VEREIN SICHERHEITSPOLITIK
UND WEHRWISSENSCHAFT

POSTFACH 65, 8024 ZÜRICH

Sicherheitspolitische Information

Herausgegeben vom Verein Sicherheitspolitik und Wehrwissenschaft (VSWW)
Postfach 65, 8024 Zürich (PC 80–500-4)

www.Chinfo.ch/vsww

Präsident: Dr. Günter Heuberger
Redaktion: Dr. Daniel Heller (heller@farner.ch)

April 2002

Information Age Conflicts

Neue Herausforderungen für die Sicherheitspolitik

Dr. Peter Forster und lic. phil. Myriam Dunn

Inhaltsverzeichnis

1. Einleitung: Gustav Däniker – Förderpreis zum 3. Mal verliehen

Die vorliegende Sicherheitspolitische Information gibt die anlässlich der 3. Verleihung des Gustav Däniker-Förderpreises gehaltenen Reden wieder. Nach der Laudatio von Dr. Peter Forster stellt die diesjährige Preisträgerin **lic. phil. Myriam A. Dunn (Zürich)** die Hauptergebnisse ihrer Arbeit vor und stellt auch einen Bezug zu aktuellen Fragestellungen der schweizerischen Sicherheitspolitik her.

Der Gustav Däniker-Förderpreis wurde aus Anlass des 70. Geburtstages von Divisionär Gustav Däniker von Farner PR und Consulting AG gestiftet, um mehrmals einen Preis für besondere Leistungen auf dem Gebiet der Erforschung der Sicherheitspolitik und der Wehrwissenschaften verleihen zu können. Mit dem Preis sollen vor allem akademische Nachwuchskräfte (Universitäten, ETH, Militärschulen) für erbrachte Leistungen oder herausragende publizistische Leistungen ausgezeichnet und zu weiteren Arbeiten ermuntert werden.

Der Preis konnte in den Jahren 2000 (Jan Metzger – «Die Milizarmee im klassischen Republikanismus») und 2001 (Daniel von Sprecher – «Generalstabschef Theophil Sprecher von Bernegg. Seine militärisch-politische Leistung unter besonderer Berücksichtigung der Neutralität» und Silvan Frick – «Neutralität in der GASP. Sicherheitspolitische Neudefinition in den EU-Staaten») an drei herausragende Arbeiten im Bereich der sicherheitspolitischen Forschung vergeben werden. Leider erlebte Gustav Däniker die Preisverleihung nur ein einziges Mal bevor er im Herbst 2000 unerwartet einem Leiden erlag. Mit dem Preis wird ein Beitrag dazu geleistet, dass seine Verdienste um die Belange der Sicherheits- und Militärpolitik präsent bleiben.

Dr. Daniel Heller, Geschäftsführer VSWW

2. Laudatio

Von Dr. Peter Forster[1], Salenstein

Ich freue mich darüber, dass die Jury eine Arbeit aus dem Gebiet der Information Operations auszeichnet. Die Informationsführung wird in Politik, Wirtschaft und Armeen immer noch wichtiger. Um so schwerer wiegt es, dass der Gustav-Däniker-Preis heute an eine Autorin verliehen wird, deren Studie die Information Operations in wissenschaftlicher Gründlichkeit ausleuchtet.

Es ist zudem eine Freude, Ihnen eine Autorin vorstellen zu dürfen, deren Studie im wahrsten Sinne des Wortes ausgezeichnet ist. In der Schweiz besteht Nachholbedarf in der wissenschaftlichen Aufarbeitung der Information Operations. Myriam Dunn legt eine Arbeit vor, die schon theoretisch einer kritischen Prüfung standhält. Sie leistet – darüber hinaus – aber auch einen Beitrag zur aktuellen Diskussion, nicht zuletzt zu den grundlegenden Definitionen und zur Auswertung der Informationsführung im Kosovo-Konflikt des Jahres 1999.

Myriam Dunn wurde 1976 in Zürich geboren. Von 1996 bis 2001 studierte sie Geschichte, Politologie und Völkerrecht an der Universität Zürich und ist seit 1999 Editor des International Relations and Security Networks (ISN) an der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse (FSK) an der ETH Zürich. Sie gehört zur Studiengruppe des Generalstabs, die unter Leitung von Major i Gst Gérald Vernez für die Armee XXI die Konzeptstudie *«Information Operations»* erstellt.[2]

---

[1] Dr. Peter Forster war langjähriger Chefredaktor der Thurgauer Zeitung, ist Verfasser militärwissenschaftlicher Werke und führt als Oberst das Informationsregiment 1.

