auftreten. Staatliche und wirtschaftliche Infrastrukturen bieten neue Möglichkeiten der Verwundbarkeit.
- Im militärischen Bereich gewinnt der Faktor Information zunehmend an Bedeutung gegenüber den traditionellen Faktoren Kräfte, Raum und Zeit und kann zum gewinnentscheidenden Faktor einer zukünftigen Auseinandersetzung werden.
- Die Hauptrisiken eines Information War werden von uns nicht im Bereiche der Streitkräfte gesehen. Moderne Staaten bieten mit ihrer zivilen Infrastruktur lukrativere Ziele.
- Wir sehen den Schutz gegen diese Risiken nicht als Hauptaufgabe der Streitkräfte. Es muss als gesamtstaatliche Aufgabe betrachtet werden, zu denen Streitkräfte ihren Beitrag zu leisten haben.
- Das militärische Nachrichtenwesen steht vor der Herausforderung, sich den grenzüberschreitenden und ressortübergreifenden Strukturen der Informationstechnologie anzupassen und aus der Informationsflut die Bedarfsträger optimal zu versorgen.

Kapitän zur See Niels Möller-Gulland (1945), ist Referatsleiter für «Militärstrategie und militärpolitische Konzeptionen» im Führungsstab der Streitkräfte des Bundesministeriums der Verteidigung in der Stabsabteilung III, die sich mit «Militärpolitik und Führung» befasst. Dieser Artikel basiert auf seinem am 20. September 1996 in Luzern vor der «Vereinigung Schweizerischer Nachrichtenoffiziere» (VSN) gehaltenen Vortrag. ■

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.

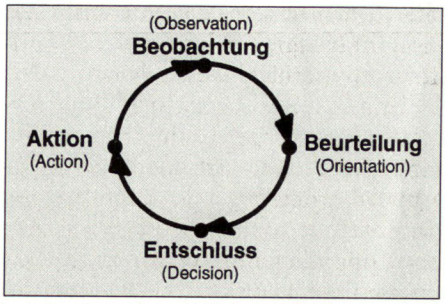


Abbildung 1: OODA-Zyklus.

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

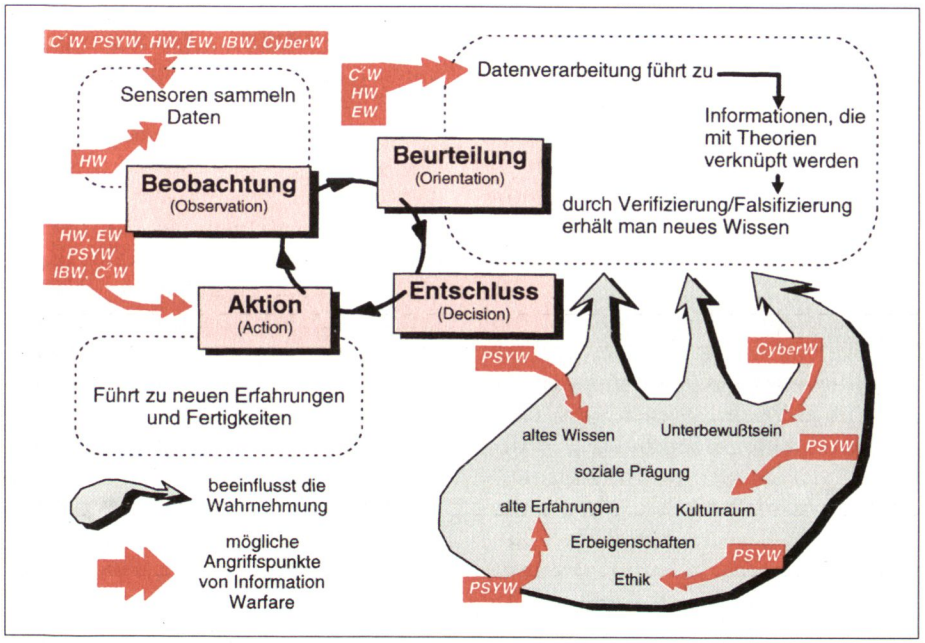


Abbildung 2: Entscheidungszyklus mit möglichen Ansatzpunkten von Information Warfare.

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

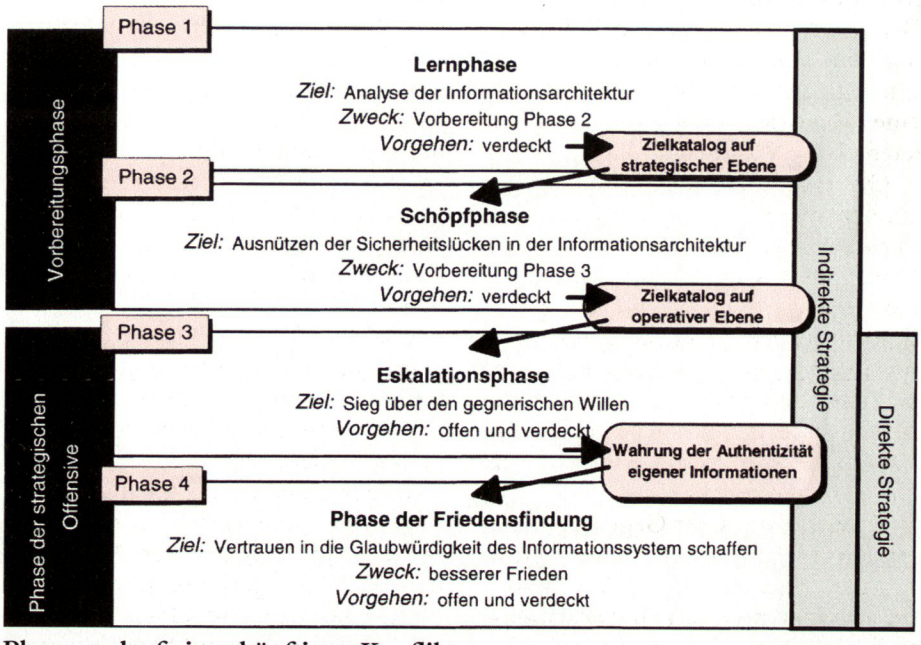
Erst in der Eskalationsphase wird zum offenen Vorgehen sowie zur direkten Strategie übergegangen. Je nach beabsichtigter Konfliktintensität reicht diese strategische Offensive von Dissuasion durch Androhung von Netwar über Erpressung, Terrorismus bis hin zum offenen Krieg mittels Cyberwar. Für diese 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. ■

Informationskonflikte sind Chefsache

Walter Altherr

Rückblickend hat Gutenbergs Buchdruck die Welt verändert – die Kirche verlor in der Folge das Informationsmonopol, und der Buchdruck förderte indirekt den Individualismus. Immer wieder haben neue Technologien unsere Kommunikationsformen erweitert und unsere Gesellschaft spürbar verändert. So kamen später das Telefon, der Radio und das Fernsehen hinzu – immer wieder standen wir vor der Frage, mit welchen gesellschaftlichen Auswirkungen zu rechnen ist. Wie werden Intelligenz, Wissen und Fähigkeiten des Individuums sowie des Kollektivs durch das neue Medium beeinflusst?

