Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 168 (2002)

Heft: 7

Artikel: Gegen ein Cyber Pearl Harbor : Information Operations als neue Herausforderung

Autor: Forster, Peter

DOI: https://doi.org/10.5169/seals-68001

Gegen ein Cyber Pearl Harbor – Information Operations als neue Herausforderung

Peter Forster

Gegen Ende der Neunzigerjahre sprach jedermann von Information Warfare; und jeder verstand darunter etwas anderes. Martin Libicki, Forscher an der National Defense University in Washington, schrieb: «Information Warfare definieren zu wollen, ist wie die Geschichte von den Blinden und dem Elefanten. Die Blinden wollen die Natur des Elefanten ergründen: Der eine berührt das Bein und nennt es einen Baum, der zweite greift an den Schwanz und nennt ihn ein Seil, und so weiter.»

Früh gab Libicki für Information Warfare die siebenteilige Umschreibung, die in den Vereinigten Staaten eine Zeitlang gültig war. Nach Libicki umfasst der Informationskrieg den Command-and-Control War, den Intelligence-Based War, den Electronic War, die Psychological Operations, den Hacker War, den Economic Information War und den Cyber oder Net War.

Hacker War bringt Gefahr

Heute sprechen wir nicht mehr so sehr von Information Warfare, sondern von Information Operations. Aber Definitionen gibt es immer noch wie Sand am Meer. Eine knappe Umschreibung bringen die amerikanischen Joint Chiefs of Staff, welche die Information Operations in ihrer Joint Doctrine wie folgt definieren: «Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO». Demgegenüber umschreibt die Joint Doctrine den Begriff Information Warfare als «Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives *over a specific adversary or adversaries.* Also called IW».

Schon Libickis alte Definition zeigt, dass nicht alles neu ist unter der Sonne. Den Command-and-Control War etwa oder den Intelligence-Based War gibt es schon lange. Ebenso werden Psychological Operations geführt, seit Feldherren und Politiker die Meinung anderer zu beeinflussen suchen. Neu ist der Hacker War und er ist es auch, der in Zeiten des Terrors Gefahren in sich birgt.

Schäden von grossem Ausmass

Unbestritten ist, dass Information in den hochvernetzten, hochverletzlichen Gesellschaften des Westens gegenwärtig ungenügend geschützt ist. Information und Wissen sind wesentliche Erfolgs- und Machtfaktoren in der industrialisierten Welt. Wie Kurt Haering, der Geschäftsführer der schweizerischen Stiftung InfoSurance, schreibt, stärkt die Informationstechnologie die entwickelten Länder im weltweiten Wettbewerb; aber sie macht diese auch verwundbar. Ihre offene Informationsarchitektur lädt zu Missbrauch und Diebstahl ein. Die unrechtmässige und kriminelle Nutzung der Daten ist nicht mehr auszuschliessen: «So kann Entwendung oder Veränderung von Information Schäden von grossem Ausmass verursachen. Als Beispiele seien Fehlentscheide, Konkurrenznachteile und der Ausfall von Arbeitsinfrastruktur genannt.»

Muhamed Al-Dura und sein Vater Jamal suchen Schutz hinter einem Betonklotz – vergebens. Muhamed stirbt in den Armen seines Vaters. (Bild: France 2)

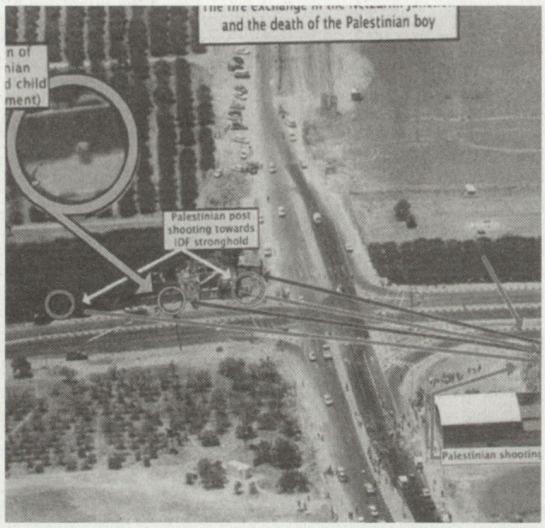
Informations Operations können mit einfachen Mitteln – unabhängig von Entfernungen, teils ohne grosse Kosten und mit kleiner Wahrscheinlichkeit, entdeckt zu werden – bei geringem Risiko geführt werden. Denkbar sind menschliche und technische Fehler, gezielte Manipulation von Daten, die Sättigung von Systemen, die Implementierung von Fehlfunktionen, die Softwarevernichtung und Einwirkungen bis zur physischen Zerstörung von Hardware und Infrastruktur. Mo-

tive können sein: die Spionage zur Erlangung von wirtschaftlichen Vorteilen, das Erzielen von Datenschäden und Störungen zur Erpressung oder die gezielte Einflussnahme auf Entscheidungen in Verwaltung, Wirtschaft oder Armee.