[2] Seit diesem Jahr arbeitet Myriam Dunn an ihrer Dissertation über Interdependenzen in kritischer Informations-Infrastruktur. Sie entwickelt ein Modell, das komplexe Systeme in ihrer Vernetzung umfasst und spezifische Interdepenzen und Verwundbarkeiten von Informations-Infrastrukturen in einem modernen sicherheitspolitischen Umfeld abbildet. Seit Januar 2002 ist sie überdies wissenschaftliche Mitarbeiterin im Projekt «The Comprehensive Risk Analysis and Management Network (CRN)», das unter der Leitung des ersten Gustav-Däniker-Preisträgers Dr. Jan Metzger steht.

2.1 Information Warfare

Vor vier Jahren war der Begriff Information Warfare noch in aller Munde. Martin Libicki, Forscher an der amerikanischen National Defense University in Washington, schrieb 1998: *«Information Warfare definieren zu wollen, ist wie die Geschichte von den Blinden und dem Elefanten. Die Blinden wollten die Natur des Elefanten ergründen: Der eine berührte das Bein und nannte es einen Baum, der zweite griff an den Schwanz und nannte ihn ein Seil, und so weiter.»*

Ebenfalls 1998 hatte ich Freude, auf dem Lilienberg eine Diskussionsrunde zu leiten, an welcher zwei kenntnisreiche deutsche Fachleute teilnahmen: der damalige Generalmajor Walter Jertz, zu jener Zeit Kommandeur der deutschen 1. Luftwaffendivision (und kurz darauf, 1999, militärischer Sprecher der NATO), und Frau Dr. Elisabeth Hauschild, damals Bundeswehr-Dozentin für Information und Kommunikation an der entsprechenden Spezialschule in Strausberg. General Jertz und Frau Hauschild kreuzten die Klingen zur Frage: *«Kann gegen ein Dritt-Welt-Land eine Informationsoperation geführt werden?»* Jertz war der Meinung: *«Nein, das geht nicht».* Frau Hauschild vertrat die Position: *«Ja, das funktioniert sehr wohl».* Beide hatten – unter ihrer Definition von Information Warfare – recht.

Jertz verstand unter einer Information Operation eine Aktion auf dem Gebiet der angestammten Elektronischen Kriegführung und des neueren Hacker War. In der Tat kann eine derartige Aktion gegen ein hochvernetztes, auf Hacker-Angriffe anfälliges Land leichter geführt werden als gegen einen Dritt-Welt-Staat.

Frau Hauschild dagegen dachte an eine Operation im Sinne der Psychological Operations. Mit den angemessenen Mitteln kann eine solche Operation auch gegen ein unterentwickeltes, ja analphabetisches Land geführt werden.

Inzwischen sprechen wir – korrekterweise – nicht mehr von Information Warfare, sondern von Information Operations. Aber Definitionen gibt es immer noch wie Sand am Meer. Es ist deshalb verdienstvoll, dass Myriam Dunn in den einleitenden Kapiteln ihrer ausgezeichneten Arbeit die Umschreibungen noch einmal kritisch unter die Lupe nimmt. Sie setzt ein mit den wissenschaftlichen Annäherungen, wie sie Forscher wie Libicki, Winn Schwartau, Edward Waltz und Carlo Kopp vornehmen. Sie stellt den akademischen Approach den militärischen Definitionen gegenüber, wie sie vor allem von den amerikanischen Streitkräften gegeben werden.

Richtigerweise lässt Myriam Dunn die Definitionen so weit wie möglich offen. Einzig mit einer offenen Umschreibung lassen sich die Information Operations gedanklich erschliessen, und auch die *«Anwender»,* um diesen prosaischen Begriff für einmal zu gebrauchen, kommen nur dann weiter, wenn sie sich definitorisch nicht von Anfang an unnötig einengen.

Im zweiten Teil ihrer Arbeit untersucht Myriam Dunn kenntnisreich die Informationsführung der Kriegsparteien während der Operation *«Allied Force»* vom 24. März bis zum 10. Juni 1999. Der 78-tägige Kampf zwischen Serbien und dem Nordatlantikpakt war ein Schulbeispiel für das Ringen um Informationsdominanz in einem militärisch und politisch heiklen Umfeld.

Die NATO setzte unter amerikanischer Führung fast alle Mittel der Information Operations ein, angefangen von der physischen Zerstörung serbischer Radio- und Fernseh-Anlagen bis zum Einsatz von Flugblättern und der Spezialflugzeuge *«Commando Solo».* Wie Myriam Dunn schreibt, waren die amerikanischen Aktionen nicht sehr erfolgreich. Sie waren nicht so sorgfältig strukturiert und wurden nicht so *«einfühlsam»* durchgeführt wie – zum Beispiel – die Operationen während des Golfkrieges vom 16. Januar bis zum 28. Februar 1991, welche vom 2. August 1990 an gründlich geplant worden waren (und Erfolg hatten).