Neue Dimension der Wissensverbreitung

Heute befinden wir uns inmitten einer neuen Dimension der Wissensverbreitung: Noch nie zuvor hat sich nämlich das Wissen so rasch verändert, noch nie zuvor wurde das Wissen so breit gestreut und noch nie zuvor wurde so viel Energie in die Technologie der Wissensverbreitung gesteckt – sei es, um Informationen rasch und breit zu streuen oder sei es, um Informationen in eine überblickbare Menge zu filtern. So ist es durchaus sinnvoll, sich ein weiteres Mal zu fragen, welche Macht in diesen immer feiner verästelten elektronischen Medien liegt? Werden sich alle diese laufenden Veränderungen nur zum Guten hin wenden oder haben wir in Zukunft mit Bedrohungsformen zu rechnen, welche mittels dieser elektronischen Informationskanäle besonders gefördert werden? Müssen wir uns speziell auf die verschiedenen möglichen Facetten eines sogenannten Information Warfare vorbereiten? Wie anfällig sind wir bei Beschädigung der technischen Infrastruktur der einzelnen Medien oder gar militärischer, staatlicher oder wirtschaftlicher Führungssysteme? Wo liegen allenfalls Sicherheitslücken, die es zu stopfen gilt?

Können die neuen elektronischen Medien zur Störung der wirtschaftlichen oder der staatlichen Autonomie benutzt werden? Können staatliche Gebilde nicht bereits mittels psychologischer Manipulationen lähmend unter Druck gesetzt werden, und braucht es dann die traditionellen militärischen Eskalationsformen noch? Ist Information Warfare nicht auch ein geeignetes Mittel für sogenannte nichtstaatliche Organisationen, um ihre angestrebten Ziele zu erreichen? Welche Abwehrmassnahmen können getroffen werden und wie haben sich die staatlichen Führungsorgane in einer sich immer näher rückenden Welt in diesem Umfeld zu verhalten?

Zur Unterstützung der Relevanz dieser Fragen werfen wir kurz einen Blick zurück und überlegen uns: Was wäre der Zweite Weltkrieg gewesen ohne das Radio? Welche Rolle spielten die täglich für die amerikanischen Haushalte erstellten Berichte über die Lage in Vietnam? Wie wäre der Golfkrieg verlaufen ohne CNN?

Im folgenden beschränken wir uns bei unseren Überlegungen bewusst auf die nicht-kriegerischen Ausprägungen und somit auf jene Aspekte, die bereits heute denkbar sind. Zudem verzichten wir auch auf eine Vertiefung von kriminellen Aktivitäten, wie beispielsweise das Unwesen der Hakker. Allerdings können solche Aktivitäten wichtiger Bestandteil eines grösseren «elektronischen Angriffs» sein. Bevor wir uns aber mit dem eigentlichen Thema auseinandersetzen können, brauchen wir ein Verständnis hinsichtlich der aktuellen Entwicklungen bei den elektronischen Medien und dem zugehörigen Umfeld. Es muss uns klar werden, wie eng die heutigen Informationssysteme mit unserem täglichen Leben verzahnt sind.

Was verändert sich?

Seit Mitte der achtziger Jahre werden die weltweiten Informationskanäle durch den Ausbau öffentlich zugänglicher Netze im wahrsten Sinne des Wortes umgekrempelt. Der Standortbezug verliert dank der Leistungsfähigkeit dieser neuen Netze immer stärker an Bedeutung. Zeit- und Raumgefühl haben sich im Verlauf der letzten zehn Jahre dramatisch verändert – in der Informationswelt verlieren nationale Grenzen ihren Stellenwert; die Welt wird zum grossen Dorf.

Mit Internet und dem diese Infrastruktur nutzenden World Wide Web (WWW) hat sich eine neue Dimension der Kommunikationsform eröffnet: Die Interaktivität bei der Informationsbeschaffung und die Öffnung dieses Informationssystems unter Nutzung des Telefonnetzes bis hin in die privaten Haushalte. Jeder kann so leicht Informationen streuen und jeder kann so zum eigenen Nachrichtenoffizier werden. Was dadurch überhaupt alles in Bewegung geraten ist, zeigen die wichtigsten Entwicklungen auf.

Globalisierung der Märkte

Die Globalisierung der Märkte, die damit verbundenen grossen Fusionen von Unternehmungen verschiedenster Branchen entziehen sich der Einflussnahme staatlicher Organisationen und begrenzen den Handlungsspielraum der Staaten.

Neue Technologien wie Internet werden zum Motor dieser Entwicklungen: Die elektronischen Vernetzungsmöglichkeiten sowie die digitalen Arbeitsplätze bilden das Rückgrat für die Führbarkeit solcher riesiger Konglomerate. Diese Infrastruktur unterstützt die Fähigkeit der globalen Unternehmungen, um flexibel handeln und um ihr über die ganze Welt gestreutes Gebilde rasch umgruppieren zu können.

Electronic Commerce

Electronic Commerce ist ein weiteres Beispiel grenzüberschreitender Veränderungen: Diese Handelsform ermöglicht virtuelle Kundennähe – und zwar ungeachtet der Entfernung. Der räumliche Vorteil des Einzelhan-

dels wird dadurch vernichtet. Kleinere, kaum lebensfähige Märkte lassen sich umgekehrt auf dem elektronischen Weg bis hin zu einem tragfähigen Markt vergrössern. Die Hersteller können sich so von den Zwischenhändlern lösen und einen eigenen, direkten Vertriebskanal aufbauen. Die Kunden werden in Zukunft über diesen Verkaufskanal über sehr präzise Produkteinformationen verfügen.

Zur Zeit werden sichere Methoden für den Zahlungsverkehr eingeführt. Damit fällt eine wichtige Hürde weg, welche bisher den elektronischen Handel immer wieder verunsicherte.

