Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 163 (1997)

Heft: 12

Artikel: Information Warfare

Autor: Möller-Gulland, Niels

DOI: https://doi.org/10.5169/seals-64788

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. ■