In einem zentralen Abschnitt hält Myriam Dunn fest, dass Serbien die Auseinandersetzung militärisch nicht gewinnen konnte. Slobodan Milosevic hatte nur eine Erfolgschance: Er

konnte versuchen, den Zusammenhalt in der atlantischen Gemeinschaft aufzubrechen, und das wiederum konnte nur im Medien- und Propagandakrieg erfolgen. Auch wenn es Milosevic nicht gelang, die Allianz zu spalten, führten seine Operationen doch zu Spannungen im NATO-Lager.

Nach der lesenswerten Fallstudie zu 1999 unterzieht Myriam Dunn fünf eigene Theoreme einer kritischen Überprüfung (vgl. dazu den 2. Teil der vorliegenden Sicherheitspolitischen Information).

2.2 Informationsoperationen: Wahrhaftigkeit, Sachlichkeit und Objektivität als Leitlinien

Lassen Sie mich zum Schluss – ausgehend von den fünf Theoremen – noch ein paar eigene Gedanken zur Situation in der Schweiz anfügen. Ich halte Myriam Dunns international gehaltene Thesen für allgemein richtig und – cum grano salis – auch für unser Land gültig.

Ich bin – erstens – der Meinung, dass sich auch die Schweiz dem Phänomen der Information Operations nicht entziehen kann. Die Schweiz ist keine Insel. Gerade auf dem Gebiet der Informationsoperationen nimmt die Bedeutung traditioneller Grenzen ab. Im modernen Informationskrieg schützen Grenzen nicht mehr. Und die Frage stellt sich: Wie stark sind unsere digitalen (und psychologischen) Abwehrlinien aufgebaut?

Ich bin deshalb – zweitens – sehr dankbar dafür, dass nun im Generalstab die Information Operations in aller Gründlichkeit angegangen werden. Die entsprechende Projektgruppe, der Myriam Dunn – wie gesagt – angehört, hat ihre erste Studie mit generalstäblerischer Präzision abgeschlossen und erstellt nun ein umfassendes Bedrohungsbild.

Dieses Bild und die Konsequenzen, die daraus zu entwickeln sind, haben – drittens – interdisziplinär zu sein. Gärtchendenken ist auf dem Gebiet der Informationsoperationen keinesfalls am Platz. Von den Chancen und Risiken sind Staat, Wirtschaft und Gesellschaft gleichermassen betroffen. Nur die Zusammenarbeit von politischer Führung, Verwaltung, Unternehmen und Armee verspricht auf diesem sensiblen Gebiet Erfolg.

Und viertens muss jeder Einsatz auch im Sektor der Informationsoperationen von einer inhaltlichen, einer moralischen Grundhaltung getragen sein. Diese kann sich meines Erachtens nur an den Grundsätzen der Wahrhaftigkeit, der Sachlichkeit und Objektivität ausrichten. Die amerikanische Informationsführung unterscheidet weisse, schwarze und neuerdings sogar graue Operationen. Wer derartige Operationen führt, muss wissen, in welchem Bereich er operiert. Im demokratisch verfassten, liberalen Rechtsstaat kann dies nach meiner Überzeugung nur ein Bereich sein, der auch ethisch hohen Kriterien standhält.

3 Information Age Conflicts und Information Assurance

Von lic. phil. Myriam A. Dunn, Zürich

3.1 Gegenstand der Arbeit «Information Age Conflicts»

Die Arbeit *«Information Age Conflicts: A Study on the Information Revolution and a Changing International Operating Environment as Experienced in Kosovo»* untersucht eine neue, erst in Ansätzen erkennbare Form von Krieg, für den der Begriff «Information Age Conflict» (IAC) entwickelt wurde. Diese IACs finden in einem internationalen Umfeld statt, welches noch andauernden Veränderungen durch die sogenannte Informationsrevolution unterworfen ist. IACs werden mit dem Ziel durchgeführt, gemäss entstehender Doktrin im Bereich der Information Operations (InfOps) Überlegenheit im Informationsbereich (Information Superiority) über den Gegner zu erlangen.