Internet wird somit zunehmend zum wichtigen Instrument für geschäftliche Transaktionsabwicklungen. Dort wo elektronische Informationsprodukte gehandelt werden, entfallen zudem jegliche Grenzkontrollen – dies hat natürlich spürbare Auswirkungen auf die staatliche Autonomie.

Electronic Publishing

Die Wissenschaft – im übrigen die erste Nutzerin des Netzes überhaupt - tauscht in breitem Masse ihre Informationen und Forschungsresultate über diesen Kanal aus. Die Wissenschaft bewegt sich somit inmitten des Electronic Publishing – die zur Verfügung gestellten Informationen werden mittels den Techniken des WWW zudem noch untereinander vernetzbar. Wissen wird so wesentlich rascher, unkontrollierbarer und vor allem breiter gestreut als dies bisher via den Informationsträger Papier üblich war. Zudem erfolgt der Wissenstransfer dabei noch praktisch kostenlos.

Der elektronische Informationsträger Internet führt durch die wesentlich raschere Wissensverbreitung zur Verkürzung der Forschungszyklen an den Universitäten.

E-Mails

Die Ansprechbarkeit von Firmen und einzelnen über eine Internet-Adresse sowie die Nutzung von Internet zur Zustellung von E-Mails ist immer mehr zur Selbstverständlichkeit geworden.

Regierungen und, wenn zwar noch etwas zögernd auch Schulen, agieren ebenfalls auf dem Netz. So entstehen allmählich neue Kommunikations-, Lern- und Arbeitsformen: Aktive Diskussionsforen – mit wissenschaftlichen Zielsetzungen bis hin zu interaktiven Klatschecken – verbinden Menschen weit über die Kontinente hinweg. Es finden sich heute auch die unterschiedlichsten Formen der Selbstdarstellung im Netz.

Präsenz auf dem Internet gilt heute bei den meisten Unternehmungen als unverzichtbar. Zugleich schafft die grenzüberschreitende Vernetzung eine gemeinsame Sprache, damit die verschiedenen Informationsquellen auch genutzt werden – Kulturen wachsen über diese gemeinsame Sprache so enger zusammen.

Generation von Informationshungrigen

Eine Generation von Informationshungrigen beschafft sich über Internet regelmässig Informationen – sei es gezielt zu speziellen Themen oder dann auch eher zufällig von Informationshäppchen zu Informationshäppchen surfend.

Seit nun bald drei Jahren steht dieses Phänomen täglich im Brennpunkt aller Medien, welche laufend auf Neuheiten im universellen Informationspool hinweisen und entsprechend kommentieren. Die Journalisten nutzen Internet aber ebenfalls als Informationsquelle für ihre eigenen Bedürfnisse und wirken so indirekt beachtungsverstärkend. Personen und Gruppierungen, welche von bisherigen Medien ausgeschlossen waren, finden dadurch über Internet ihr sich für sie interessierendes Publikum.

Aufgrund dieser Entwicklungen drängen sich etliche Zeitungsverleger mit voller Kraft in das Internet und wehren sich so gegen branchenfremde Eindringlinge – ein prominenter Neuling in dieser Szene ist interessanterweise Microsoft.

Explodierende Informationsflut

Das Informationsgefäss Internet konfrontiert uns mit einer weiterhin explodierenden Informationsflut. Als Reaktion dazu werden neue Formen der Informationsbeschaffung entwickelt: Einzelne Informationsproduzenten beliefern beispielsweise ihre Abonnenten gemäss einem individuellen Profil per E-Mail mit den gewünschten Inhalten. Verlage erstellen so individualisierte Tageszeitungen.

Als Alternative dazu überwachen spezielle, selbständig agierende Programme, sogenannte Suchagenten, gemäss einem durch den Benutzer vorgegebenen Interessensprofil die Informationsflut und machen den Benutzer auf entsprechende Neuzugänge aufmerksam.

Die Beschaffung und Verarbeitung von Informationen wird zu einem Bestandteil unseres täglichen Lebens – dabei verschwinden auch aus dieser Sicht etwelche Grenzbarrieren.

Informationskanäle

Die verschiedenen Informationskanäle wachsen über die Verbreitungskabel immer enger zusammen. Wegen ihrer Leistungsfähigkeit gewinnen in letzter Zeit auch die TV-Kabelnetze für die Feinverteilung von Internet bis in die Haushalte an Bedeutung. Da die Telekommunikation weiterhin als ein finanziell sehr interessantes Betätigungsfeld betrachtet wird, findet ein äusserst harter Wettbewerbskampf statt, und somit ist auch in Zukunft mit technischen Leistungssteigerungen zu rechnen. Die privaten und geschäftlichen Kommunikationsformen werden sich auf diese neuen Möglichkeiten ausrichten: «Electronic Banking» und «Teleworking» über Internet sind entsprechende Beispiele.

Keine Technologie ohne Schattenseite

Das weltumspannende, öffentlich zugängliche Datennetz wird – dank dem hohen Beachtungswert wohl kaum überraschend – für partikuläre Interessen und immer wieder auch für kriminelle Handlungen – sei es Vandalismus, Datendiebstahl oder Piraterie - missbraucht.

Ein weiteres Spannungsfeld dieser Entwicklungen ist die sich abzeichnende soziale Kluft zwischen Informationsreichen und -armen.

Gesamtbeurteilung

- Die Unmittelbarkeit der heutigen elektronischen Kommunikationskanäle verändert Verständnis und Gewichtung der Information.
- Raum und Zeit werden bei der Informationsverbreitung in neuen Einheiten gemessen.

- Die Verfallszeiten der Informationen oder vielleicht besser der Nachrichten werden in der Medienwelt immer kürzer – es findet ein Hüpfen von Neuigkeit zu Neuigkeit statt.
- Die Informationsüberlastung ist ein zentrales Problem – Aufmerksamkeit wird vermehrt durch Kreativität, Bildbetonung und gezielte Ansprechung emotionaler Seiten erreicht.
- Die umfassende Digitalisierung der Informationen ermöglicht kaum mehr feststellbare Verfälschungen – reale und virtuelle Welten fliessen ineinander. Der Film «Forrest Gump» ist ein gutes Beispiel, wie solche Manipulationen möglich sind.

