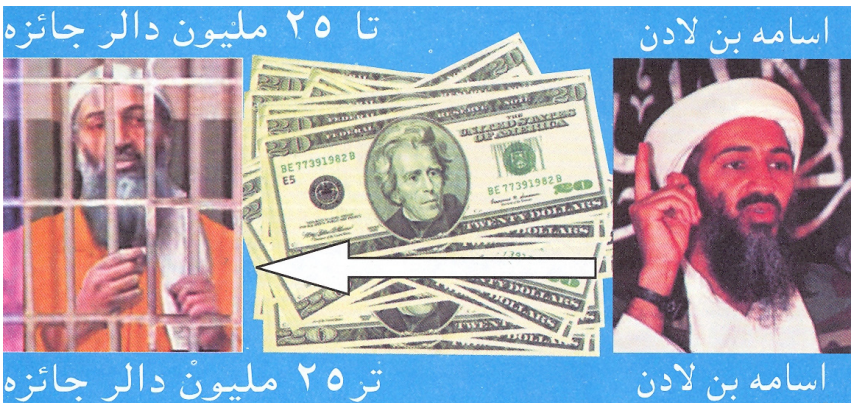
CSS Analysen zur Sicherheitspolitik

CSS ETH Zurich

Nr. 34 • Mai 2008 • 3. Jahrgang

INFORMATIONSOPERATIONEN: TRENDS UND KONTROVERSEN

Informationsoperationen haben in den vergangenen Jahren an Bedeutung gewonnen. Die Beeinflussung der Informationen eines Gegners oder der Einstellung der Zivilbevölkerung in Einsatzgebieten sowie die Sicherung der eigenen Informationen und Informationssysteme sind zu wichtigen Erfolgsfaktoren militärischer Operationen geworden. Das Konzept hat jedoch Anlass zu heftigen Kontroversen gegeben. Welche Art von Einsätzen die Streitkräfte demokratischer Rechtsstaaten in welchem Umfang durchführen dürfen und sollen, bleibt umstritten. Klärungsbedarf herrscht auch bezüglich der Zuordnung von Verantwortung und Aufgaben an der zivil-militärischen Schnittstelle.



In Afghanistan verwendetes US-Flugblatt *psywarrior.com*

Der Faktor Information ist seit jeher ein wichtiger Bestandteil von Macht, Diplomatie und Kriegsführung. Schon der chinesische Stratege Sun Tzu (ca. 400–320 v. Chr.) hielt fest, dass die Kenntnis des Gegners und der eigenen Vernichtungspotenzen Voraussetzung für Erfolg in der Schlacht sei und Kriege dank Informationsüberlegenheit selbst ohne Schlacht zu gewinnen wären. Doch auch wenn die Geschichte des Informationskriegs so alt wie der Krieg selbst ist: Erst seit neuster Zeit stehen Mittel zur Verfügung, die eine umfassende Beeinflussung des Gegners durch Information ermöglichen. Die Bedeutung von Information als Element einer effektiven Sicherheits- und Verteidigungspolitik hat deshalb in den vergangenen Jahren noch einmal stark zugenommen.

Das Konzept der «Information Operations» (Info Ops) ist in den 1990er Jahren von den USA entwickelt und in die nationale Militärdoktrin integriert worden. Es bündelt die bewährten Prinzipien traditioneller Informationsstrategien und schreibt in diesem Sinne die Zielsetzungen klassischer Kriegsinformationspolitik fort. Darüber hinaus führt es aber auch wichtige neue Elemente ein. Insbesondere wird Informationshoheit nicht mehr nur als Unterstützungselement der Kriegsführung, sondern auch als eine eigene Kampfform verstanden, die in den heutigen Konflikten entscheidende Wirkung erzielen kann. Medien und Informationen werden als zusätzliche Instrumente in das Arsenal von Angriffs- und Verteidigungswaffen integriert. Damit widerspiegelt und forciert das Konzept moderner Informationsoperationen die zunehmende Verwischung zwischen militärischen und nicht-militärischen Aspekten von Sicherheitspolitik. Gleichzeitig erfordert es eine hohe Koordinationsleistung zwischen der militärisch-operativen und der politisch-strategischen Ebene sowie zwischen staatlichen und nichtstaatlichen Akteuren.