Hindernisse für die Analyse von Information Operations im akademischen Umfeld

Die Auseinandersetzung mit der Informationskriegsführung findet heute fast ausschliesslich in amerikanischen Militärakademien und Regierungsberatungsstellen statt. Es besteht ganz allgemein grosser Nachholbedarf in der wissenschaftlichen Aufarbeitung der Thematik, vor allem ausserhalb des rein militärischen Kontextes und in Bezug auf Implikationen für Staat, Politik und Gesellschaft. Dass sich z.B. im Fachbereich Politikwissenschaft noch nicht einmal ansatzweise eine Forschungsgrundlage herausgebildet hat, liegt nicht an mangelnder Relevanz des Themas. Vielmehr ist dieses Defizit darauf zurückzuführen, dass die Beschäftigung mit der Themenstellung einen breit gefächerten und teilweise multidisziplinären Ansatz erfordert, welcher an Forschungsstätten in In- und Ausland einen schwierigen Stand hat und selten gefördert wird. Dass solche Arbeiten dennoch entstehen können, ist auf die Offenheit vereinzelter leitender Akademiker zurückzuführen. Die hier besprochene Arbeit vermag dank einer solchen Chance in einem politikwissenschaftlichen Rahmen eine Diskussion anzureissen und analytisch einem Thema nachzugehen, welches sicherheitspolitisch immer mehr an Bedeutung gewinnt.

Forschungsinteresse: Entscheidende Faktoren für Erfolg oder Misserfolg in IACs

Die Arbeit zielt auf eine Analyse der Dynamik von Konflikten in einem durch die Informationsrevolution gewandelten internationalen Umfeld. Im Zentrum des Forschungsinteresses steht dabei die Frage nach den Faktoren, die das Management und die Führung von *«Information Age Conflicts»* ausschlaggebend bestimmen, d.h. entscheidend für Erfolg oder Misserfolg im Umgang mit IACs sind. Im Rahmen einer qualitativen Fallstudie wird untersucht, ob und inwieweit ein kausaler Zusammenhang zwischen strukturellen Veränderungen des internationalen Systems und dem Ausmass des Erfolgs bzw. Nichterfolgs in IACs empirisch nachgewiesen werden kann. Als Fallbeispiel dient die *«Operation Allied Force»* der NATO in Kosovo, die sich neben dem physischen Raum vermehrt im virtuellen Raum der Information abspielte.

Die fünf Theoreme der Informationsrevolution

Um diese Faktoren bestimmen zu können, stützt sich die Arbeit auf fünf Theoreme, die aus einer Diskussion der theoretischen Fragmente und Konzepte abgeleitet werden, die sich mit den politischen, wirtschaftlichen, sozialen und militärischen Auswirkungen der Informationsrevolution auf die Strukturen und Prozesse der internationalen Beziehungen auseinandersetzen. Es handelt sich dabei um neue, ausschliesslich amerikanische Forschungsansätze der sogenannten *«Dritten Welle»* Literatur (Third Wave), um Ansätze von Modernisten (Modernization Writers) und um militärische Untersuchungen im Themenbereich der Revolution in Military Affairs. Grösstenteils sind diese Konzepte der späten neunziger Jahre stark von

der damaligen Euphorie geprägt und neigen in ihrem Glauben an absolut umwälzende Ereignisse oftmals zu übertriebenen Aussagen; dennoch lassen sich bei vorsichtiger Abwägung Denktrends oder Paradigmen herausarbeiten, welche das Informationszeitalter zu prägen scheinen. Im Zentrum steht dabei die Beobachtung, dass Machtstrukturen, Machtverteilung und ganz zentral Machtkonzept und -verständnis im internationalen System neu überdacht werden müssen. Die Arbeit konzentriert sich dabei hauptsächlich auf die Folgen der Veränderungsprozesse im militärischen Bereich.

In verknappter Form handelt es sich bei den fünf Theoremen um die folgenden:

№ 1: Im entstehenden Operationsumfeld wird die Dominanz in der Informationsdomäne (Information Superiority) über den Gegner als Schlüssel zum Erfolg bewertet;

№ 2: Asymmetrische Glaubwürdigkeit (Asymmetrical credibility) wird zur dominierenden Machtressource;

№ 3: Grenzen zwischen Staaten, zwischen dem militärischen respektive dem politischen Raum sowie zwischen dem militärischen und dem zivilen Raum werden im Informationszeitalter zusehends unschärfer;

№ 4: Zentralisierte hierarchische Organisationsformen verlieren an Einfluss gegenüber dezentralisierten flachen Strukturen und «virtuellen» Teams;

№ 5: Mittel der Asymmetrie triumphieren über diejenigen der traditionell dominanten Machtinstitutionen; *«kleine Fische»* können traditionell Stärkere einfacher schädigen.

Diese Theoreme erlauben die schrittweise Formulierung eines eigenen Modells und eine Reihe von Hypothesen, auf welche aus Platzgründen nicht im Detail eingegangen wird. Dabei wird beachtet, dass die erfolgreiche Führung von IACs nicht nur von strukturellen Faktoren abhängig ist (wie asymmetrische Bedrohung; sich verwischende Grenzen; und der Multiplikation relevanter Akteure) sondern auch von exogenen Faktoren (wie Wetter; Terrain; Entwicklungsstand der Technologie; und Doktrinentwicklung).