Vorwarnzeit fehlt

Wie in der Schweiz der Sicherheitspolitische Bericht 2000 festhält, fehlt bei Informationsoperationen in aller Regel die Vorwarnzeit. Oft können Schutz- und Gegenmassnahmen nicht rechtzeitig ausgelöst werden: «Einem einzelnen Informatiksystem ist es kaum möglich, Urheber, Absicht, Beginn, Art, Umfang und Ende der Einwirkung rasch zu erfassen. Angreifer profitieren auch vom Umstand, dass fast alle Unternehmungen und Verwaltungen ihre Datensicherheit allein zu erreichen versuchen, womit dieselben Angriffsmethoden wiederholt angewendet werden können.»

In der Umschreibung der Gefahren wird der Sicherheitspolitische Bericht sehr deutlich. Die Bedrohung reiche von massiven Beeinträchtigungen oder Störungen der Wirtschaft bis zur Lähmung der politischen und militärischen Führung. Der Bericht hebt sensitive Bereiche hervor, in denen überproportionale Schäden angerichtet werden können. Dazu gehören folgende kritischen Datenbestände und Netzwerke der nationalen Informatik- und Kommunikationsinfrastruktur: «öffentliche Verwaltung aller Ebenen; Industrie, Handel, Banken, Versicherungen, Sozialwerke; Versorgungs- und Verteilsysteme für Elektrizität, Gas, Erdöl, Wasser; Verkehrsleitung und Transportwesen (Strasse, Schiene, Luft, Wasser); Polizei, Sicherheits- und Rettungsdienste, Informations- und Kommunikationsdienste, Medien; militärische Führung.» Elektronische Angriffe auf diese vitalen Bereiche der Infrastruktur bedrohen die nationale Sicherheit.



Das israelische Luftbild zeigt die Netzarim-Kreuzung im Gazastreifen am 30. September 2000. Links im Kreis die Betontonne, hinter der sich Vater und Sohn Al-Dura verbargen. In unmittelbarer Nähe die palästinensischen Stellungen. Rechts der israelische Stützpunkt, der von den Palästinensern aus mehreren Richtungen angegriffen wurde. (Bild: Zahal)

Technik allein genügt nicht

In der zweiten Hälfte der Neunzigerjahre hat in den vernetzten Gesellschaften das Bewusstsein für die Informationssicherheit zugenommen. Technische Vorkehrungen sind in Staat und Wirtschaft getroffen worden. Allerdings ist es mit technischen Massnahmen nicht getan. Der Schutz muss auch auf «menschlicher», gesetzlicher und organisatorischer Ebene angegangen werden: «Es bringt wenig, wenn eine Datenbank durch Firewalls vor Hackern und Crackern geschützt wird, die entsprechende Information aber durch nicht sensibilisierte Mitarbeiter problemlos preisgegeben wird. Die gesetzlichen Grundlagen werden zurzeit erst den Möglichkeiten der Technik angepasst und bieten noch ungenügenden Schutz. Das Verständnis der Haftung bei ungenügendem Schutz ist ebenfalls erst in Entwicklung.» (Haering)

Immer mehr rückt im Kampf für die Informationssicherheit, gegen ein Cyber Pearl Harbor, der Faktor Vertrauen in den Brennpunkt. Sicherheit wird nicht nur als operativ-technischer (materieller) Begriff dargestellt, sondern auch als psychologischer (immaterieller). In Technologien mit langer Tradition decken sich die beiden Begriffe miteinander. In neuen Bereichen wie Telekommunikation und Information muss dies schrittweise erreicht werden. Neben der Sicherheitsinfrastruktur braucht es die Vertrauensbasis.

Öffentlichkeit reagiert (zu) spät

Erst die Ergänzung der beiden Komponenten ergibt die nachhaltige Sicherheitsarchitektur, wobei die vertrauensbildenden Massnahmen der technischen Entwicklung in der Regel nachhinken. Im professionellen Bereich von Wirtschaft, Verwaltung und Wissenschaft nimmt das Bewusstsein zu, ebenso in den Armeen. Kritischer und schwieriger ist die Lage im Publikumsbereich: Die breite Öffentlichkeit pflegt erst dann zu reagieren, wenn eine grössere Krise oder Katastrophe bereits eingetreten ist.