Defensive und offensive Komponenten

Der Stellenwert der Generierung, Verwaltung und Verwertung von Information hat aufgrund technologischer Entwicklungen im Bereich der Informations- und Kommunikationstechnologien sowie der breiten Nutzung dieser Technologien in allen Bereichen der Wirtschaft, Politik und Gesellschaft stark zugenommen. Die Beherrschung der neuen Technologien und der Einfluss über Informationsinhalte haben sich zu einer zentralen Machtressource entwickelt.

Das Konzept der Informationsoperationen ist hauptsächlich vor diesem Hintergrund entwickelt worden. Gemeinhin gilt der Golfkrieg von 1991 als Beginn einer neuen Generation von Kriegen, in denen nicht mehr in erster Linie nur physische Gewalt über den Sieg entscheidet, sondern die Fähigkeit, den «Informationskrieg» zu gewinnen und «Informationsüberlegenheit» zu erreichen. War die entsprechende Diskussion zunächst eng auf das militärisch-operative Potential von Informationsoperationen fokussiert, so traten bald auch die mit dieser Entwicklung verbundenen sehr viel breiteren Risiken zutage. Je weiter die Debatte über Angriffe auf die Informationssysteme möglicher Gegner voranschritt, desto intensiver wurde die vergleichsweise hohe Verwundbarkeit der eigenen militärischen und zivilen Datennetze thematisiert. Neben die offensive Komponente von Informationsoperationen trat deshalb Mitte der 1990er Jahre zunehmend das defensive Ziel, die eigene

kritische Infrastruktur vor Cyber-Angriffen und anderen Risiken zu schützen (siehe CSS Analyse Nr. 16). Eine entsprechend umfassende und teilstreitkräfteübergreifende Doktrin wurde erstmals 1998 von den *US Joint Chiefs of Staff* formuliert.

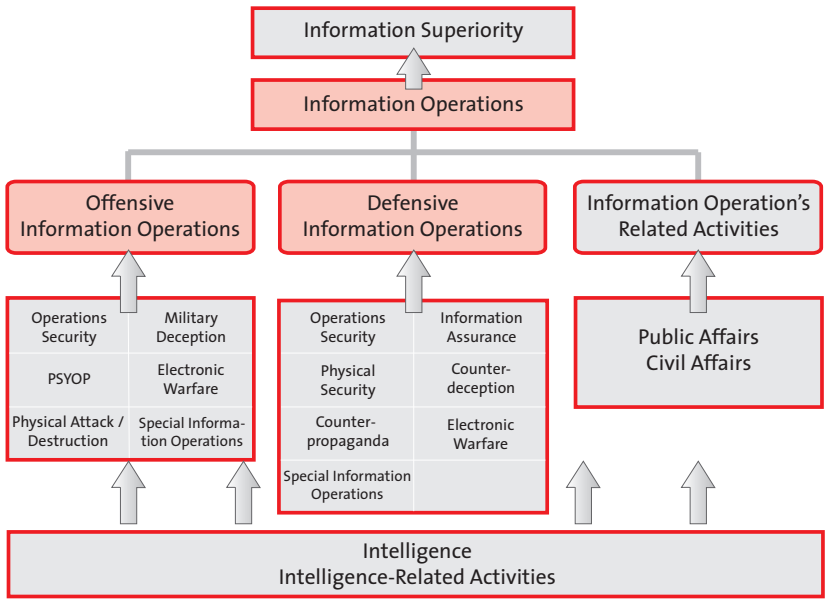
Unter Informationsoperationen versteht man heute in der Regel koordinierte militärische Aktivitäten, die das Ziel verfolgen, durch Beeinflussung von Informationen und Informationssystemen eine angestrebte Wirkung auf den Willen und die Entscheidungsfähigkeit gegnerischer Truppen und/oder die Einstellung der Zivilbevölkerung in Einsatzgebieten auszuüben und die eigenen Informationen und Informationssysteme zu schützen. Solche Operationen können eine breite Palette von Instrumenten umfassen, wie z.B. psychologische Operationen, physische Zerstörung, elektronische Kriegsführung, Angriffe auf Computernetze und deren Verteidigung, militärische Täuschung, Gegenpropaganda, Informationssicherung, Operationssicherheit und Eindringen in Computer. Ein Vergleich der mehr als 20 existierenden Info Ops Doktrinen von Staaten und der NATO macht jedoch deutlich, dass das Konzept unterschiedlich gehandhabt wird. Längst nicht alle Staaten verfügen über den politischen Willen oder die Fähigkeiten, das ganze Spektrum von Instrumenten einzusetzen. Auch gewichtet die Mehrheit der Staaten defensive Massnahmen stärker als allfällige offensive Aktionen.