3.2 Hauptergebnisse und Fazit der Studie

Die Beschreibung und Bewertung der *«Operation Allied Force»* erfolgt in zwei methodischen Schritten. Im ersten werden den Variablen des Modells Werte zugewiesen, wobei insbesondere die Analyse der aktuellen amerikanischen Doktrinpapiere zum Thema «Information Warfare / Information Operations» und die Darstellung der durchgeführten InfOps im Rahmen der Luftkriegführung der Nato breiten Raum einnehmen. Im zweiten Schritt erfolgt dann der Test der eingangs formulierten Hypothesen mittels sogenannter «*congruence procedure»* sowie *«process tracing».*

Als Faktoren, die einen negativen Einfluss auf das Management und die Führung von *«Information Age Conflicts»* haben, werden dabei identifiziert:

Starker negativer Einfluss:

– Asymmetrische Bedrohung,

– Wetter, Terrain und mangelhafte Technologie,

– sich verwischende Grenzen zwischen militärischem und politischem Raum.

Geringer negativer Einfluss:

– Mangelnde Glaubwürdigkeit,

– Multiplikation der Akteure im internationalen Umfeld.

Nicht bestätigt wird hingegen der Einfluss von sich verwischenden Grenzen zwischen militärischem und zivilem Raum auf Erfolg in IACs. Dies lässt sich einfach damit erklären, dass die

Verwischung dieser Grenze eher ein Produkt der InfOps-Handlungen selber ist und so nicht als aktive Variable auf Management und Führung von IACs einwirken kann. Diese Variable ist aber umso bedeutender, wenn man die Implikationen von InfOps für die Gesellschaft darlegen möchte.

Theoreme werden in Frage gestellt

Mit Blick auf die breiteren theoretischen Überlegungen, die den Ausgangspunkt der Arbeit bilden, muss die Arbeit einige der zentralen Annahmen der Informationsrevolutions-Literatur in Zweifel ziehen. Bestätigt wurde zwar, dass Information Superiority einer der Schlüsselfaktoren für die erfolgreiche Führung von Konflikten im Informationszeitalter ist, wobei verhältnismässig kleine Akteure unter Verfolgung asymmetrischer Strategien grosse Akteure ausmanövrieren können. Allerdings scheinen die traditionellen militärischen Machtmittel weiterhin eine zentrale Machtressource zu bilden, auch wenn ihre Bedeutung in der Literatur unter dem Hinweis auf das Konstrukt der Asymmetrical Credibility als abnehmend eingestuft wird. Dies heisst nun aber wiederum nicht, dass die theoretischen Annahmen zur Neuverteilung von Macht im internationalen System gänzlich hinfällig werden: Erstens befinden wir uns in einer Übergangsperiode mit unklarem Ausgang und zweitens werden die Resultate der Veränderungsprozesse widersprüchlicher und weniger explizit ausfallen, als sich dies die wissenschaftliche Theorie wünschen würde. Die Mehrheit der Aussagen ist also weiterhin mit grosser Vorsichtig zu geniessen und regelmässig sorgfältig zu prüfen.

Zivilbevölkerung als mögliches Hauptziel zukünftiger Informationskriege

Abgesehen von den identifizierten Faktoren, auf welche Entscheidungsträger besonders achten sollten, ergeben sich aus der Analyse eine Reihe von Gedanken in Bezug auf die breiteren Auswirkungen der Informationskriegsführung vor allem für die Zivilbevölkerung. Das Beispiel Operation Allied Force zeigt, dass weder die Nato noch die USA gegenwärtig in der Lage sind, den vielschichtigen Informationskrieg gewinnen zu können, wie ihn die USA in ihren neuesten Doktrinpapieren umreissen. Dies liegt teilweise an Unzulänglichkeiten auf der Ebene der Doktrinbildung, teilweise an der schlechten Umsetzung von bestehenden Konzepten, aber hauptsächlich an den noch existierenden *«second wave»* Organisationsformen. Grundsätzlich ist die Neuausrichtung der Streitkräfte, die die Revolution in Military Affairs möglich macht, in der Theorie entworfen; bis anhin wurden die neuen Ideen jedoch noch nicht genügend umgesetzt.