Dieses Umfeld ist nun die Plattform für Agitateure eines Information Warfare. In diesem Umfeld bewegen sich aber auch der Staat und die Wirtschaft. So mag es erstaunen, dass deren Repräsentanten das hohe Konfliktpotential nicht wahrhaben wollen.

Reales Bedrohungspotential

Die beiden treibenden Motoren CNN und Internet haben den elektronisch vernetzten Teil unserer Hemisphäre im wahrsten Sinne des Wortes zu einem weltumspannenden Dorf werden lassen. Lokale Ereignisse werden zum Welthappening gemacht. Ereignisse aus anderen Kontinenten, aus anderen Ländern werden mindestens mit demselben Interesse verfolgt wie das Geschehen im eigenen Umfeld. Wegen der wegfallenden Distanz führen die gegenwärtigen Kommunikationsmittel zum Zusammenprall der verschiedenen Kulturen und Mentalitäten. Die Vernetzung der Kommunikationskanäle erschweren lineare, rational geprägte Argumentationsketten – wir befinden uns in einem Prozess der Oberflächlichkeit. Ereignisse werden oft durch andere überholt und sofort zur Bedeutungslosigkeit entwertet.

Wir nehmen diese umfassenden Veränderungen zwar täglich wahr, stehen ihnen jedoch zurückhaltend und im Fall einer Bedrohung sogar wehrlos gegenüber. Das elektronische Wissen, die umfangreichen elektronischen Informationsflüsse sind zum etablierten und unverzichtbaren Bestandteil unseres täglichen Lebens geworden, und zwar sowohl für unsere Arbeitswelt als auch für unsere privaten Bedürfnisse.

- Die hohe Abhängigkeit von der elektronischen Infrastruktur könnte für terroristische Aktionen zum lohnenden Ziel werden, um dadurch auf Regierungen, Unternehmungen entsprechenden Druck auszuüben.
- Die zunehmende Leistungsfähigkeit der elektronischen Distributionskanäle könnte zu einer Verschiebung der Machtverhältnisse führen – einzelne Medien werden dabei an Gewicht verlieren.
- Bei der Kommunikation über die elektronischen Informationskanäle entsteht eine virtuelle Nähe und Unmittelbarkeit. Daher kann aus sicherer Distanz – und somit kaum greifbar – agiert werden.
- Das fein verästelte Internet zieht illegale Aktivitäten an, die unsere Gesellschaft nicht nur punktuell gefährden, sondern auch das ganze soziale Gefüge in Frage stellen können.

Und so fühlen wir uns hin und her getrieben zwischen den vorwiegend technologisch geprägten Euphorikern der Informationsgesellschaft und den die neuen Technologien ablehnenden Warnern.

Kommunikation – eine komplexe Interaktion

Kommunikation ist vielschichtig und beschränkt sich nicht nur auf die rein sachliche Aussage. Kommunikation bezweckt immer, eine Veränderung des Wissens oder des Verhaltens zu erreichen. Jede Information ist somit begleitet – ob direkt oder indirekt – von Aussagen über die Informationsquelle, über die beabsichtigte Einflussnahme auf die Informationsempfänger und über die Beziehung zwischen dem Informationslieferant und dem potentiellen Empfänger. In den meisten Fällen ist es – im Sinne eines Feedbacks – für den Informationslieferanten sehr wichtig zu erfahren, was seine verbreitete Information beim Empfänger auslöst. Mit dieser Reaktion kann die nächste Information gezielter gesendet werden.

Die Wahl des Kommunikationsmittels ist für den «Erfolg» oder «Misserfolg» einer Information entscheidend, denn jedes Informationsmedium verstärkt oder reduziert die emotionale Seite der Kommunikation und hat spezifische Eigenschaften bezüglich der verschiedenen Dialogformen.

Informationen stehen zudem immer in einem Kontext, der nicht in jedem Fall aus dem Sachinhalt der Information herausgelesen werden kann. Wie können wir beispielsweise entscheiden, ob die Aussage «Ich sehe rot!» auf eine etwas blumige Art auf einen Wutausbruch hinweist oder ob damit die Farbe eines vorbeifahrenden Autos gemeint ist? Dazu brauchen wir eben den Kontext. Daher ist auch leicht einzusehen, dass körpergebundene Kommunikationsformen – wie das Gespräch, die Diskussion oder der Vortrag - für den Informationsempfänger immer noch die idealste Form ist.

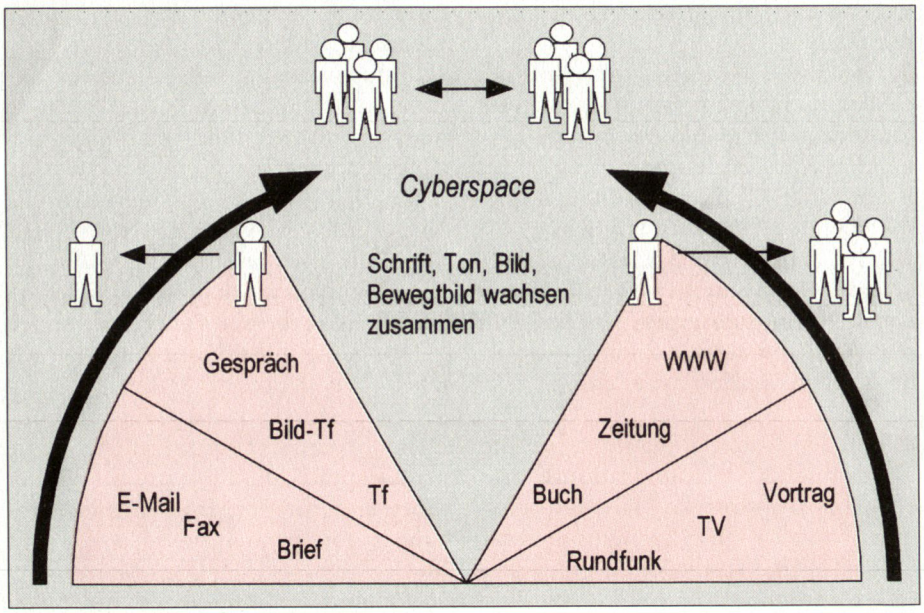
In einem unmittelbaren Gespräch ist den Beteiligten der Kontext, in dem Aussagen gemacht werden, implizit bekannt. Je nach Wahl des Kommunikationsmittels kann dieser Kontext jedoch verloren gehen, und er muss zur Klärung der Informationsaussage daher auf geeignete Form beigefügt werden. Genau hier – die kontextreduzierende Schwäche elektronischer Medien geschickt ausnutzend – liegt das Potential für entsprechende Manipulationen:

- Kontext kann künstlich beigefügt werden, um so die gewünschten Assoziationen auszulösen. Hier liegen die potentiellen Möglichkeiten für einen Information Warfare: Es gilt dabei, eine virtuelle Welt zu schaffen und mit geschickter Wahl Informationen – in einen emotionalen Kontext gestellt – über verschiedene elektronische Kommunikationskanäle zu streuen.