Eine Querschnitts- und Verbundaufgabe

Trotz dieser Heterogenität lassen sich drei Elemente identifizieren, die für Informationsoperationen heute charakteristisch sind. Erstens nehmen diese Operationen im Spektrum der militärischen Operationstypen eine Querschnittsfunktion ein. Informationsoperationen spielen sowohl in Verteidigungsoperation wie in Einsätzen unterhalb der Kriegsschwelle und in internationalen Stabilisierungseinsätzen eine bedeutsame Rolle. Während Massnahmen wie die Bombardierung von Radarstellungen nur im Kriegsfall zum Tragen kommen, werden andere Instrumente in allen Operationstypen eingesetzt.

Zweitens sind Informationsoperationen nicht isoliert als eine rein militärische Aufgabe, sondern als Teil einer Verbundaufgabe von Militär und zivilen staatlichen und nichtstaatlichen Akteuren im Sinne einer umfassenden Informationsstrategie zu verstehen. So kann die Armee im Bereich

Informationsoperationen gemäss US-Dokrin (JP3-13)



defensiver Informationsoperationen häufig nur einen begrenzten Beitrag leisten. Beim Schutz kritischer Infrastrukturen beispielsweise spielt sie eine untergeordnete Rolle, die sich im Wesentlichen auf die Sicherung der eigenen Netzwerke beschränkt. Der Umgang mit *Informatik*risiken, d.h. mit möglichen Angriffen staatlicher oder nichtstaatlicher Akteure auf Informatiksysteme und Informatikinfrastrukturen, erfordert primär eine enge Partnerschaft zwischen Staat und Wirtschaft sowie intensive zwischenstaatliche Kooperation. Aber auch *Informations*risiken, d.h. Risiken, die mit dem Inhalt von Information zu tun haben, gehören in erster Linie in den politischen Verantwortungsbereich. Allerdings kann das Militär wichtige Beiträge etwa zur Erkennung von feindlicher Desinformation oder zum Schutz von nationalen Führungsstrukturen erbringen.

In anderen, primär offensiven Bereichen der Informationsoperationen spielen die operative und die taktische militärische Ebene bezüglich Führung und Umsetzung von Informationsoperationen zwar häufig eine massgebliche Rolle. Aber auch solche Operationen sind ohne parallele und koordinierte Massnahmen der politisch-strategischen Ebene vielfach von begrenzter Wirkung. Zudem mangelt es ihnen oftmals an Legitimität (siehe unten). Der Bedarf an sektorübergreifender Kooperation und Koordination steigt umso mehr, als Informationsoperationen heute oft nicht mehr nur auf die Beeinflussung geographisch klar umrissener Informationsräume und -systeme, sondern der gesamten Weltöffentlichkeit zielen.