Gleichzeitig entwickeln konventionell unterlegene Gegner als Reaktion auf *«virtuell»* anmutende, von aktuellen Kriegsschauplätzen abgekoppelte, ferngesteuerte Kriegshandlungen moderner Hightech-Truppen vermehrt asymmetrische Formen der Kriegsführung auf sub- oder supranationaler Ebene. Die heute den Truppen zur Verfügung stehenden Mittel sind trotz neuer Denkansätze nur sehr beschränkt geeignet, um den Herausforderungen dieser asymmetrischen Strategien und Taktiken entgegenzutreten. In Hinblick auf zukünftige Konflikte ist es daher wahrscheinlich, dass es zu einer verstärkten Entwicklung in Richtung Fourth Generation of Warfare kommt. Das Konzept besagt, dass zunehmend ganze Gesellschaften in Kriegshandlungen einbezogen werden und dabei die Unterscheidung zwischen zivil und militärisch vollständig verschwindet. Interessanterweise ist es aber nicht nur die unterlegene Seite, welche durch asymmetrische Kriegsführung eine solche Entwicklung beschleunigen könnte; die heute existierenden InfOps-Konzepte beinhalten ebenfalls eine Reihe von Ansätzen, welche zivile Ziele auf der physischen, psychischen und Cyberebene in Erwägung ziehen.

Diese Entwicklung hin zu gewolltem Einbezug ziviler Installationen sowie verstärkte Ausrichtung auf Täuschung ganzer Gesellschaften gibt zu Besorgnis Anlass. Gewisse Aspekte der Informationskriegsführung drohen den Kriegsschauplatz zu Domänen zu erweitern, wo er

nichts zu suchen hat. Da gewisse InfOps immerwährend, d.h. auch in Friedenszeiten und unterhalb der Konfliktschwelle, durchgeführt werden, verwischen sich nicht nur die Grenzen zwischen zivil und militärisch, sondern auch jene zwischen Krieg und Frieden. Durch diese Veränderungen in Raum und Zeit zukünftiger Kriegshandlungen ergeben sich neue Herausforderungen für den Schutz der Zivilbevölkerung und der zivilen Installationen.

Information Assurance als Herausforderung für die Sicherheitspolitik

Der Fokus der Arbeit ist zwar generell und international gehalten, die aufgeführten Gedanken gelten aber auch für die Schweiz. Die Natur der Information Operations ist absolut grenzübergreifend, so wie es die globalen Datennetze sind, in welchen ein Teil der Informationskriegsführung stattfinden könnte. Für die Schweiz und viele andere Staaten ist in diesem Bereich jedoch nicht hauptsächlich der offensive Aspekt von InfOps von Bedeutung, sondern vor allem der defensive Gesichtspunkt. Dabei geht es um mehr als nur sog. Defensive Information Operations, welche im Kriegs- oder Krisenfall gegen die ganze Palette von offensiven InfOps wirksam sein müssen und neben Cyberattacken auch physische und psychologische Komponenten umfassen. Anzustreben ist vielmehr der breitere Ansatz der Information Assurance, welcher über die Zuständigkeit und Aufgabe des Militärs hinausgeht. Information Assurance vereint Staat und Privatwirtschaft im fortwährenden Kampf gegen eine ganze Palette von Vorkommnissen, welche katastrophale Auswirkungen auf die Informationsinfrastruktur unseres Landes haben könnten.

Unter dem Schlagwort Critical Information Infrastructure Protection (CIIP) hat die Thematik seit einigen Jahren ausgehend von den USA auch in Europa und der Schweiz Einzug in die (sicherheits-)politische Diskussion gehalten. Dabei geht es um den Schutz des Sektors Information und Kommunikation, aber auch um die Totalität der vernetzten Computer, welche für das Funktionieren aller Infrastrukturen notwendig ist. Weiter stehen die Datenflüsse, welche in diesen Netzwerken transportiert werden, im Zentrum des Schutzinteresses und, ganz zentral, die Dienstleistungen, welche diese Infrastrukturen ermöglichen.

Die neuen Verwundbarkeiten der Informationsgesellschaft

Die Informationsgesellschaft ist beträchtlich vernetzt und befindet sich dabei in grosser Abhängigkeit von Informationstechnologien und Software- und Hardwaresystemen. Durch diese Abhängigkeit von hoch komplexen Systemen, die wesentliche Grundlagen sind für jene *«kritischen»* Infrastrukturen, welche für ein reibungsloses Funktionieren unserer Gesellschaft notwendig sind, wird die Informationsgesellschaft zur verletzlichen «Risikogesellschaft». Dabei sind InfOps nur ein Teilaspekt des Gefährdungspotentials dieser Infrastrukturen.