Betrachten wir die gegenwärtige Entwicklung, muss uns auffallen, dass mit den Kommunikationsformen, welche gegenwärtig im Internet entstehen, eine Entwicklung im Gange ist, die sich immer mehr der Form des direkten Gesprächs nähert – daher wird in diesem Zusammenhang vermehrt der Begriff «Cyberworld» verwendet.

Was sind die Bedrohungsformen?

Im beginnenden Informationszeitalter ist die Informationsverbreitung zum wertschöpfenden Geschäft geworden. Die Medienunternehmungen brauchen laufend neue Informations-



inhalte und sind daher für jedes Ereignis dankbar. Dieses Faktum kann durch geschickt geplante, schachspielähnliche Inszenierungen ausgenutzt werden: Kleine Gruppierungen können mittels des Multiplikationseffekts der Medien einen überproportionalen Beachtungswert erhalten.

Einzelne Könner beherrschen diese Informationskanäle bereits so perfekt, dass ihre Informationen zu emotionalen Botschaften werden, welche Massen bewegen und Staaten oder Unternehmungen in arge Bedrängnis bringen. Mit List und perfektem Timing werden Fakten mit plakativen Assoziationen zur Welt des Vertrauten zum eigenen Vorteil ausgenützt. Hier berühren sich Führen und Verführen.

Vorbei sind die Zeiten der Flugblätter abwerfenden Flugzeuge oder der freien Radiosender. Mit Internet und dem Satellitenfernsehen steht den verschiedenen Interessenvertretern heute ein kostengünstiges, über Distanz einsetzbares und viel direkter wirkendes Instrumentarium zur Verfügung. Beide Medien unterwandern das bisherige wohlkontrollierbare Monopol weniger Informationsproduzenten – eine Situation, mit der heute alle die Staatsautonomie schützenden Regierungen in unangenehmer Art und Weise konfrontiert werden. So waren es beispielsweise privat betriebene Internet-Anschlüsse, welche der Opposition in Bosnien und Serbien als Informationsnetz dienten.

Dieses Umfeld und diese Basis werden in Zukunft mit Sicherheit sowohl staatliche als auch nichtstaatliche Gruppen vermehrt zu zwielichtigen oder unberechtigten Manipulationen veranlassen. Vermeintliche Ungerechtigkeiten, vage Visionen werden vorerst einmal versuchsweise und ohne hohe Kosten in den virtuellen Raum gestellt, um Unternehmungen oder Nationen zu verändertem Verhalten oder zu bestimmten Aktivitäten zu veranlassen. Je nach Erfolg kann anschliessend der Druck verstärkt werden, und zwar mit einer unmittelbaren Reaktionsfähigkeit.

Neben der Gefahr der Manipulation der Meinungen ist auch mit unberechtigten Veränderungen an den elektronischen Informationen zu rechnen. Dabei handelt es sich um unberechtigtes Beschaffen, Erzeugen, Verändern oder Zerstören von Informationen – eben elektronischen Terrorismus. Das Arsenal reicht dabei von psychologischem bis zu handfestem Terror wie das zerstörerische Eindringen in sensitive Führungs- und Informationssysteme – da ist jede Eskalationsstufe denkbar und auch möglich.

Es ist damit zu rechnen, dass so territoriale oder wirtschaftliche Ziele erreicht werden können, ohne überhaupt zu den traditionellen Waffen greifen zu müssen – Cyberworld wird zur Plattform für Terrorismus.

Meinungsbeeinflussung bedeutet oft auch ein Bombardement mit Informationen, und es ist denn nicht erstaunlich, dass in diesem Zusammenhang die Metapher «Information Warfare» herbeigezogen wird. Diese Metapher ist allerdings auch etwas irreführend, da viele Aktivitäten, die wir als «Produkt» des Information Warfare verstehen, in absolut friedlichen Zeiten stattfinden: Die Abwehrmassnahmen obliegen somit nicht dem Militär, sondern zivilen Organisationen. Es ist deshalb wichtig, dass sich deren Vertreter entsprechend auf die neuartigen Bedrohungsformen vorbereiten.

Unsere Gesellschaft ist auf vier Ebenen – zugleich unsere historischen Entwicklungsphasen repräsentierend – verletzbar:

- auf der elementarsten Ebene – nämlich auf jener der Erde – wird unser eigenes Leben gefährdet;
- auf der Ebene des Territoriums kann die Autonomie des Staates bedrängt werden;
- auf der Ebene der Waren, welche sich über die Jahre vom Warenaustausch zum Industriezeitalter wandelte, steht der Verlust des Kapitals in Gefahr;
- und als Letztes fürchtet die Informationsgesellschaft auf der Ebene des Wissens den Ausschluss von neuen Erkenntnissen oder die Entwendung von Wissen.

Wird Information Warfare wirklich wahrgenommen?

Der Krieg ist das letzte Mittel zum Schutz des Territoriums. Denken und Verhalten einer Verteidigungsarmee im Kriegsfall sind auf die Erhaltung des Staates ausgerichtet – sei es zur Sicherung des territorialen Anspruchs oder dann auch nur zur Wahrung des Machtanspruchs der Herrschenden.

Information Warfare hingegen ist primär eine «Erfindung» des Wissens. Das Bedrohungspotential des Information Warfare ist somit auf den «höheren» Ebenen am intensivsten. Wird dies wirklich ernsthaft wahrgenommen?

Obwohl wir bereits einige Stufen der Entwicklung der Informationsgesellschaft hinter uns haben, sind wir mit diesen unfreundlichen Spielmöglichkeiten neuer Kommunikationsformen noch zu wenig vertraut.

Die Erfahrung lehrt uns jedoch, dass neben den zahlreichen unverzichtbaren Vorteilen dieser elektronischen Informationskanäle auch ein ernstzunehmendes Gefahrenpotential existiert, das es mit einiger Besorgnis zu analysieren gilt. Wir müssen lernen,

wie wir Manipulationsversuche aller Art verhindern oder – falls sie bereits im Gange sind – wirkungsvoll bekämpfen können.