Fokus auf psychologische Operationen

Dieser letzten Beobachtung entsprechend lässt sich drittens auch eine zunehmende Bedeutung von psychologischen Operationen (PSYOP) innerhalb der Informationsoperationen feststellen. Mit diesem Begriff sind Massnahmen zur Beeinflussung des Verhaltens und der Einstellungen von gegnerischen Truppen und/oder fremder Zivilbevölkerungen im Kontext von militärischen Operationen gemeint. Der Bedeutungszuwachs dieser Operationen lässt sich einerseits auf die Bedrohung durch den internationalen Terrorismus zurückführen, die aus Sicht der Staaten umfassende Gegenmassnahmen auch im Informationsbereich erfordert. Terrorismus ist nicht nur als asymmetrische Methode der Kriegsführung, sondern auch als Kommunikationsstrategie zu begreifen. Dank moderner Kommunikationsmittel können die Terroristen ihre Taten dokumentieren und ihre Botschaften mit geringem Aufwand global verbreiten. Eine positive Beeinflussung der islamischen Öffentlichkeit und das Überzeugen der eigenen Öffentlichkeit von der Notwendigkeit des Kampfs gegen den Terrorismus sind deshalb zentrale Ecksteine der westlichen Anti-Terror-Strategie. Andererseits haben auch die Erfahrungen im Bereich der multilateralen Stabilisierungseinsätze in Konfliktgebieten in den vergangenen Jahren die eminente Bedeutung von psychologischen Operationen erkennen lassen. Ohne die Akzeptanz der

lokalen Bevölkerung sind solche Einsätze langfristig zum Scheitern verurteilt, weshalb der Informationsvermittlung und -steuerung durch Radioprogramme, Flugblätter, Internetauftritte etc. wachsende Aufmerksamkeit zukommt.

Allerdings wird auch PSYOP von den Staaten unterschiedlich gehandhabt. So erhebt die Deutsche Bundeswehr (die von Operativer Information statt PSYOP spricht) den Anspruch, keine unwahren Informationen zu verbreiten und höchstens durch selektive Information Meinungen zu beeinflussen. In der US-Doktrin hingegen sind auch bewusste Fehlinformationen als Teil der Einflusskommunikation vorgesehen. «Weisse Propaganda», also möglichst sachliche und wahre Information, soll beispielsweise im US-Aussenministerium unter dem Titel «Public Diplomacy» vermittelt werden. Darunter lässt sich eine Mischung aus Auslandspropaganda, politischem Marketing und Kulturdiplomatie verstehen. «Schwarze Propaganda», d.h. Desinformation und sogenannte Zersetzungspropaganda, wurde im US-Verteidigungsministerium durch das «Office of Strategic Influence» im Jahr 2002 institutionalisiert. Auch wenn dieses Büro infolge weltweiter Proteste wieder geschlossen wurde, schliessen die US-Streitkräfte die Verwendung von Desinformation nach wie vor nicht explizit aus. Zudem hat das Weisse Haus seither ein «Office of Global Communications» gegründet, das ähnliche Aufgaben wahrnimmt und die gesamte Auslandspropaganda der USA koordinieren soll. Anzufügen ist, dass die USA häufig auf «graue Propaganda» setzen, d.h. bewusst ambivalente Informationen, die weder richtig noch falsch sind, sondern einen gewünschten Interpretationsrahmen setzen.

Klärungsbedarf

Auch wenn Informationsoperationen in den letzten Jahren stark an Bedeutung gewonnen haben, bleibt das Konzept kontrovers. Aus der Sicht demokratischer Rechtsstaaten betrifft dies vor allem die offensive Dimension solcher Operationen. Hier gilt es, vor dem Aufbau allfälliger Fähigkeiten grundlegende Fragen zu klären.

So ist festzulegen, auf welche konkreten Aspekte offensiver Informationsoperationen ein Rechtsstaat in welcher Situation und in welchem Ausmass legitimerweise zurückgreifen darf. Offensive Tätigkeiten grundsätzlich auszuschliessen dürfte nicht zweckmässig sein, zumal etwa psychologische Operationen für das Gelingen multilateraler Friedensoperationen wie dargelegt eine zunehmend wichtige Rolle spielen. In welchen Kontexten aber kann und soll ein Staat beispielsweise mit Desinformation operieren?

Klärungsbedarf herrscht auch in der Rollenzuordnung zwischen der Armee und den politischen Behörden. Hier stellt sich insbesondere die Frage, inwieweit Streitkräfte Aufgaben im Bereich offensiver Informationsoperationen übernehmen sollen und können. Zu prüfen wäre auch, wie sich gegebenenfalls die politische Kontrolle und Steuerung von solchen militärischen Operationen respektive die Koordination mit Aktivitäten auf der politisch-strategischen Ebene sicherstellen liessen. Ganz allgemein gilt es, Klarheit über die Anforderungen an die doktrinale Entwicklung und die Ausbildung des militärischen Personals im Bereich der Informationsoperationen zu erlangen.