Die neuen Verwundbarkeiten der Informationsgesellschaft sind schwierig zu erfassen. Vor allem können Bedrohungen heute nur mehr sehr ungenau in die drei Dimensionen Akteur, Absichten und Möglichkeiten kategorisiert werden, was eine ganze Reihe von Problemen für die Erfassung und das Verständnis von modernen Risiken nach sich zieht. Das Spektrum möglicher Angreifer ist weit gespannt und reicht vom verärgerten oder unzufriedenen Mitarbeiter über Industriespione, organisiertes Verbrechen, Fanatiker, Terroreinheiten bis hin zu feindlichen Staaten. Das Spektrum der Angriffsoptionen reicht von Hackerangriffen bis zur gezielten Störung oder Zerstörung ziviler oder militärischer Einrichtungen. So könnten einzelne Komponenten von InfOps auch von nichtstaatlichen Akteuren durchgeführt werden, eventuell auch konzertierte und mit strategischen Absichten vollführte Aktionen, welche durch ihre Aktionen einen Grossteil der gesamten InfOps-Palette abdecken. Im Ernstfall ist die Einschätzung von Gefahren und somit das zeitgerechte Einleiten von Massnahmen oder Gegenschlägen also ungemein schwierig geworden.

Der unbestimmte Charakter neuer Gefahren
Tatsächlich ist die Definition von Schwellenwerten in Bezug auf die Zuständigkeit im Falle eines Angriffs eines der Hauptprobleme im Themenkomplex. Der unbestimmte Charakter dieser neuen Gefahren trägt nämlich dazu bei, dass die Grenzen zwischen innerer und äusserer Sicherheit und so zwischen Aufgaben der Streitkräfte und jenen für die innere Sicherheit immer schwieriger auszumachen sind, ja sogar eine neue Aufgabendefinition und Aufgabenverteilung erforderlich scheinen.

Die Schwierigkeit, mit territorial nicht mehr begrenzten und auf keine identifizierbaren Akteure mehr festlegbaren Bedrohungen umzugehen, werfen grundlegende Fragen über Kompetenzaufteilungen und politische sowie technische Strategien auf. Zusätzliche Unsicherheiten bewirkt die unklare nationale und internationale Rechtsgrundlage im Bereich der InfOps im speziellen und der Cyberrisiken im allgemeinen; so auch erkannt von der Rechtsabteilung des Pentagon, welche zu Zeiten des Kosovokonflikts vor völkerrechtlichen Konsequenzen warnte, falls die US-Streitkräfte digitale Angriffe auf andere Staaten durchführen würden.

Kernaspekte einer Politik zum Schutz kritischer Informationsinfrastrukturen
Obwohl vor allem in den USA die Debatte vorerst stark militärstrategisch ausgerichtet war – sie ist dabei eng verknüpft mit der Entwicklung von Information-Warfare-Ideen: Je weiter die Diskussion über Angriffe auf die Informationssysteme möglicher Gegner voranschritt, desto intensiver wurden mögliche Gefahren der eigenen militärischen und zivilen Datennetze thematisiert – wird das Thema heute überall interdepartemental angegangen. Allen bis jetzt bestehenden nationalen und internationalen Initiativen im Bereich des CIIP ist die Anlage eines Kooperationsprogramms gemein, welches möglichst viele Zuständige und allenfalls Betroffene zusammenführt. Als entscheidend für den Erfolg werden Partnerschaften zwischen dem Staat und dem privaten Sektor eingeschätzt. Dabei wird dem Faktum Rechnung getragen, dass Einzelmassnahmen auf der technischen Ebene heute nicht ausreichen, um gegen massive und konzertierte Cyberattacken mit kriegerischer bzw. terroristischer Absicht gewappnet zu sein und dass sich heute die Mehrheit der Informationsinfrastrukturen in den Händen von Privaten befindet.

Um den Schutz gegen Gefahren und Risiken im *«normalen»* Rahmen – dazu gehören neben Hackerangriffen auch kleinere natürliche Katastrophen – muss der Infrastrukturbetreiber selber bemüht sein. Vom Staat hingegen wird erwartet, dass er Schutz gegen Gefahren einer höheren Stufe bieten kann, wie zum Beispiel Angriffe von Terroristen und anderen Staaten. Hier ist die Rolle des Militärs in der Führung von Defensive Information Operations als Teil der Informationssicherung zentral. Das primäre Schutzziel ist dabei nicht in erster Linie der Schutz von Objekten der Informationsinfrastruktur, sondern hauptsächlich die Robustheit kritischer Dienstleistungen. Dabei muss die langfristige Überlebensfähigkeit aller relevanten Netzwerke gewährleistet werden, also die Sicherung eines robusten CIIP-Gesamtsystems: Unterbrüche der Dienstleistungen, welche diese Infrastrukturen ermöglichen, müssen von kurzer Dauer und schnell behebbar sein. Dies stellt zu jeder Zeit hohe Anforderungen an die interdepartementale Zusammenarbeit und die Koordination zwischen öffentlichem und privatem Sektor.