Im Gegensatz zum Krieg, der primär auf die Beherrschung des Territoriums ausgerichtet ist und bei einer Eskalation Leben und Kapital gefährdet oder zerstört, zielen die verschiedenen Ausprägungen eines Information Warfare auf ein wesentlich breiteres Spektrum. Während bei einer kriegerischen Auseinandersetzung bereits in der Vorphase rein physisch die Konfliktsituation klar ersichtlich wird, wird Information Warfare viel verdeckter geführt. Oft muss erst erkannt werden, dass es sich um eine Ausprägung des Information Warfare handelt.

Konflikt unterhalb der Kriegsschwelle

Das Bedrohungspotential einer psychologischen oder wirtschaftlichen Kriegführung über das elektronische Netz wird in den staatlichen Führungskreisen stark unterschätzt – daher sind die Reaktionen in einer entsprechenden Konfliktsituation meistens wirkungslos.

Das Konfliktpotential wird sich in Zukunft auf die beiden Ebenen «Waren» und «Wissen» verlagern, da mit dem zunehmenden Wegfall der Grenzen die territoriale Bedeutung entsprechend reduziert wird. Information Warfare wird somit zur Schwächung der territorialen Wirtschaft oder zur Beherrschung von speziellem Wissen geführt werden – dies immer in einem Konfliktrahmen, welchen wir als «unter der Kriegsschwelle liegend» bezeichnen und somit keine unmittelbaren militärischen Aktionen erforderlich machen. Dies wird in den meisten Fällen auch gar nicht möglich sein, da bei diesen Konfliktformen ohnehin nur aus sicherer Entfernung gehandelt wird. So gesehen sind Staat und Wirtschaft gefordert, sich entsprechend auf solche Konfliktsituationen vorzubereiten. Es sind sowohl staatliche Entscheidungsträger sowie auch Wirtschaftsmanager auf diese Bedrohungsformen vorzubereiten.

Bei diesen auf der Informationsebene professionell geführten Angriffen dürfen weder Spontaneität noch Schweigen als wirkungsvolle Abwehrmassnahmen betrachtet werden. In solchen Auseinandersetzungen ist eine Kommunikationsstrategie unverzichtbar. Dies bedingt entsprechende Vorbereitungsmassnahmen und Planspiele, sonst wird es dem Informationsgegner, welcher sich immer als ernsthafter, verantwortungsbewusster und vertrauenswürdiger Kommunikationspartner maskiert, zu leicht gemacht.

In Zukunft gehört zur Wahrung der staatlichen Autonomie und der wirtschaftlichen Behauptung eben auch die Fähigkeit, sich in der Informationsgesellschaft durchsetzen zu können. Dies bedeutet nun aber nicht, dass sich entsprechende Gedankenspiele nur mit dem Reagieren auseinandersetzen. Die Vielfalt der Medien führt auch zu einer Zersplitterung der Beachtung. Informationsverantwortliche müssen lernen, sich in diesem Umfeld zu bewegen und sich die verschiedenen Kanäle offenzuhalten. Kurz gesagt: Es gilt, den Beachtungswert und die Vertrauenswürdigkeit der vorgesehenen eigenen Vertreter sorgfältig aufzubauen und zu pflegen. Nur so kann verhindert werden, dass es dem Gegner gelingt, durch geschickte Manipulation zusätzlichen Druck via der «Meinung von der Strasse» auszulösen.

Trojanisches Pferd?

Die modernen Informationstechnologien – allen voran die Informationstechnologien – haben uns zu Möglichkeiten geführt, die vor wenigen Jahrzehnten noch undenkbar waren. Mit den elektronischen, leicht zugänglichen Mitteln haben wir zudem ein wunderbares Kommunikationsinstrument geschaffen. Wissen wird breiter gestreut, soziale Bindungen werden über nationale Grenzen hinweg verstärkt. Die Entwicklung unserer politischen und wirtschaftlichen Räume in Richtung des sogenannten Cyberspace wird zu neuen Wirkungsformen führen. Wir alle profitieren täglich von den Errungenschaften der elektronischen Kommunikationsmöglichkeiten. Dies wird sich indirekt allerdings auch auf territoriale Autonomie- und Kapitalansprüche auswirken.

Hier besteht für die nächsten Jahrzehnte ein Konfliktpotential, welches vor allem mittels der Methoden und Techniken des sog. Information Warfare ausgetragen werden könnte.

Will die Wirtschaft und wollen die staatlichen Gefüge ihre Ansprüche weiterhin verteidigen, haben beide sich die entsprechende Kompetenz auf verschiedenen Ebenen anzueignen:

- So sind weiterhin alle technischen Massnahmen voranzutreiben, welche unberechtigtes Eindringen oder Zerstören unserer wirtschaftlichen, staatlichen und letztlich auch militärischen Informationsnetze verhindert.
- Die potentiell in solche Konflikte involvierten Personen haben sich mit den Eigenschaften der verschiedenen Informationsmedien und Informationsträger sowie mit deren Stärken und Schwächen vertraut zu machen.
- Entscheidungsträger haben sich auf solche mögliche Konfliktsituationen entsprechend vorzubereiten, denn ihr richtiges, vor allem glaubwürdiges Verhalten ist in den meisten Fällen zentral. Nur wenn diese Massnahmen ernsthaft getroffen werden und das Kommunikationswissen laufend nachgeführt wird, gelingt es Staat und Wirtschaft, ihre territoriale Eigenständigkeit auf friedlichem Weg zu wahren. Denn dann wird auch das territoriale Selbstbewusstsein ansprechbar, und dem Gegner aus Distanz wird es wesentlich schwerer gemacht, Mitläufer um sich zu scharen.

Es bleibt nur zu hoffen, dass sich die elektronische Vernetzung und die breite Streuung von Informationen nicht als Trojanisches Pferd erweisen. Es bleibt aber auch zu hoffen, dass wir die neuen Konfliktformen endlich in vollem Umfang ernst nehmen und entsprechend handeln. Die subtilen Methoden des Information Warfare stellen gegenwärtig eine weit höhere Bedrohung als das militärische Waffenarsenal dar. Staat und Wirtschaft, welche beide an unserer Autonomie interessiert sein müssten, haben hier eine wichtige Verantwortung zu übernehmen.

