Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 176 (2010)

Heft: 09

Artikel: Informationsoperationen : den Entscheidfindungsprozess im Fokus

Autor: Varesio, Pascal

DOI: https://doi.org/10.5169/seals-131210

Informationsoperationen: den Entscheidfindungsprozess im Fokus

Informationsoperationen (InfoOps) übernehmen im Einsatzspektrum einer modernen Armee zunehmend eine Schlüsselfunktion. Auch in der Schweizer Armee arbeitet man am Aufbau dieser Kompetenzen. Trotz «Helvetisierung» des Konzepts und der offensichtlichen Bedeutung der Informationssphäre[1], wird der Operationslinie Information noch zu wenig Beachtung geschenkt.

Pascal Varesio

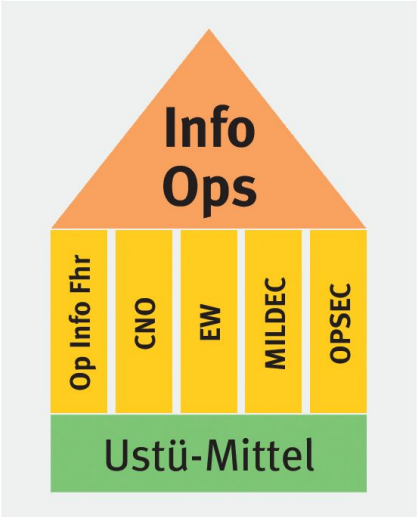
Am frühen Morgen des 31. Mai 2010 nähert sich die Flotte des «Free Gaza Movements» der Küste des Gaza-Streifens. Mit an Bord der Schiffe sind Videoreporter. Als israelische Elitesoldaten die Schiffe entern, werden sie gefilmt. Fotos und Filme gelangen dank mobilen Netzwerken rasch an die Öffentlichkeit. Die visuelle Ausschlachtung der Aktion war von Anfang an zentraler Bestandteil der Strategie der Aktivisten. Auf Videoplattformen, Blogs und sozialen Medien wie Twitter und Facebook entwickelt sich sofort eine Auseinandersetzung um die Deutungshoheit über das, was an diesem Morgen auf den Schiffen geschah. Obwohl die israelische Armee eigene Filmaufnahmen in den folgenden Tagen veröffentlichte, reagierte sie insgesamt zu langsam, um die Debatte in eine für sie günstige Richtung zu lenken.

Verletzlicher Staat und Gesellschaft

Das Informationszeitalter zeichnet sich durch globale Vernetzung, den uneingeschränkten Zugang zu Informationen, sowie deren rasche Verarbeitung und Verbreitung in einem mobilen Umfeld aus. Die Verwundbarkeit des Staates bzw. seiner Gesellschaft gegenüber technischen Störfällen oder manipulierten Informationen nimmt dadurch drastisch zu. Störungen können das ordentliche Funktionieren von Staat und Gesellschaft empfindlich beeinträchtigen. Primäres Ziel eines Angreifers in der Informationssphäre ist, die Handlungsmöglichkeiten eines Akteurs einzuschränken sowie dessen Entscheidungsfindung zu beeinflussen. Klassische Mittel wie Propaganda oder Desinformation und Täuschung können im Informationszeitalter quantitativ und qualitativ wirkungsvoller eingesetzt werden als bis anhin. Dabei kommt dem Cyberspace eine tragende Rolle zu; Aktivitäten darin sind unmittelbar, billig und anonym. Er ist Teil der Informationssphäre und umfasst das gesamte Netzwerk der informationstechnologischen Infrastruktur, einschliesslich Internet und Computersysteme.

Emblem U.S. Army PSYOP. Quelle: US Army

InfoOps-Mittel.



Auch die Armee ist vernetzt – und verletzlich

Im Zuge des technologischen Fortschritts basiert die Armee ebenfalls auf vernetzten Führungs-, Kommunikations- und Informationssystemen, die teilweise mit dem Web verknüpft sind. Aktionen in der Informationssphäre können daher gezielt und unter Umständen unbemerkt gegen die Armee gerichtet sein. Massnahmen in der Informationssphäre, die darauf Abzielen, entweder militärische Entscheidfindungsprozesse und die Handlungsmöglichkeiten einer Gegenseite zu beeinflussen, oder die eigenen Informationen, Informationssysteme und Prozesse zu schützen, werden als Informationsoperationen (InfoOps) bezeichnet. Der Begriff InfoOps ist ausschliesslich militärisch zu verwenden, um in diesem politisch heiklen Bereich, die klare Trennung zwischen Politik und Armee hervorzuheben. Obwohl in Zukunft eine gegen die Schweiz gerichtete InfoOps wahrscheinlicher ist, als eine konventionelle militärische Bedrohung, wird nach wie vor wenig in die Fähigkeiten zu deren Abwehr investiert. Dies mag einerseits im mangelnden Verständnis bedingt durch die hohe Komplexität der Thematik begründet sein. Andererseits gibt es auch Befürchtungen, dass InfoOps-Fähigkeiten gegen die Schweizer Bevölkerung gerichtet werden könnten.