El-Burej, das Lager, in dem Muhamed Al-Dura gewohnt hatte, ist heute eine Pilgerstätte. (Bild: Peter Forster)

Um in der Schweiz die Öffentlichkeit zu sensibilisieren, konfrontiert der Fachbereich Strategische Führungsausbildung (SFA) der Bundeskanzlei seit 1997 Vertreter aus Verwaltung, Armee, Wirtschaft und Wissenschaft in Übungen und Seminaren mit den Bedürfnissen der Informationssicherheit. Information Assurance wird als interdisziplinäre Verbundaufgabe aufgefasst. In der letzten umfassenden Veranstaltung, der «InformOrena» vom Mai 2002, ergab sich als handfestes Postulat die Schaffung einer Melde- und Analysestelle für Hackerangriffe. Neben der Prävention bildet die Frühwarnung eine zweite Möglichkeit, um das Eintreten einer Krise zu verhindern oder möglichst früh Vorkehrungen zu deren Abschwächung zu treffen.

Verlässlich und unabhängig

Bei der Meldestelle geht es weniger um die staatliche Nachrichtenbeschaffung als um das freiwillige Melden von Vorfällen an eine zentrale Instanz. Dass die Schweiz eine Meldestelle braucht, ist weitgehend unbestritten. Damit sie funktioniert, ist sie auf Meldungen aus einem breiten Spektrum von Informationslieferanten angewiesen. Konsens herrscht unter den Fachleuten darüber, dass sich die Meldestelle nur dann Vertrauen erwerben kann, wenn sie vertraulich, verlässlich und unabhängig von Strafverfolgungsbehörden arbeitet. Wert wird auf den Quellenschutz gelegt. Bereits eingerichtet ist in der Schweiz der Sonderstab Information Assurance unter Leitung des Bundesdelegierten für Informatikstrategie.

In der Armee arbeitet seit einiger Zeit im Generalstab eine Projektgruppe Information Operations unter der Leitung von Major i Gst Gérald Vernez. Sie hat eine umfassende Vorstudie zum gesamten Themenkomplex der Informationsoperationen abgeschlossen und nimmt nun in der ganzen Breite das eigentliche Hauptprojekt an die Hand. Die Arbeitsgruppe denkt einerseits interdisziplinär, was bedeutet, dass sie die Gesamtheit der Entwicklung im Auge behält. Anderseits muss sie die spezifischen Bedürfnisse der Armee abdecken; das führt zwingend dazu, dass sie die unbestreitbar bedeutende militärische Komponente der Information Operations hervorheben muss.

Psychological Operations

Zu diesen Komponenten gehören – mit wachsender Bedeutung – die Psychological Operations. Im Golfkrieg von 1991 setzte General Norman Schwarzkopf die 4. Psyop-Brigade mit Erfolg ein. In den Balkankriegen der Neunzigerjahre spielten Information, Desinformation, psychologischer Terror, Lug und Trug eine zentrale Rolle. Alle Kriegsparteien bedienten sich dieser Mittel in vorher nie dagewesenem Umfang. In unerhörtem Mass wurden die Medien in die Planungen miteinbezogen. Während der Haiti-Operation von 1994 bekannte der amerikanische Generalstabschef John Shalikashvili freimütig: «Wir haben erst gewonnen, wenn CNN sagt, wir haben gewonnen.»

Unentwirrbar sind die Psychological Operations auch mit dem blutigen Kampf zwischen Israel und Palästina verhängt. Die Intifada, der arabische Aufstand in den besetzten Gebieten, die grausamen Terrorattentate gegen Israel und die harte israelische Reaktion tragen wie alle bewaffneten Auseinandersetzungen Züge des Medienkriegs. Einen ersten fürchterlichen Tiefpunkt erreichte das Ringen schon am 30. September 2000, zwei Tage nach Ariel Scharons provokativem «Spaziergang» auf dem Tempelberg.

Vor der Kamera von France 2

An der Netzarim-Kreuzung südlich von Gaza verblutete der 12-jährige Muhamed Al-Dura in den Armen seines Vaters Jamal. Vater und Sohn waren ins Kreuzfeuer der Aufständischen und der Israeli geraten. Ausgerechnet zwischen zwei Fedayin-Stellungen suchten die beiden Schutz. Sie duckten sich vor einer Wand und verbargen sich hinter einem Betonklotz. 45 Minuten lang lagen sie unter Beschuss. Der Vater

wollte den Knaben mit seinem Körper decken. Aber er konnte Muhamed nicht retten.

Die grausame Szene wurde integral vom französischen Fernsehen France 2 aufgenommen. Die Bilder zeigten Muhameds Todeskampf ungeschützt. Zuerst erschütterten sie Israel und dann die Welt. Der Film lief in allen Nachrichtensendungen und fast jede Zeitung brachte das Foto. Für Israel waren die Horrorbilder ein schwerer Schlag. Die Frage wurde laut: War das nötig? Und im Ausland schadete die Szene dem Ansehen des Landes, das im Angesicht der Intifada um seinen Ruf kämpfte.