Dr. sc. techn. ETH Walter Altherr (1946), Fachoffizier und Vorstandsmitglied der VSN, hat 1989 mit dem Thema «Führungsinformationen in Krisenlagen – Aufgaben und Stellenwert EDV-geschützter Verfahren in der militärischen Führung» promoviert. Er ist verantwortlich für Informatikstrategien in Banken und Informationssystemen im Multimedia-Bereich. ■

Psychologische Kriegführung im Zweiten Weltkrieg

Toby E. Rodes

Major Toby E. Rodes war als Assistent von Generalmajor C. R. Powell verantwortlich für die operative psychologische Kriegführung der 12. US-Armeegruppe unter General Omar Bradley. Seine Aufgabe war die administrative Leitung des Stabes, die Kontrolle der deutschsprachigen Publikationen auf ihre Konformität zur von General Eisenhower bestimmten Politik sowie gelegentliche Teilnahme an Radiosendungen. Dort trat er, kraft seiner Sprachkenntnisse, als italienischer Offizier auf. Er landete wenige Tage nach Beginn der Invasion aus England kommend in der Normandie und blieb bis nach Kriegsende als Assistent des operativen Chefs der Informationskontrolle bis März 1946 in Deutschland. 1950 wurde er nach Deutschland zurückgerufen, zunächst als Presseoffizier des US-Kommandanten von Berlin, dann als Informationsoffizier des amerikanischen Marshall-Plans an der Botschaft der USA in Bonn.

Auftrag und Mittel

Der Auftrag der psychologischen Kriegführung war, ohne kriegerische Handlungen den Feind zu demoralisieren und zur Aufgabe zu veranlassen. Uns standen rund 1200 Mann und eine in England stationierte Bomberstaffel zur Verfügung. Je nach Lage wurden auch Artillerieeinheiten (105 cm) eingesetzt.

Die «PsyWar»-Truppe bestand aus drei «Mobil Radio Broadcasting Companies (MRB)», einer zentralen, mobilen Monitorstation und mobilen Druckereianlagen. Die MRBs verfügten über Lautsprecheranlagen, die grundsätzlich auf Jeeps montiert waren. Unsere damalige Technologie war neu, oft aber etwas handgestrickt. Unsere Radios waren noch mit Röhren bestückt - im Vergleich zur heutigen Technologie kann man den damaligen Stand als primitiv bezeichnen.

Produkte

- Flugblätter, die wir anstatt der Rauchkanister in 105er Geschosse steckten oder für die Flugstaffel in spezielle Kartonbomben. Die Zünder für beide waren so eingestellt, dass sie in zirka 100 m Höhe explodierten. (Als ehemaliger Artillerieoffizier war meine erste Aufgabe nach unserer Ankunft in England die Erarbeitung neuer Schiesstabellen für die 105er Kanonen.) Als wir uns dem Rhein näherten, setzten wir zusätzlich zu den Flugblättern eine Art von Feldpostzeitung ein.
- An geeigneten Positionen an der Front sprachen wir zu den deutschen Soldaten über Lautsprecher.
- Wir betrieben mobile Radiostationen sowie
- ab September 1945 Radio Luxemburg. (Die Briten verfügten über den «Soldatensender Calais» und die BBC.)

Glaubwürdigkeit

Unsere Kommunikation an die Adresse der deutschen Soldaten und der Zivilbevölkerung waren geprägt von der Überzeugung, dass wir eine über alle Zweifel erhabene Glaubwürdigkeit etablieren mussten.

Das gelang uns in hohem Mass und ermöglichte uns danach, in den letzten Monaten des Krieges mittels Falschmeldungen die deutsche Kriegführung zu Truppenbewegungen zu veranlassen, die uns – beispielsweise General Patton bei Nürnberg - einen unblutigen Vormarsch ermöglichten.

Unsere Produkte hatten wohl meistens sowohl eine taktische wie auch eine strategische Komponente. Die Zermürbung des Kampfgeistes der Truppe und des Durchhaltevermögens der Bevölkerung war die wichtigste strategische Komponente. Dabei war das erfolgreichste Produkte der «Passierschein» - ein Flugblatt, das wir in Millionenauflage verteilten. Es sicherte mit der faksimilierten Unterschrift von General Eisenhower dem Soldaten, der mit diesem Zettel in der Hand bei uns antrat, gemäss der Genfer Kriegsgefangenenkonvention zu, sofort von der Front in ein rückwärtiges geschütztes Lager interniert und dort gut verpflegt zu werden. Die meisten der zirka 2 Millionen Kriegsgefangenen, die auf das Konto der PsyWar-Aktivitäten gingen, hatten den Passierschein irgendwo im Stiefel oder am Körper versteckt – damit von Nazioffizieren erwischt zu werden, war lebensgefährlich.

Nachprüfbare Fakten

Unsere Glaubwürdigkeit erweckten wir durch Hinweise auf für die andere Seite nachprüfbare Fakten. Einige von uns hatten ständigen Zutritt zum Lageraum von General Bradley und wussten somit ständig genau, wo die Front momentan verlief. Wir hatten ebenso Zugang zum Auswerteraum der Luftwaffe, so dass wir anhand von Aufklärungsfotos den angerichteten Schaden genau lokalisieren konnten. Ausserdem hatten wir das Recht, jeden beliebigen Kriegsgefangenen auf dem Weg ins Lager, im Lager oder – bei hohen Offizieren – in einer unter unserem Schutz stehenden Villa zu befragen. Nachdem wir die deutsche Grenze überschritten hatten, machten wir Anti-Nazis ausfindig, die sich im Rheinland besonders gut auskannten. Nach einem Angriff zeigten wir diesen «freien Mitarbeitern» Aufklärungsfotos. Auf diese Weise erfuhren wir oft die Namen – manchmal auch noch weitere Details – von Besitzerfamilien der zerstörten Liegenschaften.

Solche Informationen nutzten wir anschliessend am Radio aus. Es ist verständlich, dass wenn wir am Radio der Familie X, deren Laden kaputt war, unser Mitgefühl aussprachen, alle Leute im Umkreis von Kilometern sicher waren, das wir nur über Tatsachen be-

richteten. Wenn wir in der gleichen Sendung dann behaupteten, an der Ostfront herrsche Aufbruch und Antikriegsstimmung, weil der Krieg dort so schlecht für Deutschland verlaufe, glaubte man uns auch trotz gegenteiliger Nazipropaganda.

Erfolgreiche Radiosendungen

Eine der erfolgreichsten Aktivitäten war das Radio 1212. Monatelang schalteten wir jeden Abend um Mitternacht Radio Luxemburg auf die Wellenlänge 1212, reduzierten die Sendeleistung und benahmen uns, als ob wir dissidente deutsche Offiziere innerhalb Deutschlands waren.