Herausforderungen für die Forschung
Damit eine umfassende Schutzpolitik formuliert werden kann, ist nicht nur die Zusammenarbeit zwischen Privatwirtschaft und Regierung unerlässlich, sondern auch internationale Koalitionen in Politik und Forschung. Die Sicherheit von Infrastrukturen ist zu einem wichtigen Aktionsfeld politischen Handelns geworden. Dabei müssen wir unsere Fähigkeiten verbessern, um die Absichten zur Ausnutzung der Informationstechnik für feindliche und demokratiegefährdende Aktionen zu erkennen, zu beurteilen, zu verhindern, und wenn nötig, zu bekämpfen.

Dabei kommt insbesondere auf die Forschung in der nächsten Zeit eine Reihe von Herausforderungen zu.

Man ist heute nicht nur in der Schweiz weit davon entfernt zu verstehen, welche IT-Strukturen durch realistisch anzunehmende Attacken auf welche Weise verwundbar sind. Die kontinuierliche Bewertung von Verwundbarkeiten und Risiken fehlt genauso wie die gründliche Beschäftigung mit komplexen vernetzten Systemen und insbesondere mit Interdependenzen und Verwundbarkeiten von Informations-Infrastrukturen in einem modernen sicherheitspolitischen Umfeld. Isolierte Ansätze vermögen kaum mehr zu befriedigen. Vielmehr ist die umfassende Risiko- und Verwundbarkeitsanalyse auf der Ebene des Staates gefragt. Dafür braucht es eine holistische Perspektive von Risiken und Verwundbarkeiten, die physische, digitale, psychologische und logische Aspekte mit einbezieht. Die eingehende Beschäftigung mit den Akteuren darf im Zusammenhang mit Cyberrisiken ebenfalls nicht fehlen. Eine solche Forschung verlangt aber eine starke inter- und multidisziplinäre Ausrichtung, die zahlreiche Aspekte – dazu gehören technische, politik- und rechtswissenschaftliche – unter einen Hut bringt. Damit eine solche Forschung entstehen und florieren kann, braucht es noch viel Arbeit und Offenheit gegenüber Themen, welche die traditionellen Grenzen gängiger akademischer Forschung sprengen.

Verein Sicherheitspolitik und Wehrwissenschaft

Unsere Ziele

Der Verein und seine Mitglieder wollen
- bekräftigen, dass die Schweiz auch in Zukunft ein militärisch ausreichend geschützter Raum bleiben soll,
- erklären, dass ein wirksamer Schweizer Beitrag an die Stabilisierung primär des europäischen Umfeldes eine glaubwürdige, kalkulierbare und umfassende Schweizer Sicherheitspolitik benötigt,
- herausarbeiten, dass die Schweiz nicht nur als Staat, sondern auch als Wirtschaftsstandort, Denk-, Werk- und Finanzplatz sicherheitspolitisch stabil bleiben muss, um weiterhin erfolgreich existieren zu können,
- darlegen, dass eine sichere Schweiz angemessene Mittel für ihre Sicherheitspolitik benötigt,
- aufzeigen, was für eine effiziente und glaubwürdige Armee im Rahmen des integralen Selbstbehauptungsapparates an Führungscharakter und Kompetenz, an Ausbildung, Ausrüstung und Organisation nötig ist,
- sich dafür einsetzen, dass künftige Reformen der Milizarmee und ihrer Einsatzdoktrin diesen Postulaten entsprechen.

Unsere Leistungen

Der Verein und seine Mitglieder verfolgen diese Ziele seit 1956 durch Informationsarbeit in Form von
- Studien, Fachbeiträgen, Publizität und Stellungnahmen,
- von Vorträgen, Interviews und Gesprächsbeiträgen.

So hat er wesentlich geholfen
- armeefeindliche Volksinitiativen zu bekämpfen (1987, 1989, 1993, 1997, 2000, 2001),
- Expertenbeiträge zur einer neuen Sicherheitspolitik und zu einer glaubwürdig ausgebildeten und ausgerüsteten Armee zu leisten.

Unsere Zukunftsvision

Wir wollen mit unserer Arbeit dazu beitragen,
- dass die Schaffung eines breit abgestützten inneren Konsenses im Bereich der militärischen Selbstbehauptung in der Schweiz gelingt und
- die gesellschaftliche, wirtschaftliche und politische Integration unserer Milizarmee auch in Zukunft intakt bleibt.

Unsere Finanzierung

Wir finanzieren uns durch Mitgliederbeiträge, Gönnerbeiträge, Spenden sowie Legate und danken allen im voraus für Ihre Unterstützung.

Sie erreichen uns unter:
Postfach 65, 8024 Zürich, Internet: www.Chinfo.ch/vsww
PC-Konto 80-500-4
Telefon: 01-266 67 67 oder Fax: 01-266 67 00