«Psychologische Operationen werden auch für die Schweizer Armee an Bedeutung gewinnen.»

Bedeutung für die Schweiz

Auch in der Schweiz ist der sicherheitspolitische Umgang mit Information zu einem wichtigen Thema geworden. So befassen sich heute mehrere Bundesstellen mit Informationssicherheit, wie z.B. das Informatik-Strategieorgan des Bundes, die Koordinationsstelle zur Bekämpfung der Internetkriminalität und die Melde- und Analysestelle Informationssicherung (MELANI). Jedoch fehlt es bundesweit an einer gesamtheitlichen Betrachtung von Risiken und Gegenmassnahmen. Das Bundesamt für Bevölkerungsschutz wurde Mitte 2005 vom Bundesrat beauftragt, zusammen mit allen beteiligten Departementen den Handlungsbedarf im Bereich der kritischen Infrastrukturen zu identifizieren und entsprechende Massnahmen zu erarbeiten. Risiken der Informationsgesellschaft sollten hierbei besondere Beachtung finden.

In der Armee ist im Jahr 2005 nach langer Arbeit die Konzeptionsstudie «Information Operations» abgeschlossen worden, die ein umfassendes Bild über Risiken, Gefahren und Chancen in der Verwendung von Informationen und Informationssystemen in Kriegs- und Krisenzeiten zeichnet. Die Erkenntnisse der Konzeptstudie führten zu mehreren Anträgen in den Bereichen Organisation, Doktrin und Ausbildung. Umgesetzt wurde bisher aber nur die Schaffung entsprechender Führungselemente auf Stufe Armeeführung. Der Aufbau eines Armeestabsteils für «Operationelle Informationsführung», d.h. für psychologische Operationen, wurde im Sommer 2007 aufgrund von Unklarheiten im rechtlichen, doktrinalen und finanziellen Bereich zurückgestellt.

Die Schweiz tut sich offenkundig schwer mit Informationsoperationen. Dies vermag nicht weiter zu erstaunen, zumal auch in anderen europäischen Staaten ähnliche Entwicklungen zu beobachten sind. Eine besondere Herausforderung für die Schweiz stellt die Kompetenzzuordnung an den zivil-militärischen Schnittstellen von Informationsoperationen dar. Auf Seiten der Politik besteht eine beträchtliche Skepsis bezüglich Aufgaben der Armee im Informationsbereich. Dennoch lassen es die heute wahrscheinlichen Bedrohungen und Risiken kaum zu, das Konzept der Informationsoperationen pauschal über Bord zu werfen. Vielmehr ist im Detail zu prüfen, in welchen Bereichen die Armee Beiträge leisten und entsprechende Fähigkeiten entwickeln soll. Psychologische Operationen etwa dürften zur Erfüllung der Armeeaufträge weiter an Bedeutung gewinnen. Erforderlich wären hier allerdings klare politische Vorgaben, da beispielsweise die Reaktion auf Desinformation klar im Verantwortungsbereich der politischen Entscheidungsträger liegt.

Anzustreben wäre eine konzeptionelle Einbindung von Informationsoperationen in eine Informationsgesamtstrategie auf Stufe Bund. Allerdings ist die strategische Informations- und Kommunikationspolitik in Krisenzeiten aufgrund von Eigenheiten des Regierungssystems und der föderale Grundordnung der Schweiz eine schwierige Aufgabe. Einen wichtigen internationalen Beitrag könnte die Schweiz bezüglich der Klärung völkerrechtlicher Fragen zu Informationsoperationen leisten. Auch könnte sie sich für ein international abgestimmtes Moratorium bei der Entwicklung und beim Einsatz von Computerwaffen und für die Förderung der Universalität von Abkommen zur friedlichen Nutzung des Cyberspace stark machen.

Verantwortlicher Editor: Daniel Möckli
analysen@sipo.gess.ethz.ch

Bezug und kostenloses Abonnement:
www.ssn.ethz.ch