Aussage gegen Aussage

Was sich dann vom 30. September an in der «Auswertung» des Geschehens abspielte, wirft mehr als alle Theorien ein grelles Licht auf die «modernen» Praktiken der Information Operations. Vater Al-Dura wurde nach Amman geflogen, wo er den Korrespondenten seine Version darbot: Er habe in Gaza ein Occasionsauto besichtigt und sei mit Muhamed auf dem Rückweg in das Flüchtlingslager gewesen, in dem die Familie wohnte. Mit dem Knaben sei er unschuldig in den Kugelhagel geraten, und die Israeli hätten mit ihrem Feuer nicht innegehalten, bis Muhamed verblutet sei.

Dieser Darstellung widersprach scharf General Giora Eiland, der Operationschef der israelischen Armee. Jamal Al-Dura habe Muhamed absichtlich ins Feuer geschickt. Der Knabe habe die Kreuzung betreten, um Steine zu werfen – und das nicht zum ersten Mal. Auch am 30. September sei Muhamed mitten im Kampfgetümmel erschienen, aber diesmal sei scharf geschossen worden. Jamal Al-Dura habe den Knaben beobachtet, wie dieser Steine warf. Als er erkannt habe, dass das Kind unter Beschuss geriet, habe er es herausholen wollen – ohne Erfolg.

Sofort nach dem Vorfall wurden die Spuren verwischt. Der Betonklotz und die Mauer fielen. Alle Geschosse verschwanden. Die Israeli schossen mit M-16-Gewehren, die Palästinenser mit Kalaschnikows. Das Kaliber der M-16 beträgt 5,56 Millimeter, das der Kalaschnikow 7,62. Aufgrund der Geschosse hätte festgestellt werden können, wer geschossen hatte. Aber in den Spitälern von Gaza und Amman liessen die Ärzte die Kugeln verschwinden, bevor ihre Kaliber festgehalten werden konnten. Die Israeli bauten dann die Wand und den Klotz nochmals auf, um in Schussversuchen zu beweisen, dass es palästinensische Schützen waren, die Muhamed töteten. Aber die Bilder von France 2 konnten sie nicht ungeschehen machen.

Terrain früh besetzen

In den Psychological Operations geht es darum, die Gefahren rechtzeitig zu erkennen. Wer Erfolg haben will, muss Krisen, muss Angriffe, muss Gegner früh orten. Geeignete Strukturen müssen vor dem Ernstfall geschaffen werden. Ebenso kann es entscheidend sein, dass das Terrain rasch besetzt wird. Wer mit seiner Aktion zu lange wartet, riskiert den Anspruch auf Informationsführung zu verlieren. Offensive Operationen können eine bessere Aufnahme finden als defensive Taktiken, bei denen die Information unter Druck erfolgt.

Den Ausschlag gibt in aller Regel eine Informationsführung, die einheitlich angelegt und widerspruchsfrei ist. Namentlich im Kampf gegen den Terror kann nur bestehen, wer glaubwürdig auftritt. Terroranschläge wie die Attacke vom 11. September 2001 erschüttern die Welt wie kaum andere Ereignisse. In Zeiten von Panik und Schrecken stiften widersprüchliche Aussagen Verwirrung; sie schaffen Raum für unwillkommene Gerüchte und Spekulationen. Um so mehr zählen dann Qualitäten wie Offenheit, Sicherheit und Transparenz.

Literaturhinweise

Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz: Sicherheit durch Kooperation. Bern 2000.

Forster, Peter: Informationssicherheit als Verbundaufgabe. Hohe Verletzlichkeit von Staat, Wirtschaft und Gesellschaft. In: NZZ, 28. Mai 2002.

Haering, Kurt: Information – die entscheidende Qualität: Die hohe Verletzlichkeit. In: MQ Management und Qualität, Spezialausgabe Informationssicherheit 05/2002.

Joint Chiefs of Staff: Joint Doctrine for Information Operations. Joint Pub 3–13. Washington 1998.

Libicki, Martin: What is Information Warfare? National Defense University. SACIS Paper. Washington 1995.

United States Air Force: Informations Operations. Air Force Doctrine Document 2–5. Washington 1998.

Peter Forster
Dr. phil., Oberst, Kommandant Informationsregiment 1, Präsident der eidgenössischen Konsultativ-Kommission für Innere Sicherheit, Mitglied der Projektgruppe Information Operations des Generalstabs. Weinbergstrasse 11, 8268 Salenstein. ■