Die Glaubwürdigkeit etablierten wir mit einem in Metz erbeuteten «Hellschreiber», der bei allen deutschen Zeitungen und Radiostationen die Meldungen der Regierung und – vor allem – der Wehrmacht empfing.

Zu dieser Zeit durften deutsche Radiostationen nachts nicht senden, weil sie sonst unseren Bombern als Zielvorrichtung gedient hätten. Die Zeitungen erschienen erst am Morgen. Wir aber brachten das letzte Wehrmachtscommuniqué bereits um 00.30 Uhr oder 01.00 Uhr. Wer uns hörte, las dasselbe Communiqué am Morgen in der Zeitung und hörte es am deutschen Radio.

Anfänglich halfen uns diese Sendungen, die Truppen zu demoralisieren, später verfälschten wir Informationen über den Verlauf der Fronten und konnten so deutsche Truppen zu Bewegungen veranlassen, die sie sonst nicht unternommen hätten.

Neben dieser eher strategischen Operation fanden verschiedene eher taktische Aktionen statt. Beispielsweise als wir Lorient in der Bretagne umzingelt hatten und es belagerten – ohne zu schiessen, weil wir Menschenleben schonen wollten –, erfuhren wir durch einen Überlaufer die Namen von zwei auf deutsche Marineoffiziere und -unteroffiziere «spezialisierten» Prostituierten. Wir sendeten regelmässig Frontberichte über eine mobile Radiostation, welche wir vor die Stadt gestellt hatten und warnten nun die Besatzer, dass Fräulein X mit Sicherheit, Fräulein Y eventuell Syphilis hätten und dass wir über die notwendigen Medikamente verfügten, um eine Ansteckung zu heilen.

Die Deutschen litten offenbar sehr unter diesen Informationen. Wir registrierten anschliessend jedenfalls eine grössere Zahl an Überläufern …

Den Gegner kennen

Die absolute Notwendigkeit, die Kultur und den Charakter des Gegners zu kennen, zeigte sich verschiedentlich.

In Cherbourg hatte sich die deutsche Garnison in der Festung verschanzt. Wir hielten die Stadt. Die Deutschen mit Waffengewalt zu bezwingen, hätte in den engen Strassen ein sinnloses Blutbad angerichtet. Andererseits wollte der zuständige General keine Kampftruppen «zur Bewachung» abstellen.

Wir fuhren einen Kastenwagen mit Lautsprechern um die Ecke einer engen Strasse vor das Festungstor. Ein paar Gewehrschüsse wurden von den Deutschen auf den Wagen abgegeben. Der Teamchef blieb unbeirrt und begann, den Deutschen den Sachverhalt – Umzingelung, Front zig Kilometer weiter weg in Richtung Paris – über die Lautsprecher zu erklären und forderte sie auf, sich zu ergeben.

Der Wehrmachtsgeneral, der die Garnison befehligte, sandte nach einiger Zeit einen Offizier mit weisser Fahne, der unserem Major erklärte, der General könne der Ehre und des Reglements wegen sich und seine Leute nur übergeben, um diese vor dem sicheren Tod zu bewahren. Daraufhin wurde vereinbart, dass wir einen Panzer vor das Tor fahren würden.

Wir liessen einen Panzer auffahren. Die Deutschen hätten diesen, als er nach einigen Stunden um die Ecke bog, leicht zerstören können. Als der Panzer dem deutschen General gemeldet war, liess er seine Truppe im Festungshof aufmarschieren, das Tor öffnen und übergab seinen Säbel unserem Major, der ihn zeremonienhaft zurückgab. Dann marschierte die Truppe ab ins nächste Gefangenenlager.

Ähnliches geschah auf dem Weg nach Paris. Ein deutsches Bataillon sass auf einem Hügel, im Tal preschte – entgegen dem Befehl von General Eisenhower – General Leclerc mit seiner 2. Division (die einzige, die Frankreich noch hatte) vorbei und hätte die Deutschen bald im Rücken gehabt.

Wir sandten einen Lautsprecherwagen, der dem deutschen Oberst kund tat, dass sie umzingelt seien – was nicht ganz stimmte. Der Oberst aber wusste, dass der Krieg verloren war und wollte Menschenleben retten. Er sandte einen Parlamentär, der unseren Leuten erklärte, er könne und dürfe sich nur einer Übermacht ergeben.

Unser Leutnant beriet zusammen mit dem deutschen Offizier, was wir tun könnten, dass es nach einer Übermacht aussah. Es wurde festgestellt, dass das deutsche Bataillon nicht gegen Schwefelgas gewappnet war. Daraufhin zündeten unsere Leute ein paar Rauchkanister, die sie eilends besorgt hatten, und der Oberst führte sein Bataillon in die Gefangenschaft. Andererseits machten wir entlang der Front immer wieder die Erfahrung, dass wir nichts ausrichten konnten, wenn der Gegner zu Recht oder zu Unrecht überzeugt war, dass er gewinne.

Schlussfolgerungen

Aus diesen Erfahrungen lassen sich folgende Schlüsse ziehen, die auch heute meines Erachtens noch Gültigkeit haben:

- Das erste Ziel der psychologischen Kriegführung muss das Erreichen der Glaubwürdigkeit sein. Dazu benötigt werden kontinuierliche, auf den Moment genaue Lageinformationen sowie gründliche Recherchen und Kenntnis der Eigenart des Gegners.
- Wenn der Gegner das Gefühl hat, er sei am Gewinnen, sind taktische PsyWar-Massnahmen nutzlos.
- Strategische Massnahmen können helfen, die Aufnahme späterer, taktischer Kommunikationen etwas zu erleichtern.
- Eine subtile, objektiv erscheinende Ansprache ist doppelt so wirksam wie eine auftrumpfende selbstherrliche.
- Offiziere sind schwerer zu überzeugen als Soldaten.
- In einer negativen Situation ist der Feind am leichtesten mit PsyWar-Mitteln zur Aufgabe zu bewegen.
- Um sich gegen PsyWar-Angriffe zu schützen ist es unabdingbar, für eine gute Moral der Truppe zu sorgen und die Soldaten auf einem sie befriedigenden Informationsstand zu halten. Ein über Lage und Ziele mangelnd informierter Frontsoldat ist auf PsyWar-Informationen anfällig. ■