Informationsoperationen in der Schweizer Armee

Im Führungsstab der Armee (FST A) ist eine Sektion verantwortlich, die InfoOps-Aktivitäten der Armee zu planen, koordinieren, synchronisieren sowie Handlungsrichtlinien für Übungen und den Einsatz aufzustellen. Zusätzlich leistet sie

einen Beitrag zur InfoOps-Sensibilisierung in der Armee und Verwaltung. Die Rechtsgrundlagen für den Ausbildungsdienst und die normale Lage erlauben heute den Kompetenzaufbau und das Üben InfoOps-relevanter Fähigkeiten. Im Verteidigungsfall gelten die Regeln des Völkerrechts. Die Sektion wird von einem hoch spezialisierten Armeestabsteil (Astt) unterstützt. Sie verfügt über keine weiteren eigenen materiellen Ressourcen und ist daher auf verschiedene Leistungserbringer aus dem VBS, wie der Führungsunterstützungsbasis der Armee (FUB), angewiesen. Die Mittel einer InfoOps setzen sich in der Regel aus fünf Elementen zusammen, die im Folgenden erläutert werden.

Charta InfoOps:
Die Angehörigen der Sektion InfoOps und des Armeestabs respektieren das Gesetz, ethische und moralische Prinzipien sowie internationale Verpflichtungen. Sie halten sich bei der Erfüllung militärischer Aufträge ausschliesslich an die Wahrheit. Die Schweizer Bevölkerung und die eigenen Truppen dürfen nie getäuscht werden.

Die Operationelle Informationsführung (Op Info Fhr): gemeint sind alle Aktivitäten, die zur Veränderung des Verhaltens und der Werte einer Gegenseite gegenüber der Armee und ihrem Auftrag beitragen (winning hearts & minds).

Computer Network Operations (CNO): Diese beinhalten alle aktiven und passiven Massnahmen in Bezug auf Datenverarbeitungsanlagen und Cyberspace. Sie umfassen den Schutz (Computer Network Defense, CND), den Angriff (Computer Network Attack, CNA) und die Ausspähung (Computer Network Exploitation, CNE). Die heutigen Rechtsgrundlagen erlauben der Schweizer Armee Aktivitäten im Teilbereich der Computer Network Defense (CND).

Electronic Warfare (EW): Sämtliche Massnahmen, die das elektromagnetische Spektrum nutzen. EW dient also beispielsweise dazu, elektromagnetische Strahlung zu identifizieren oder selbst auszusenden, um einer Gegenseite die Nutzung des Spektrums zu verwehren. Die Massnahmen richten sich hauptsächlich gegen die C3I-Infrastruktur (Command, Control, Communications and Intelligence) der Gegenseite.

Military Deception (MILDEC): Massnahmen zwecks Täuschung der Gegenseite bezüglich eigener Fähigkeiten und Absichten. Ziel ist es, die Gegenseite zu einer für uns günstigen Handlung (oder Nicht-Handlung) zu verleiten.

Operation Security (OPSEC): Die Summe aller Massnahmen, die Gegenseite daran zu hindern, Informationen zu sammeln, die Rückschlüsse auf eigene Operationen, Führungsinfrastruktur und Schlüsselpersonal erlauben. Gerade in den Zeiten von Facebook, Twitter etc. kommt dieser Fähigkeit zunehmende Bedeutung zu.

Entscheidungsfindung und Handlungsfreiheit

Die Armee ist heute ebenfalls Teil der globalen Vernetzung. Sie kann sich nicht einfach abschotten bei Bedrohungen aus der Informationssphäre. Ein wirksamer Schutz ist erst erreicht, wenn die Führung jederzeit sowohl unbeeinflusst entscheiden kann als auch ihre Handlungsfreiheit bewahrt. Dieser Schutz kann aber nicht alleine mit defensiven Massnahmen erreicht werden. Wie die visuelle Kriegsführung rund um den Hilfskonvoi für Gaza gezeigt hat, geht es darum, die eigene Sicht der Ereignisse proaktiv, rasch, wirksam und glaubwürdig darzustellen. Solange wir nur reagieren können, verlieren wir neben der Handlungsfreiheit auch zwangsläufig die Möglichkeit, die Fakten korrekt darzustellen. InfoOps sind ein Instrument, welches verschiedene Fähigkeiten der Armee bündelt und es ihr ermöglicht, nicht nur reaktiv sondern auch proaktiv Bedrohungen aus der Informationssphäre zu begegnen.

Was ist CNO?

- Einsatz von Malware (Trojaner, Viren) gegen IT-Netzwerke.
- Überlastung von Servern und Netzwerken (Spam, DDOS).
- Online-Informationsbeschaffung (Phishing).
- Schutz der eigenen Netzwerke und Server.

Was ist Op Info Fhr?

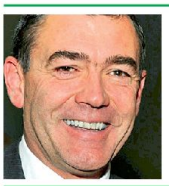
- Mit wahrer Information Werte, Meinungen und Verhalten der Gegenseite in besonderen und ausserordentlichen Lagen beeinflussen.

China baut seine Abwehr gegen den mächtigen amerikanischen Konzern Google aus.
Quelle: http://www.gizomodo.de

Fazit

Zukünftige Auseinandersetzungen beginnen in der Informationssphäre, ungeachtet dessen, ob es sich um zwischenstaatliche Konflikte handelt oder nicht. Falls Streitkräfte ebenfalls zu den Akteuren gehören und diese ihre Informations- und Informationsführungssysteme nicht ausreichend schützen können, werden diese nicht mehr in der Lage sein, ihre Mittel rechtzeitig, in der richtigen Menge und am richtigen Ort zum Einsatz zu bringen. ■

1 Die Informationssphäre umfasst sämtliche Interaktionen zwischen Sender und Empfänger sowie weiteren Beteiligten unter Nutzung der Informationsinfrastrukturen.
2 CNA und CNE sind heute nur im Aktivdienst der Armee möglich. Für die beiden anderen Einsatzarten (Assistenzdienst und Friedensförderungsdienst) fehlen die notwendigen Rechtsgrundlagen.



Colonel
Pascal Varesio
Chef frac EM A 234
2013 Colombier NE